Naciones Unidas A/CN.9/WG.IV/WP.120

Asamblea General

Distr. limitada
27 de julio de 2012
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
Grupo de Trabajo IV (Comercio Electrónico)
46º período de sesiones
Viena, 29 de octubre a 2 de noviembre de 2012

Panorama general de la gestión de la identidad digital

Documento de antecedentes presentado por el *Identity Management Legal Task Force* de la *American Bar Association*

Nota de la Secretaría

En el marco de la preparación del 46º período de sesiones del Grupo de Trabajo IV (Comercio Electrónico), el equipo de tareas *Identity Management Legal Task Force* de la *American Bar Association* ha presentado a la Secretaría el documento adjunto.

El documento es traducción de un texto que fue reproducido en la forma en que lo recibió la Secretaría.

V.12-55149 (S) 040912 050912

I. Introducción

1. En 2011, en un informe de la Organización de Cooperación y Desarrollo Económicos (OCDE) se señalaba que la gestión de la identidad digital es fundamental para el desarrollo ulterior de la economía de la Internet[1] y es requisito esencial de todas las formas de comercio electrónico.

2. El presente documento ofrece una visión general de la gestión de la identidad digital, su función en el comercio electrónico, las cuestiones jurídicas que plantea y las barreras legales que plantea[2]. Se basa en la labor que adelanta el grupo de tareas *Identity Management Legal Task Force de la American Bar Association* (ABA)[3], y se presenta como material de antecedentes para informar al Grupo de Trabajo de cuestiones pertinentes[4].

3. En su 44º período de sesiones, celebrado en 2011, la Comisión convino en volver a reunir al Grupo de Trabajo IV (Comercio Electrónico) para que se ocupara del tema de los documentos electrónicos transferibles[5]. Al mismo tiempo, la Comisión convino en la ampliación del mandato del Grupo de Trabajo para que abarcase, por separado y no en relación con los documentos electrónicos transferibles, temas tratados en los documentos A/CN.9/728 y Add.1[6]. Esos temas comprendían la gestión de la identidad, la ventanilla única y los pagos mediante dispositivos móviles[7].

4. Como se señala más adelante (párrs. 6 y 7), la gestión de la identidad digital es un requisito fundamental respecto de cada uno de los temas pertinentes que la Comisión examinó en su 44º período de sesiones (documentos electrónicos transferibles, ventanilla única y pagos mediante dispositivos móviles). Por ello, será también un tema importante para la labor en curso del Grupo de Trabajo relacionada con los documentos electrónicos transferibles y para cualquier posible labor futura relacionada con los demás temas.

---

[1] OECD (2011) "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers," *OECD Digital Economy Papers*, núm. 196, OECD Publishing, pág. 3; el texto se puede consultar en www.oecd-ilibrary.org/science-and-technology/digital-identity-management-for-natural-persons_5kg1zqsm3pns-en.

[2] El presente documento se centra en los sistemas de gestión de la identidad comerciales concebidos para su utilización en el contexto empresarial, en particular en las comunicaciones entre empresas, entre empresas y gobiernos y entre empresas y consumidores.

[3] Identity Management Legal Task Force, Cyberspace Law Committee, American Bar Association, Section of Business Law; http://apps.americanbar.org/dch/committee.cfm?com=CL320041. Las opiniones expresadas en el presente documento no han recibido la aprobación de la comisión de delegados o la junta de gobernadores de la *American Bar Association* y, en consecuencia, no se deben interpretar como representación de la política de la ABA.

[4] Se puede consultar asimismo material adicional en la documentación del Coloquio de la CNUDMI sobre Comercio Electrónico, celebrado en Nueva York del 14 al 16 de febrero de 2011, disponible en www.uncitral.org/uncitral/en/commission/colloquia/electronic-commerce-2010.html.

[5] *Documentos Oficiales de la Asamblea General, sexagésimo sexto período de sesiones, Suplemento núm. 17* (A/66/17), párr. 250.

[6] *Ibid*., párr. 251.

[7] *Ibid*., párr. 241 a 249.

5. Es bien reconocida la importancia decisiva de la gestión de la identidad digital para facilitar el comercio electrónico fiable. Numerosos grupos intergubernamentales, estados, grupos internacionales privados y entidades comerciales estudian activamente las cuestiones y oportunidades relacionadas con la gestión de la identidad, elaboran normas técnicas y procesos empresariales y buscan formas de aplicar sistemas de identidad digital viables. A título de ejemplo, cabe mencionar:

a) Los Grupos intergubernamentales que trabajan activamente en cuestiones y normas de gestión de la identidad digital, entre los que figuran la OCDE[8], la Organización Internacional de Normalización (ISO)[9] y la Unión Internacional de Telecomunicaciones (UIT)[10];

b) En un estudio emprendido por la OCDE[11] se identificaron 18 países de esa Organización que adelantan activamente estrategias nacionales relacionadas con la gestión de la identidad (Alemania, Australia, Austria, Canadá, Chile, Dinamarca, Eslovenia, España, Estados Unidos de América, Italia, Japón, Luxemburgo, Nueva Zelandia, Países Bajos, Portugal, República de Corea, Suecia y Turquía)[12]. Otros varios países, como Estonia, la India y Nigeria, también aplican activamente estrategias de esa índole;

c) Varios proyectos regionales relacionados con la identidad digital se encuentran en marcha en la Unión Europea, entre los que cabe mencionar PrimeLife (un proyecto del Séptimo Programa Marco de la Comisión Europea)[13], Global Identity Networking of Individuals - Support Action (GINI-SA)[14], STORK (encaminado a establecer una plataforma europea de interoperabilidad de la eID)[15], y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)[16];

d) Entre las organizaciones privadas que trabajan en normas y políticas de identidad digital a nivel internacional figuran la Organization for the Advancement of Structured Information Standards (OASIS)[17], la Open Identity Exchange (OIX)[18], la Iniciativa Kantara[19], la Open ID Foundation[20], tScheme[21] y la Internet Society[22];

---

[8] www.oecd.org/document/38/0,3746,en_2649_34255_49319782_1_1_1_1,00.html.

[9] www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45306.

[10] www.itu.int/ITU-T/studygroups/com17/fgidm.

[11] Bernat, L. (2011), "National Strategies and Policies for Digital Identity Management in OECD Countries", OECD Digital Economy Papers, No. 177, OECD Publishing. doi: 10.1787/5kgdzvn5rfs2-en; at www.oecd-ilibrary.org/content/workingpaper/5kgdzvn5rfs2-en.

[12] *Ibid*., en las págs. 28 a 35 figura una lista de enlaces a documentos de los países.

[13] www.primelife.eu.

[14] www.gini-sa.eu.

[15] www.eid-stork.eu.

[16] www.enisa.europa.eu.

[17] www.oasis-open.org/home/index.php.

[18] www.openidentityexchange.com.

[19] http://kantarainitiative.org, conocida anteriormente como la Liberty Alliance, www.projectliberty.org.

[20] http://openid.net/foundation.

[21] www.tscheme.org.

[22] www.internetsociety.org.

e) Se han establecido algunos sistemas de identidad digital comerciales que funcionan a escala mundial en esferas reducidas. Entre ellos figuran los que administran Transglobal Secure Collaboration Program (TSCP)[23] y CertiPath[24] para las industrias aeroespacial y de defensa, la SAFE-BioPharma Association[25] para la industria biofarmacéutica, IdemTrust[26] para el sector financiero, el CA/Browser Forum[27] para los certificados EV-SSL de sitios web y FiXs - Federation for Identity and Cross-Credentialing Systems (FiXs)[28]. La labor de esos grupos se centra primordialmente en cuestiones relacionadas con normas técnicas y procesos empresariales y no en cuestiones de orden jurídico.

II. Relación entre la gestión de la identidad digital y el comercio electrónico

6. La gestión de la identidad digital es una cuestión fundamental para la mayoría de las transacciones del comercio electrónico y otras actividades en línea. Una preocupación primordial es la verificación de la identidad de partes alejadas que tratan, por ejemplo, de acceder a una base de datos en línea que contienen información confidencial, para realizar una transferencia en línea de fondos con cargo a una cuenta, o que han firmado un contrato electrónico, autorizado a distancia el despacho de un producto o enviado un correo electrónico. Si bien los participantes en muchas transacciones de bajo riesgo realizadas en línea tienden a confiar en que están tratando con una persona o entidad concreta, a medida que aumenta la confidencialidad o el valor de la transacción aumenta también la importancia de garantizar la disponibilidad y fiabilidad de información exacta acerca de la identidad de la parte que se encuentra a distancia a fin de tomar una decisión fundada en la confianza.

7. La gestión de la identidad digital es un requisito básico en lo tocante a las firmas electrónicas, al tema de los documentos electrónicos transferibles y a cualquier posible labor futura relacionada con los demás temas (ventanilla única y pagos mediante dispositivos móviles)[29].

a) La determinación de la identidad del signatario es uno de los requisitos para crear una firma electrónica válida. Tanto el artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996) como el artículo 9 de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (2005, Convención sobre Comunicaciones Electrónicas) estipulan, como condición de una firma electrónica válida, que se utilice para identificar al signatario un método que sea tan viable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos. El artículo 2 de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas

---

[23] www.tscp.org.
[24] www.certipath.com.
[25] www.safe-biopharma.org.
[26] www.identrust.com.
[27] www.cabforum.org.
[28] www.fixs.org.
[29] *Documentos Oficiales de la Asamblea General, sexagésimo sexto período de sesiones, Suplemento núm. 17* (A/66/17), párrs. 241 a 252.

requiere también como componente de una firma electrónica datos “que puedan ser utilizados para identificar al firmante”;

b) La verificación de la identidad es también un requisito decisivo de los documentos electrónicos transferibles, la ventanilla única y los pagos mediante dispositivos móviles. Las leyes vigentes relativas a los documentos electrónicos transferibles requieren que se determine la identidad tanto del firmante del documento como de la persona habilitada para hacer valer los derechos incorporados en él[30]. Los procesos de ventanilla única requerirán la determinación de la identidad del firmante de los documentos de aduana y la identidad de la persona o entidad que los archiva y la persona o entidad habilitada para hacerlos efectivos[31]. Asimismo, los pagos mediante dispositivos móviles, al igual que todos los demás sistemas de pago, requieren (a efecto de autorización) la identidad de la persona que afirme que transfiere los fondos[32].

III. Definición de la gestión de la identidad digital

8. Esencialmente, la gestión de la identidad digital tiene por objeto responder a dos preguntas sencillas que cada una de las partes en una transacción en línea se formula acerca de la otra parte, a saber, “¿quién es usted?” y “¿cómo puede demostrarlo?”. La capacidad para dar una respuesta fiable y creíble a esas preguntas se ha venido convirtiendo rápidamente en un requisito decisivo de las actividades del comercio electrónico, especialmente a medida que aumenta la índole, la importancia y la confidencialidad de ese tipo de transacciones. Apoyándose en las respuestas a esas dos preguntas, la parte en una transacción en línea puede decidir si procede o no a efectuar la transacción (por ejemplo, si celebra un contrato con la otra parte, si permite a la otra parte el acceso a una base de datos confidencial o si otorga a la otra parte algún otro privilegio o tipo de acceso).

9. Si bien toda entidad que sea parte en transacciones digitales podría crear su propio sistema para identificar a cada una de sus contrapartes comerciales y autenticar su identidad (como lo hacen actualmente muchas empresas mediante la utilización de distintos procesos de registro, unidos a un sistema de nombre de usuario y contraseña), esa modalidad está demostrando ser cada vez más costosa e inadecuada y plantea el problema de adaptar el sistema a poblaciones más amplias. Además, la creciente necesidad de la colaboración interinstitucional, las preocupaciones de seguridad y el problema de la administración de las contraseñas de los usuarios indican que ya no es adecuado el método habitual de nombres de usuario y contraseñas asignados por una empresa o por un proveedor.

10. En consecuencia, están surgiendo como método preferido los sistemas de identidad digital en los que el proveedor de la identidad de terceros (o proveedor de atributos) cumple una función básica. El objetivo es permitir que las empresas y los organismos gubernamentales realicen transacciones electrónicas con partes distantes apoyándose en la información sobre la identidad y los procesos de autenticación que ofrezca cualquiera de los varios proveedores independientes de identidad de terceros. Esa modalidad se denomina a menudo sistema de identidad “federado”.

---

[30] A/CN.9/WG.IV/WP.115, párrs. 24 a 26 y 45 a 48.

[31] A/CN.9/728/Add.1, párrs. 42 y 45.

[32] Véase, A/CN.9/728, parr. 52.

En otras palabras, la información sobre la identidad verificada por una entidad se facilita de manera convenida y controlada a múltiples partes en el marco de diferentes sistemas que tengan necesidad de información sobre la identidad con diversos propósitos. Ello permitiría, por ejemplo, que los particulares y las empresas utilizaran una credencial de identidad de su elección para realizar transacciones en línea con numerosas empresas, de la misma manera que una persona podría utilizar una licencia de conducir para una diversidad de transacciones diferentes de tipo no electrónico con diferentes entidades, como la compra de alcohol, la admisión a la zona de embarque de un aeropuerto o la apertura de una cuenta bancaria.

11. El desarrollo de un sistema de identidad federado requiere una combinación de normas y sistemas técnicos[33], procesos y procedimientos empresariales y normas jurídicas que, tomados en conjunto, creen un sistema fiable a fin de: i) verificar la identidad y vincular esa identidad con una persona física, entidad jurídica, dispositivo u objeto digital; ii) suministrar esa información sobre la identidad a una parte que la requiera para autorizar una transacción; y iii) mantener y proteger esa información durante su ciclo de duración. Un elemento fundamental para hacer que ese sistema funcione en un contexto comercial es el requisito de un marco jurídico idóneo y, típicamente, basado en un contrato que defina los derechos y responsabilidades de las partes, distribuya los riesgos y sirva de base para su aplicación. Ese marco jurídico se conoce a menudo como "reglas de funcionamiento" o "marco de confianza".

IV. Consideraciones básicas sobre la gestión de la identidad

12. Aunque la expresión "gestión de la identidad" es relativamente nueva, el concepto no lo es. Los procesos en que se apoya se han venido utilizando por largo tiempo en entornos fuera de línea. Los pasaportes, las licencias de conducir y las tarjetas de identificación de empleados son todos componentes de sistemas de identidad (en otras palabras, son credenciales expedidas por una entidad a personas cuya identidad ha confirmado de modo que posteriormente puedan demostrarla). El proceso de identificación de una persona y expedición de la correspondiente credencial también lo puede efectuar la parte que acepta la credencial (como ocurre con las tarjetas de identificación de empleados expedidas por una empresa) o un tercero (como ocurre con las licencias de conducir o el pasaporte). Un elemento básico de los sistemas federados, en los que hay un tercero que expide la credencial, es que el empleo de esas credenciales de identidad no está restringido a transacciones con las entidades que las expiden. Por el contrario, han sido concebidos y se utilizan previendo que las credenciales serán aceptadas por terceros (por ejemplo, el personal de seguridad de un aeropuerto, un banco o un barman en el caso de las licencias de conducir) cuando se exige prueba de determinados atributos de la propia identidad (como el nombre o la edad).

13. El problema se plantea a la hora de implantar una capacidad similar en un contexto en línea, o sea, crear un sistema de credenciales de identidad digital seguro, fiable y fehaciente que se puedan utilizar a distancia en el marco de sistemas

[33] Uno de los métodos que podría utilizarse para establecer un sistema de identidad es la infraestructura de clave pública (ICP). Sin embargo, se están desarrollando y aplicando muchas otras tecnologías y métodos.

y entidades diferentes (o sea, crear un sistema de identidad federado). Ese sistema permitirá a los sujetos a los que corresponden los datos utilizar la misma credencial de identidad para identificarse a fin de poder acceder a recursos o realizar transacciones con múltiples organizaciones.

14. Si bien hay muchos enfoques diferentes de la gestión de la identidad, esta entraña esencialmente dos procesos fundamentales: i) el proceso de reunir y verificar determinados atributos de identidad que corresponden a una persona (o a una entidad, dispositivo u objeto digital)[34] y expedir una credencial de identidad que refleje esas características ("identificación") y ii) el proceso de verificar posteriormente que una persona determinada que presenta esa credencial y sostiene que es la persona previamente identificada es, de hecho, esa persona ("autenticación"). Cada uno de esos procesos básicos puede entrañar diversos subprocesos, según la naturaleza de los datos y el contexto en que tienen lugar los dos procesos. Una vez que se han autenticado positivamente los atributos de identidad de una persona, viene un tercer grupo de procesos, conocidos en conjunto como "autorización", que están a cargo de la entidad que se propone apoyarse en la identidad autenticada para determinar los derechos y privilegios que se concederán a esa persona (por ejemplo, si se celebra un contrato con ella o si se le debe conceder acceso a una base de datos o una cuenta bancaria en línea).

A. Identificación

15. La finalidad del proceso de identificación es responder a la pregunta "¿quién es usted?". Ese proceso, que realiza alguien que cumple la función de proveedor de identidad[35], entraña la vinculación de los atributos identificantes (como nombre, número de afiliación, dirección o fecha de nacimiento) con una persona determinada, a fin de identificarla y definirla al nivel adecuado para el propósito previsto. Llamado a veces "comprobación de la identidad" o "inscripción", ese proceso a menudo se lleva a cabo una sola vez. Un proveedor de identidad suele reunir información acerca de la persona que ha de ser identificada (denominada el "sujeto") y se apoya con frecuencia en una diversidad de documentos emitidos oficialmente (por ejemplo, partida de nacimiento, tarjeta de la seguridad social, licencia de conducir y pasaporte) y en credenciales expedidas por entidades del sector privado (por ejemplo, distintivo de identificación de empleado, tarjeta SIM de comunicación inalámbrica por móvil y tarjetas de crédito). Aunque esos documentos y credenciales de identidad hayan sido expedidos con otros fines, con frecuencia se pueden volver a utilizar para facilitar más adelante procesos de identificación en nuevos contextos. Así ocurre, por ejemplo, cuando alguien presenta una licencia de conducir para demostrar su identidad a la hora de recibir un distintivo de identificación de empleado.

16. Al final del proceso de identificación, los atributos de identidad pertinentes del sujeto suelen quedar recogidos en datos consignados en un documento electrónico

---

[34] La información acerca de la identidad se puede reunir y verificar (y se pueden emitir las correspondientes credenciales de identidad) respecto de particulares, entidades jurídicas, dispositivos y objetos digitales. El presente documento se centra únicamente en los sistemas de identidad relacionados con personas físicas.

[35] En algún caso, cuando solo se requieren atributos seleccionados para el proceso de identificación, una entidad conocida como proveedor de atributos cumple esa función.

expedido por el proveedor de la identidad y que se conoce como credencial de identidad. La credencial presenta (o vincula o correlaciona) los datos que se utilizan para autenticar la identidad digital invocada o los atributos de una persona, entidad o dispositivo[36]. Una credencial puede ser incorporada en una diversidad de medios. En el mundo físico, son ejemplos de una credencial de identidad el sello real, la licencia de conducir, el pasaporte, la tarjeta de una biblioteca o el distintivo de identificación de empleado. En el mundo en línea, la credencial de identidad puede ser tan sencilla como la identificación de usuario o tan compleja como un certificado digital expresado criptográficamente que puede ser almacenado en una computadora, un teléfono móvil, una tarjeta inteligente, una tarjeta de cajero automático, una memoria informática o cualquier dispositivo similar.

B. Autenticación

17. Cuando una persona presenta una credencial (por ejemplo, una licencia de conducir en un aeropuerto o al registrar la identificación de usuario en una red de empresas) declara que es la persona identificada en la credencial y pide ejercitar un derecho o privilegio otorgado a esa persona (por ejemplo, abordar un avión, acceder a una red corporativa o a una base de datos confidencial), la "parte receptora" recurre a un proceso de autenticación para determinar si esa persona es, de hecho, quien afirma ser. En otras palabras, una vez que alguien declara quién es (afirmando ser la persona identificada en la credencial de identidad), la autenticación tiene por objeto responder a la pregunta "muy bien, ¿cómo puede probarlo?". Se trata de un trámite relacionado con una transacción concreta que supone la vinculación de la persona con la credencial de identidad presentada, a fin de verificar que la persona que desea intervenir en la transacción es realmente la que ha sido identificada mediante la credencial.

18. La autenticación suele requerir un elemento que vincule a la persona con la credencial, elemento que se conoce por lo general como autenticador. Cuando la credencial es una licencia de conducir o un pasaporte, el autenticador es la fotografía y la vinculación se hace de ordinario comparando la fotografía que se encuentra en la licencia o el pasaporte con la persona que los presente. En el caso de las credenciales electrónicas, el autenticador es normalmente un dato que la persona "conoce" (por ejemplo, una contraseña secreta o un número de identificación personal), una información que la persona "posee" (por ejemplo, una clave criptográfica privada, un dispositivo físico como una tarjeta inteligente, un USB u otro tipo de seña) o algo que la persona "es", por ejemplo, una característica física (comprobada en una fotografía, las huellas digitales u otros datos biométricos).

C. Autorización

19. Una vez hecha la autenticación debida de una persona, la parte receptora puede emplear su propio proceso de autorización para determinar los derechos y privilegios que se otorgan a esa persona (por ejemplo, si se le debe dar acceso a un sitio web, una base de datos, un bar o la zona de embarque de un aeropuerto).

[36] OECD Guidance for Electronic Authentication (2007), pág. 12, se puede consultar en www.oecd.org/dataoecd/32/45/38921342.pdf.

Ese proceso plantea la pregunta "¿A qué está usted autorizado?". Por ello, la autenticación de la identidad no constituye solamente un fin en sí. Con frecuencia se emplea para facilitar las decisiones de autorización de la parte receptora como la concesión de derechos o privilegios (por ejemplo, el acceso a los recursos en línea del sistema) o para celebrar una transacción. Por ejemplo, una vez que la identidad de una persona que solicita acceso a una red informática ha sido autenticada, el propietario del sistema (o sea, la parte receptora) puede emplear un proceso de autorización a fin de determinar los derechos de acceso que se le deberían conceder. Asimismo, una vez autenticada la identidad de alguien que desee celebrar una transacción electrónica (por ejemplo, un contrato electrónico), la parte receptora puede utilizar un proceso de autorización para determinar si procede a realizar la transacción con el interesado o utiliza de alguna otra forma la comunicación.

D. Identidad federada

20. Tratándose de transacciones en línea, comúnmente la identificación y la expedición de credenciales las ha efectuado la misma parte que tiene también la intención de exigir la credencial. Por ejemplo, una empresa identificará a un empleado y le asignará un nombre de usuario y una contraseña que le permita acceder a la red de la empresa. En tal caso, esta actúa tanto como proveedor de la identidad (ya que ha identificado la persona como su empleado y le ha expedido una credencial de identidad) y como parte receptora (puesto que también acepta y se sirve de esa credencial para autorizar el acceso a su red).

21. En un sistema de identidad "federado", las funciones de proveedor de la identidad y parte receptora no las cumple necesariamente la misma entidad. Por el contrario, múltiples partes receptoras no relacionadas entre sí pueden aceptar las credenciales de identidad que expida cualquiera de los diversos proveedores de identidad independientes. De acuerdo con ese modelo, una única credencial de identidad puede ser aceptada por numerosas organizaciones que no hayan tenido participación directa en la expedición original de la credencial.

22. En los servicios fuera de línea, un ejemplo conocido de un proceso federado de gestión de la identidad es la forma en que actualmente se expiden y utilizan las licencias de conducir. Esas licencias, expedidas por una entidad gubernamental, las utilizan diversas partes receptoras no relacionadas entre sí para verificar los atributos de identidad del titular de la licencia. Por ejemplo, un agente de seguridad la utiliza para comprobar el nombre de una persona que solicita ingresar a la zona de embarque de un aeropuerto o un barman para verificar la edad de la persona que pide una bebida alcohólica.

23. En los servicios en línea de sistema de identidad federado, un ejemplo es el de los cajeros automáticos. En una transacción típica en un cajero automático una persona que tenga una cuenta en el banco A puede utilizar la credencial de identidad que le ha expedido su propio banco (la tarjeta de cajero) para retirar dinero en efectivo en un cajero operado por el banco B (con el que el interesado no tiene ninguna vinculación). Para dar curso a la transacción, a pesar de que no exista una vinculación de esa índole, el banco B se pone en contacto con el banco A a través de la red de cajeros automáticos para determinar si la persona es un cliente autorizado del banco A, hacer que el banco A autentique la identidad del cliente (o sea,

determine si utilizó la contraseña correcta) y para obtener de ese banco determinada información sobre la identidad relacionada con el cliente (por ejemplo, si en la cuenta hay fondos suficientes que respalden el retiro de dinero solicitado y, en algunos casos, obtener el saldo de la cuenta a fin de que el banco B lo pueda imprimir en el recibo de la transacción).

IV. Riesgos de los sistemas de identidad

24. La participación en un sistema de identidad y el recurso a los datos correspondientes entraña varios riesgos posibles, entre los que figuran:

a) Riesgo en la identificación: la fiabilidad de la información reunida y declarada sobre la identidad de los sujetos es de importancia decisiva para la utilización de cualquier sistema de identidad. El riesgo en la identificación representa el riesgo de que los datos sobre los atributos de la identidad reunidos y vinculados a un sujeto determinado sean inexactos. Ese riesgo está a menudo en relación directa con la calidad de las credenciales de identidad en contextos fuera de línea suministradas por el sujeto para la verificación de su identidad;

b) Riesgo en la autenticación: la identificación no tiene utilidad a menos que la parte receptora tenga la capacidad de autenticarla (o sea, de vincular los atributos de identidad declarados con el sujeto correcto). El riesgo en la autenticación incluye tanto el riesgo de que un sujeto legítimo no pueda ser adecuadamente objeto de autenticación como el riesgo de que el proceso de autenticación indique incorrectamente que un impostor es el sujeto legítimo;

c) Riesgo relacionado con la privacidad: en el caso de los particulares la gestión de la identidad conlleva la reunión y verificación de información personal acerca de un sujeto por parte de un proveedor de identidad y el intercambio de esa información con múltiples partes receptoras. Además, las transacciones basadas en la identidad pueden facilitar también el rastreo de las actividades de una persona, con lo cual se genera información personal adicional. El riesgo relacionado con la privacidad tiene que ver principalmente con la utilización no autorizada o el abuso de la información personal acerca del sujeto por una de las partes que tiene acceso a ella y con el cumplimiento por esas entidades de las obligaciones tocantes a la elaboración y protección de los datos;

d) Riesgo relacionado con la seguridad de los datos: en cualquier sistema de identidad es de importancia decisiva la protección de la información personal acerca de los sujetos identificados y el mantenimiento de la seguridad de los procesos necesarios para crear credenciales de identidad seguras, comunicar información exacta sobre la identidad, verificar la situación de las credenciales de identidad y autenticar a los sujetos. El riesgo de seguridad comprende el peligro de que una parte no autorizada pueda obtener acceso a datos personales y el riesgo de que se vea comprometido cualquiera de los procesos fundamentales para el funcionamiento general del sistema de identidad o cualquiera de las distintas transacciones relacionadas con la identidad;

e) Riesgo relacionado con la responsabilidad: en todo sistema de identidad ocurrirán inevitablemente fallos y se ocasionarán perjuicios. Los participantes en un sistema de identidad deben enfrentarse al riesgo de que se les haga responsables de

perjuicios sufridos por un tercero como resultado de un problema que hayan ocasionado o del que se les considere jurídicamente responsables. Un aspecto básico del riesgo de responsabilidad es la incertidumbre jurídica respeto de la responsabilidad inherente a un acto u omisión determinados por parte de un participante en un sistema de identidad, en particular cuando opera en múltiples sectores empresariales y jurisdiccionales;

f) Riesgo relacionado con la ejecutoriedad: el riesgo relacionado con la ejecutoriedad es complementario del riesgo de responsabilidad. Se trata del riesgo de que un participante no pueda hacer valer i) su derecho a que otro participante cumpla con las normas, o ii) su derecho a recibir indemnización por daños y perjuicios cuando sufra efectivamente daños en caso de que otro participante sea jurídicamente "responsable". Este riesgo se da cuando algo sale mal y alguien trata de reclamar indemnización por daños y perjuicios. Se aplica también en situaciones en que aunque un problema no haya surgido todavía, un error de ejecución por parte de uno o más participantes puede poner en peligro la totalidad del sistema de identidad. Ese aspecto es particularmente importante en un sistema multijurisdiccional. En tal caso, el riesgo relacionado con la ejecutoriedad se refiere tanto a la capacidad de detectar el problema como a la capacidad de exigir que el participante subsane su error de ejecución o se retire del sistema;

g) Riesgo relacionado con el cumplimiento reglamentario: en muchos casos, la participación en un sistema de identidad plantea cuestiones de cumplimiento jurídico para uno o más de los participantes (o sea, determinar si la conducta del participante cumple con las leyes nacionales aplicables). En otros casos, el propósito de la participación en el sistema de identidad es, por su propia índole, un esfuerzo por cumplir los requisitos legales impuestos a un participante. Por ejemplo, una institución financiera puede participar en el sistema y apoyarse en las credenciales de identidad con miras a satisfacer sus obligaciones jurídicas de autenticar debidamente a las personas a las que concede acceso en línea a cuentas bancarias y servicios de pago. En tales casos, el riesgo relacionado con el cumplimiento tiene que ver principalmente con la determinación de si esa participación satisface las obligaciones jurídicas.

25. Como ocurre con cualquier sistema, los riesgos anteriormente descritos dependen de la tecnología utilizada, de los diversos procesos ejecutados y de la forma en que los propios participantes cumplen o dejan de cumplir las obligaciones (así como de la posible influencia de partes externas). La creación de un sistema de identidad fiable exigirá medidas para abordar esos riesgos, o sea, medidas para garantizar que los participantes pueden confiar en la tecnología empleada (garantizar que funciona adecuadamente), en los procesos aplicados (garantizar que producen el resultado correcto) y en otros participantes (garantizar que habrán de cumplir debidamente sus obligaciones).

V. Relación entre funcionalidad y riesgo: reglas de funcionamiento

26. Para lograr que un sistema de identidad federado funcione en un entorno en línea y abordar riesgos como los arriba indicados se requiere no solo la aplicación de una tecnología apropiada, sino también el cumplimiento por todos los

participantes (sujetos, proveedores de identidad y partes receptoras) de un cuerpo común de normas técnicas, requisitos operacionales y reglas jurídicas. Los sistemas de identidad comerciales suelen tratar de lograr ese objetivo mediante la formulación de "reglas de funcionamiento" apropiadas (que a veces se conocen como "marco de confianza") a cuyo cumplimiento los participantes están contractualmente obligados.

27. Las reglas de funcionamiento de los sistemas de identidad se agrupan en dos categorías generales de componentes, a saber: i) las reglas operacionales y especificaciones técnicas y empresariales necesarias para hacer que el sistema sea funcional y fiable y ii) las normas jurídicas de tipo contractual que, además de las leyes y reglamentos aplicables, definen los derechos y obligaciones jurídicas de las partes que sean específicos del sistema de identidad y faciliten cuando sea necesario su cumplimiento.

a) Las reglas operacionales técnicas y empresariales definen los requisitos de funcionamiento adecuado del sistema de identidad y las funciones y responsabilidades operacionales de los participantes, y ofrecen una garantía adecuada de la exactitud, integridad, privacidad y seguridad de sus procesos y datos (de modo que las diversas partes se muestren dispuestas a participar y que el sistema merezca confianza). En muchos casos esas reglas se basan en normas ya existentes;

b) Las normas jurídicas de tipo contractual corresponden a acuerdos celebrados entre los participantes sobre la base de un contrato que definen y regulan los derechos, responsabilidades y obligaciones jurídicas de los participantes con respecto al sistema de identidad de que se trate, clarifican los riesgos jurídicos que las partes asumen por el hecho de participar en el sistema de identidad (por ejemplo, garantías, responsabilidad por daños, riesgos para sus datos personales); y prevén recursos en caso de que surjan diferencias entre las partes, entre ellos métodos de solución de controversias, mecanismos de ejecución, derechos de rescisión y medidas de indemnización por daños y perjuicios, sanciones y otras formas de responsabilidad. En virtud de esas normas las reglas operacionales técnicas y empresariales adquieren carácter jurídico vinculante para los participantes y tienen fuerza legal frente a ellos.

28. Tanto las normas operacionales técnicas y empresariales como las reglas jurídicas de base contractual están, desde luego, sujetas a otros deberes y obligaciones existentes derivados del derecho estatutario y reglamentario que se aplique a las partes, y se suelen interpretar con referencia a ellos. Los dos componentes de las normas operativas del sistema de identidad (o sea, las normas operacionales técnicas y empresariales y las normas jurídicas) están sujetos a los estatutos y reglamentaciones vigentes que se apliquen en la jurisdicción o jurisdicciones pertinentes y en las que el sistema de identidad habrá de funcionar o se habrá de utilizar.

29. Las normas de funcionamiento de los sistemas de identidad son en gran medida similares a las normas de funcionamiento utilizadas en los sistemas de tarjetas de crédito o los sistemas de pago electrónico, que deberán poder incluir a numerosos participantes de una diversidad de jurisdicciones de acuerdo con un conjunto de normas comunes. Las reglas de funcionamiento de las tarjetas de crédito, por ejemplo, contienen disposiciones relativas a las entidades emisoras y procesadoras, los comerciantes que las aceptan y los titulares de la tarjeta, y prevén

las especificaciones y reglas aplicables a los participantes en transacciones de crédito en línea y su procesamiento ulterior[37]. Asimismo, las normas de funcionamiento de los sistemas de transferencia electrónica de fondos regulan las responsabilidades de todos los bancos que intervienen en el proceso de pago y, en medida limitada, las de los consumidores y otros pagadores, y estipulan las especificaciones y reglas aplicables a los participantes cuando se utilizan las transferencias electrónicas de fondos (por ejemplo, las transferencias SWIFT)[38] a fin de facilitar el pago en una transacción en línea.

30. Aunque se suele reconocer la necesidad de que las reglas de funcionamiento del sistema de identidad contengan normas jurídicas idóneas, su formulación es en gran medida un territorio sin explorar. Es preciso determinar y abordar numerosas cuestiones y barreras de orden jurídico.

VI. Régimen jurídico que rige los sistemas de identidad

31. En la mayoría de las jurisdicciones, hay numerosas leyes y reglamentaciones en vigencia que tendrán una repercusión significativa desde el punto de vista reglamentario en la participación en un sistema de identidad (y que pueden imponer barreras, requisitos de cumplimiento o riesgos de responsabilidad). Además, las diferencias entre las legislaciones de diferentes jurisdicciones, vistas a la luz de la naturaleza mundial de la Internet, crean un panorama reglamentario muy variado que puede plantear de por sí un reto para la estructuración jurídica. Aunque algunas de las leyes y reglamentaciones aplicables se centran concretamente en actividades relacionadas con la identidad, la mayoría han sido formuladas en un contexto completamente ajeno a la gestión de la identidad (por ejemplo, el derecho de responsabilidad civil, el derecho contractual o el derecho de garantías). No obstante, pueden tener, una repercusión significativa, a menudo en formas que no se preveían en el momento de su adopción original.

32. Algunas de las categorías de ordenamiento jurídico aplicables a los sistemas de identidad (o a los participantes en ellos) son las siguientes:

---

[37] Las normas de funcionamiento de las tarjetas de crédito incluyen las especificaciones y reglas relacionadas con el emisor de la tarjeta de crédito (véase, por ejemplo, Visa International Operating Regulations at http://usa.visa.com/merchants/operations/op_regulations.html and the Payment Card Industry Data Security Standards - PCIDSS at www.pcisecuritystandards.org/security_standards/index.php), que tienen carácter vinculante para los bancos procesadores y los comerciantes, y los contratos entre los bancos emisores de la tarjeta de crédito y los bancos procesadores, los contratos entre los bancos procesadores y los comerciantes y los contratos entre los bancos procesadores y los titulares de la tarjeta. Además se complementan mediante leyes y reglamentos que rigen el procesamiento de tarjetas de crédito en cada jurisdicción.

[38] Las reglas de funcionamiento de la transferencia electrónica de fondos incluyen las especificaciones y normas aplicables a ese tipo de transacciones (por ejemplo, the Operating Rules and Guidelines of U.S.-based NACHA - The Electronic Payments Association, www.nacha.org/) que adquieren carácter vinculante para los bancos procesadores y los comerciantes, así como los contratos entre los comerciantes y los distintos pagadores. Asimismo, se complementan con leyes y reglamentos que rigen las transferencias electrónicas de fondos, como la Electronics Funds Transfer Act and Regulations E (en los Estados Unidos de América).

a) La legislación que regula la exactitud de la información sobre la identidad: las actividades de los sistemas de identidad se centran en la recopilación y verificación por parte de los proveedores de identidad o de atributos de la información acerca de los sujetos y la comunicación de alguna de esa información a las partes receptoras. En tales casos la exactitud y la fiabilidad de dicha información son de importancia. Por ello, las leyes relativas al suministro de información falsa o incorrecta, ya sea intencionalmente o por negligencia, serán pertinentes para la evaluación de los derechos, obligaciones y responsabilidades de los participantes en los sistemas de identidad. Entre ellas son de importancia básica las leyes del régimen de responsabilidad civil que rigen la declaración falsa por negligente, el endoso negligente y la difamación, así como las leyes sobre garantías, las leyes sobre robo de la identidad y las leyes que rigen las prácticas comerciales injustas y engañosas;

b) La legislación que regula la privacidad de la información sobre la identidad: por su propia índole, la gestión de la identidad entraña normalmente la reunión por el proveedor de identidad o sus agentes de información personal acerca de un sujeto, y su revelación a la parte receptora[39]. Por ello, las leyes de protección de datos, las leyes sobre privacidad y otras leyes y reglamentaciones que regulan la reunión, utilización, procesamiento, transferencia y almacenamiento de datos personales tendrán una importante repercusión en las actividades de gestión de la identidad. Aunque muchas de esas leyes fueron redactadas en épocas anteriores al advenimiento de los sistemas de identidad digital y, en consecuencia, no podrían haber previsto los procesos particulares o daños potenciales inherentes a esos sistemas, pueden, con todo, tener un efecto directo en esas actividades;

c) La legislación que regula la reunión de información sobre la identidad: además de las leyes sobre privacidad y protección de los datos, las leyes que regulan la reutilización de información proveniente del sector público afecta a las empresas que crean productos y servicios de información basados en datos recopilados masivamente por el sector público. Esas leyes pueden crear barreras jurídicas a la utilización en gran escala de los datos que mantienen los órganos del sector público en el contexto de los servicios de identidad[40];

d) La legislación que regula la seguridad de la información sobre la identidad y de los procesos conexos: muchas leyes imponen a las empresas obligaciones en lo que respecta a la seguridad de la información personal (según se define de diversas maneras en jurisdicciones diferentes y en virtud de leyes concretas de un sector determinado) y otros datos en su poder. Además de las leyes y reglamentaciones que imponen la obligación de aplicar medidas de seguridad para proteger los datos, muchas jurisdicciones han promulgado también leyes y reglamentaciones que imponen la obligación de revelar a las personas afectadas las violaciones de la seguridad relacionadas con su información personal;

---

[39] Excepto cuando el sujeto no es un ser humano, por ejemplo, cuando se trata de una persona jurídica, un dispositivo, una aplicación informática, entre otros.

[40] Véase, de manera general, Global Networking of Individuals (GINI), Legal provisions for Deploying INDI Services (5 de octubre de 2011) Sección 5, en www.gini-sa.eu/images/stories/2011.11.06_GINI_D3.1_Legal%20Provisions%20for%20Deploying%20INDI%20Services_FINAL.pdf.

e) La legislación relativa a la obligación de determinar la identidad: muchas leyes y reglamentaciones exigen la identificación, como elemento constitutivo de una transacción, en particular en un entorno electrónico. Por ejemplo, la Convención sobre la Utilización de las Comunicaciones Electrónicas requiere expresamente la determinación de identidad como elemento de una firma electrónica jurídicamente vinculante. En concreto, cuando la ley requiera que una parte firme una comunicación o un contrato, la Convención estipula que el requisito de la firma se dará por cumplido si se utiliza un método para determinar la identidad de esa parte y para indicar la voluntad que tiene tal parte respecto de la información consignada en la comunicación electrónica[41];

f) La legislación relativa a la obligación de autenticación: varias leyes regulan uno o más elementos de la autenticación. Algunas imponen a las empresas la obligación de proceder a la autenticación de las personas con los que realizan transacciones a distancia y otros regulan aspectos del proceso de autenticación. Un ejemplo destacado es el requisito establecido en los Estados Unidos de América por los reguladores del sector bancario en relación con la autenticación de las actividades bancarias en línea. En concreto, las instituciones financieras que ofrecen a sus clientes productos y servicios a través de la Internet deberán utilizar métodos eficaces para autenticar la identidad de los clientes que utilizan esos productos y servicios[42]. Otros países (por ejemplo Singapur) también han adoptado requisitos similares[43];

g) La legislación que regula específicamente las actividades de los sistemas de identidad: algunas jurisdicciones cuentan con estatutos que regulan expresamente algunos aspectos de las actividades de gestión de la identidad. Un ejemplo es la Directiva de la Unión Europea sobre firmas electrónicas[44], que estipula que los Estados miembros deben regular la reunión de datos personales por parte de determinados proveedores de identidad (llamados proveedores de servicios de certificación) y reglamentar la expedición de credenciales[45]. De igual manera, la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (artículos 8 a 12) establece reglas para la expedición y utilización de las credenciales de identidad requeridas para la creación de determinadas firmas electrónicas.

---

41 Convención sobre la Utilización de Comunicaciones Electrónicas, artículo 9, 3).

42 Federal Financial Institutions Examination Council (“FFIEC”), “Authentication in an Internet Banking Environment”, 12 de octubre de 2005, pág. 1; se puede consultar en www.ffiec.gov/pdf/authentication_guidance.pdf.

43 Monetary Authority of Singapore, circular núm. SRD TR 02/2005, 25 de noviembre de 2005.

44 Directiva 1999/93/CE por la que se estable un marco comunitario para la firma electrónica (“Directiva de la Unión Europea sobre firmas electrónicas”), artículos 6 a 8 y Anexos I y II, que se puede consultar en http://europa.eu/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf.

45 Directiva de la Unión Europea sobre firmas electrónicas, artículo 8.

H. Problemas y barreras jurídicas

33. Las leyes y reglamentaciones existentes de los tipos indicados anteriormente, al igual que otras, plantean varios problemas básicos para la creación y funcionamiento de sistemas de identidad en el sector privado. Entre esos problemas cabe mencionar los siguientes:

a) Legislación no escrita para abordar la gestión de la identidad: la legislación vigente simplemente no se ocupa de muchas de las cuestiones de reciente aparición que plantean los procesos de gestión de la identidad digital. La mayor parte de las leyes existentes que se aplican en esos contextos no fueron redactadas desde la perspectiva de los sistemas de identidad digital y, por tanto, abordan o reglamentan inadecuada o inapropiadamente las actividades pertinentes. Por ejemplo, la legislación en vigor suele pasar por alto la obligación que debe cumplir el certificador de la identidad de proceder con la debida cautela al evaluar la autenticidad de los documentos de prueba de la identidad, o el alcance de la obligación de proporcionar información que el proveedor de la identidad tiene con el titular de los datos;

b) Incertidumbre/ambigüedad jurídica: si bien hay algunas cuestiones relacionadas con la gestión de la identidad digital que posiblemente estén contempladas en las leyes y reglamentaciones vigentes, frecuentemente la aplicabilidad de esas leyes no está clara o es ambigua, lo que deja en los participantes en los sistemas de identidad un grado considerable de incertidumbre jurídica, que puede retardar el crecimiento, la innovación y la inversión. Incluso cuando las leyes vigentes se aplican a la gestión de la identidad, la manera en que se aplican a una cuestión concreta o un enfoque propuesto de un sistema de identidad tal vez no sea clara. Esta afirmación es particularmente válida en relación con las leyes que se centran en una tecnología concreta. Ello puede limitar la capacidad de las partes que conciertan transacciones relacionadas con la identidad para evaluar y gestionar los riesgos que asumen al hacerlo;

c) Cuestiones de privacidad: por su propia naturaleza, en la gestión de la identidad comúnmente un proveedor de la identidad reúne determinada información personal acerca de un sujeto y la da a conocer a la parte receptora. Para participar en un sistema de identidad, los sujetos deben revelar información personal y exponerse así al riesgo de que la información se utilice sin su autorización o en forma indebida. Además, puesto que los sujetos interactúan con múltiples partes receptoras, la comunicación o verificación requeridas de su información por parte del proveedor de la identidad le permite a este rastrear las actividades de cada sujeto, lo que da pie a preocupaciones acerca de la reunión y utilización de la información relacionada con cada transacción. La privacidad es, por tanto, una cuestión básica de todo sistema de identidad digital, que puede entrañar el planteamiento de cuestiones como: i) el tipo de información que puede reunir el proveedor de la identidad; ii) la cantidad de información que se podrá revelar a las partes receptoras; iii) el control que el sujeto tiene respecto de la revelación de la información; iv) el nivel de seguridad que deben tener los datos que manejan las partes; y v) los límites que se aplican al empleo de la información por parte del proveedor de la identidad y las partes receptoras. Esas cuestiones están con frecuencia previstas en las leyes vigentes, que podrán también complementarse mediante reglas operativas basadas en un contrato;

d) Cuestiones de responsabilidad: una preocupación de orden jurídico de importancia fundamental para los participantes en todo sistema de identidad es la de determinar quién asumirá la responsabilidad asociada con cualquiera de los riesgos (véase párr. 24 *supra*). Se han planteado numerosas teorías de derecho consuetudinario, estatutario y contractual para determinar, definir y esclarecer la fuente y el alcance de esas posibles responsabilidades[46]. Con todo, esos riesgos jurídicos con frecuencia no están bien definidos y son inciertos. Las preocupaciones en torno a la responsabilidad jurídica representan una barrera básica para el sector privado a la hora de adoptar soluciones interoperables en materia de identidad digital. Con frecuencia el mejor criterio es abordar las cuestiones relacionadas con la responsabilidad mediante reglas operativas u otras formas de acuerdo contractual entre los participantes, en vista particularmente de que ese enfoque permite la "personalización" de los contratos necesaria para establecer una distribución de riesgos idónea, que habrá de variar de un caso a otro;

e) Variaciones y conflictos jurisdiccionales: hay algunas cuestiones básicas respecto de las cuales la aplicación de las leyes y reglamentaciones vigentes a las actividades relacionadas con la identidad varía considerablemente entre las distintas jurisdicciones. Así ocurre a menudo respecto de las leyes que rigen la responsabilidad del participante y las leyes de protección de datos que regulan la privacidad de la información personal. Además, en algunos casos, la regulación o la concesión de licencias de actividades de los sistemas de identidad pueden plantear barreras adicionales al funcionamiento de los sistemas de identidad a nivel transfronterizo. En consecuencia, cuando los sistemas de identidad funcionan más allá de las fronteras jurisdiccionales, el hecho de que las leyes y reglamentaciones vigentes varíen (con frecuencia considerablemente) entre jurisdicciones agravan las dificultades de la formulación de reglas de funcionamiento adecuadas;

f) Necesidad de interoperabilidad jurídica: los sistemas de identidad se ven ante el problema que plantea el hecho de que las leyes aplicables pueden diferir de una jurisdicción a otra. A falta de leyes uniformes que regulen esas actividades, los sistemas de identidad tratan de resolver el problema elaborando reglas de funcionamiento que prevean la interoperabilidad en todo el sistema. La variación de leyes y reglamentaciones entre jurisdicciones dificultará la elaboración de esas reglas de funcionamiento y de otros contratos que son necesarios para lograr que la actuación de los participantes en el sistema sea más uniforme entre sistemas en línea;

g) Restricciones de la capacidad de modificar la legislación por contrato: algunas de las leyes y reglamentaciones vigentes pueden ser modificadas mediante contrato. Por ejemplo, muchos estatutos incorporan doctrinas de derecho comercial o contractual que simplemente establecen "reglas supletorias" que se aplican cuando no ha habido una elección expresa por las partes en una transacción, aunque permiten su modificación mediante acuerdo entre ellas. En tales casos, las partes en el sistema de identidad están en libertad de modificar las reglas supletorias y subsanar los vacíos mediante la aplicación de reglas de funcionamiento apropiadas

---

[46] Véase *Certification Authority Liability Analysis* (estudio preparado para la American Bankers Association, en el que se examinan los posibles riesgos en materia de responsabilidad de un proveedor de identidades que actúa como autoridad de certificación); se puede consultar en http://64.78.35.30/article/ca-liability-analysis.pdf.

de base contractual. Sin embargo, en otros casos no se puede hacer caso omiso de normas de derecho imperativas mediante el simple acuerdo de las partes, puesto que esas reglas cumplen finalidades de política pública como la protección de los consumidores o de terceros.

34. En consecuencia, las leyes vigentes pueden crear barreras a la adopción de sistemas de identidad eficientes, interoperables y fiables que puedan funcionar a nivel transfronterizo. La formulación de reglas de funcionamiento de un sistema de identidad digital basadas en contratos es el método principal de abordar esas dificultades jurídicas y reducir la incertidumbre para los participantes. Asimismo, facilita la experimentación con sistemas diferentes y criterios diferentes a medida que el mercado se ocupa de resolver la cuestión de la gestión de la identidad digital.

35. Todos los participantes en un sistema de identidad federado tienen interés tanto en la distribución equitativa, por anticipado, de los riesgos de responsabilidad que se derivan de la participación en el proceso como en la mitigación de esos riesgos en la medida posible. Si no se determina la forma en que se debe distribuir la responsabilidad o quién está en mejores condiciones de asumir los riesgos, las incertidumbres jurídicas existentes seguirán siendo una gran barrera para la aplicación de un sistema de identidad fiable. A medida que los procesos de gestión de la identidad digital se utilicen para transacciones más importantes y los riesgos para las partes aumenten en forma acorde, cobrarán importancia los beneficios que tiene para todas las partes la aplicación de reglas de funcionamiento apropiadas para abordar esos riesgos anticipadamente y mitigarlos (en la medida posible) estipulando que cada participante cumpla obligaciones concretas.

36. De cara al futuro el reto es crear sistemas de identidad digital aplicables a las transacciones comerciales en el sector privado, a escala transfronteriza y en forma interoperable. Al igual que los sistemas de tarjetas de crédito y pagos electrónicos, las reglas de funcionamiento de los sistemas de identidad habrán de basarse probablemente en arreglos contractuales, sobre todo en la medida en que se tenga la intención de aplicarlas a nivel de la Internet sobrepasando las fronteras jurisdiccionales. Tal vez sea oportuno plantearse el examen de legislación destinada a eliminar las barreras a esos sistemas (y no a reglamentarlos).

* * *

DEFINICIONES

[*NOTA: Las presentes definiciones son de carácter general y se consignan exclusivamente para ayudar a comprender el texto anterior*]

Atributo: Cualidad o característica identificada inherente o adscrita a un sujeto como, en el caso de una persona física, el nombre, dirección, edad, sexo, cargo, sueldo, patrimonio neto, número de la licencia de conducir y número de seguridad social, entre otras, y en el caso de un dispositivo, marca y modelo, número de serie, ubicación y capacidad, entre otras. Sinónimos: atributo de identidad.

Autenticación: proceso de verificación de la identidad que un sujeto afirma poseer mediante la confirmación de su vinculación con la credencial. Por ejemplo, al introducir una contraseña que esté vinculada a un nombre de usuario se supone que de esa manera se verifica que el usuario es realmente la persona a la que se asignó dicho nombre. De igual manera, al comparar el aspecto de una persona que presenta

un pasaporte con la fotografía que aparece en el documento se verifica o confirma que se trata efectivamente la persona descrita en él.

Autenticador: Indicador referente que se utiliza para verificar la relación entre un sujeto y una credencial; suele ser un objeto, un elemento de conocimiento o alguna característica del poseedor que se utiliza para vincular a la persona con una credencial de identidad. Por ejemplo, una contraseña hace las veces de autenticador de la identidad del usuario y una fotografía sirve como autenticador de un pasaporte o una licencia de conducir.

Autorización: proceso de otorgamiento de derechos y privilegios a los sujetos que han sido objetos de autenticación basándose en criterios determinados por la parte receptora; su finalidad es controlar el acceso a la información o los recursos de modo que solo tengan acceso a ellos las personas a las que esté expresamente permitido utilizarlos.

Credencial: datos presentados como prueba de la identidad que declara un sujeto. Entre los ejemplos de credenciales en papel cabe citar el pasaporte, la partida de nacimiento, la licencia de conducir y la tarjeta de identificación de un empleado. Entre los ejemplos de credenciales digitales figuran los nombres de usuario, las tarjetas inteligentes y los certificados digitales.

Gestión de la identidad: procesos, funciones y capacidades de reunir, verificar e interrelacionar información de identidad acerca de un sujeto y comunicarla a una parte receptora a fin de que esta pueda comprobar que la información de identidad recibida corresponde al sujeto concreto de que se trate.

Identidad: información acerca de un sujeto concreto en forma de uno o más atributos que permiten que el sujeto sea debidamente diferenciado en un contexto particular. Es el conjunto de los atributos de una persona que permiten distinguirla de las demás en un contexto determinado.

Identificación: proceso de reunión, verificación y validación de información de atributos adecuada acerca de un sujeto concreto para definir y confirmar su identidad en un contexto específico. (Sinónimos: registro; comprobación de identidad)

Parte receptora: la persona física o entidad jurídica que se basa en la credencial de identidad o la aseveración de identidad para decidir las medidas que deberá tomar en un contexto de aplicación determinado, por ejemplo, procesar una transacción o autorizar el acceso a información o a un sistema. (Sinónimo: proveedor de servicios)

Proveedor de atributos: entidad que actúa como fuente autorizada de uno o más atributos de la identidad de un sujeto y tiene a su cargo los procesos relacionados con la reunión y mantenimiento de los datos sobre esos atributos. Un proveedor de atributos corrobora la fiabilidad y validez de las aseveraciones sobre los atributos, en respuesta a solicitudes de información sobre esos atributos formulados por los proveedores de la identidad y las partes receptoras. Como ejemplos de proveedores de atributos cabe citar el registro oficial de títulos de propiedad, una agencia nacional de información sobre solvencia crediticia o una base de datos comercial de marketing.

Proveedor de identidad: entidad encargada de la 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. (Sinónimos: proveedor de servicios de credenciales; autoridad de certificación; proveedor de atributos (cuando se suministran datos limitados sobre atributos))

Reglas de funcionamiento: procesos comerciales, especificaciones técnicas y normas jurídicas definidas por contrato que rigen el funcionamiento de un sistema de identidad concreto. Suelen ser elaboradas a nivel privado (por ejemplo, por el operador del sistema de identidad) y en virtud del contrato adquieren carácter vinculante y fuerza legal para los participantes. (Sinónimos: marco de confianza; normas del sistema; reglas comunes de funcionamiento; reglamentos de funcionamiento)

Sistema de identidad: entorno en línea utilizado para la gestión de la identidad digital que se rige por un conjunto de reglas de funcionamiento y en el que puede haber confianza recíproca entre individuos, organizaciones, servicios y dispositivos dado que fuentes autorizadas han establecido y autenticado sus identidades respectivas.

Sistema de identidad federado: sistema de identidad en el que un sujeto puede utilizar una credencial de identidad expedida por cualquiera de los distintos proveedores de identidad a efectos de autenticación en sistemas diferentes ante múltiples partes receptoras no relacionadas entre sí.

Sujeto: la persona física, entidad jurídica, dispositivo u objeto digital que es objeto de identificación en una credencial concreta y cuyos datos el proveedor de la identidad puede autenticar y certificar. (Sinónimo: sujeto de datos; usuario)