



Asamblea General

Distr. limitada
30 de enero de 2017
Español
Original: francés/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

Labor en el ámbito del comercio electrónico: cuestiones jurídicas relacionadas con la gestión de la identidad electrónica y los servicios de confianza

**Propuesta presentada por Austria, Bélgica, Francia, Italia,
el Reino Unido y la Unión Europea**

Nota de la Secretaría

Los Gobiernos de Bélgica, Francia, Italia y el Reino Unido, la delegación de Austria y la Unión Europea presentaron a la Secretaría un documento para que se examinara en el 55º período de sesiones del Grupo de Trabajo. En el anexo de la presente nota figura la traducción al español del texto recibido por la Secretaría.



Anexo

Propuesta presentada por Austria, Bélgica, Francia, Italia, el Reino Unido y la Unión Europea

Fecha: 26 de enero de 2017

Propuesta de los Gobiernos de Bélgica, Francia, Italia y el Reino Unido de Gran Bretaña e Irlanda del Norte, la delegación de Austria y la Unión Europea: labor en el ámbito del comercio electrónico: cuestiones jurídicas relacionadas con la gestión de la identidad electrónica y los servicios de confianza

I. Introducción

1. De conformidad con el mandato otorgado por la Comisión en su 44º período de sesiones, celebrado en 2011, el Grupo de Trabajo IV sobre comercio electrónico (en lo sucesivo denominado Grupo de Trabajo IV) comenzó a ocuparse del tema de los documentos transmisibles electrónicos¹. Durante el 49º período de sesiones de la Comisión, el Grupo de Trabajo IV informó sobre la labor realizada en sus períodos de sesiones 52º y 53º. La preparación de las disposiciones del proyecto de ley modelo sobre los documentos transmisibles electrónicos está llegando a su fin.

2. En 2011, durante su 44º período de sesiones, la Comisión también observó que se había manifestado cierto apoyo a la idea de abordar la problemática jurídica relativa a la gestión de los datos identificadores como posible tema comprendido en el mandato del Grupo de Trabajo IV². En su 48º período de sesiones, celebrado en 2015, la Comisión encargó a la Secretaría que realizara una labor preparatoria sobre la gestión de la identidad y los servicios de confianza, la computación en la nube y el comercio móvil, incluso mediante la organización de coloquios y reuniones de grupos de expertos, para que el Grupo de Trabajo examinara esas cuestiones en un futuro, una vez finalizada la labor que estaba realizando en relación con los documentos transmisibles electrónicos. La Comisión también pidió a la Secretaría que comunicara los resultados de esa labor preparatoria al Grupo de Trabajo IV, con miras a que este formulara recomendaciones acerca del alcance exacto, la metodología posible y las prioridades, a fin de que la Comisión las examinara en su 49º período de sesiones³.

3. En respuesta a esa solicitud, la Secretaría presentó a la Comisión, en su 49º período de sesiones, una nota sobre los aspectos jurídicos relacionados con la gestión de la identidad y los servicios de confianza, en la que figuraba un resumen de las deliberaciones celebradas durante el coloquio y en otras reuniones pertinentes sobre el tema⁴.

4. En su 49º período de sesiones, celebrado en 2016, la Comisión reafirmó el mandato conferido al Grupo de Trabajo IV de que finalizara el proyecto de ley modelo sobre los documentos transmisibles electrónicos y la nota explicativa correspondiente

¹ Informe de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, 44º período de sesiones (27 de junio a 8 de julio de 2011), A/66/17, párr. 238.

² *Ibid.*, párr. 236.

³ Informe de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre la labor realizada en su 48º período de sesiones (2015), documento A/70/17 de las Naciones Unidas, párr. 358.

⁴ Documento A/CN.9/891.

y, una vez concluida la labor relativa al proyecto de ley modelo, examinara los temas de la gestión de la identidad y los servicios de confianza, así como la computación en la nube⁵.

5. En consonancia con la reafirmación de ese mandato, durante el 54º período de sesiones del Grupo de Trabajo IV se finalizó el proyecto de ley modelo sobre los documentos transmisibles electrónicos y se inició la labor relativa a la gestión de la identidad y los servicios de confianza. Tras un debate fructífero sobre este último tema⁶, el Grupo de Trabajo IV decidió que el siguiente período de sesiones se dedicara en particular a aclarar los objetivos del proyecto sobre la gestión de la identidad y los servicios de confianza, precisar su ámbito de aplicación, determinar los principios generales aplicables, enumerar los conceptos que habría que definir y preparar un primer proyecto de definición de estos últimos⁷.

6. En este contexto, el objetivo de la presente propuesta es aportar al Grupo de Trabajo IV una contribución sobre los elementos mencionados en el párrafo anterior que sirva de base para las deliberaciones del 55º período de sesiones de este Grupo, manteniendo al mismo tiempo una actitud abierta frente a cualquier otra propuesta que tenga por objeto coadyuvar a los debates.

II. Contexto, alcance y objetivos del proyecto

7. La labor propuesta en el ámbito de la gestión de la identidad y los servicios de confianza está directamente relacionada con la labor que el Grupo de Trabajo IV: 1) llevó a cabo con anterioridad (en particular con respecto a la Ley Modelo sobre Comercio Electrónico, la Ley Modelo sobre las Firmas Electrónicas y la Convención sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales); 2) está realizando actualmente (en relación con los documentos transmisibles electrónicos), y 3) prevé realizar en el futuro, sobre otros temas que se han examinado, como la computación en la nube o los pagos mediante dispositivos móviles.

8. En los hechos, la gestión de la identidad es un requisito fundamental en el que se sustenta la mayor parte de la labor que ha llevado a cabo o está en vías de realizar el Grupo de Trabajo IV. Además, el cumplimiento de muchos de los requisitos aplicables al comercio electrónico que están previstos en los textos de la CNUDMI puede facilitarse mediante la utilización de uno o más servicios de confianza ofrecidos por los proveedores de esos servicios. Un “servicio de confianza” puede consistir en la creación de una firma electrónica, la aplicación de un precinto electrónico para garantizar el origen y la integridad de un documento, el uso de un sello electrónico de fecha y hora para darle fecha cierta a un documento, la transmisión segura de un documento entre las partes (servicio electrónico de envío certificado) o la autenticación de sitios web.

9. Una gestión de la identidad que sea fiable, así como el uso de servicios de confianza fiables, se han convertido en requisitos esenciales de las actividades de comercio electrónico debido a la importancia y la sensibilidad cada vez mayores de las operaciones en línea.

⁵ Informe de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre la labor realizada en su 49º período de sesiones (2016), documento A/71/17 de las Naciones Unidas, párr. 353.

⁶ Informe del Grupo de Trabajo IV (Comercio Electrónico) sobre la labor realizada en su 54º período de sesiones (16 de noviembre 2016), A/CN.9/897, párrs. 107 a 123.

⁷ *Ibid.*, párr. 120.

10. En muchas de las operaciones electrónicas que se realizan por Internet, es necesario verificar la identidad del depositario de un sitio web para comprobar que el sitio web le pertenece al sujeto de derecho que afirma estar a cargo de su funcionamiento y es efectivamente administrado por esa persona. Del mismo modo, en muchos casos es importante que las partes se identifiquen al comienzo de las negociaciones. Además, a los efectos de la firma electrónica del acuerdo definitivo también puede ser necesario identificar a los diversos firmantes, verificar que han expresado su consentimiento respecto de un contenido que mantendrá su integridad, y estampar la fecha y hora en el documento para dotarlo de fecha cierta. Por último, en algunos casos es importante que los documentos se transmitan a la otra parte a través de un canal seguro que garantice la fecha de envío y recepción del documento.

11. Los servicios de autenticación de la identidad y de confianza contribuyen de manera considerable al surgimiento de un entorno comercial sin papel, ya que las actividades cotidianas de las administraciones públicas y las empresas pueden realizarse con mayor rapidez y eficacia y a un costo menor. En este contexto, muchas entidades, tanto del sector público como del privado, diseñan (o querían diseñar) modelos económicos que ofrezcan o utilicen el sistema de gestión de la identidad y los servicios de confianza.

12. Hoy en día las reflexiones e iniciativas nacionales y regionales en el ámbito de la gestión de la identidad y los servicios de confianza son numerosas y ya han alcanzado la madurez. Si bien a veces adoptan enfoques divergentes, permiten determinar cuáles son las cuestiones pertinentes y pueden arrojar luz sobre el debate relativo a la creación de marcos jurídicos apropiados en el plano internacional que puedan aplicarse en los distintos ordenamientos jurídicos existentes.

13. La labor relativa a la gestión de la identidad y los servicios de confianza tiene diversos objetivos, a saber:

- Facilitar el desarrollo del derecho mercantil internacional y responder a la necesidad de dar a los agentes económicos instrumentos que les permitan garantizar la seguridad jurídica de sus operaciones electrónicas.
- Contribuir a la armonización de los aspectos jurídicos que surjan de los proyectos de diversos grupos nacionales e internacionales que actualmente tratan estos temas de manera aislada. El objetivo sería proporcionar un marco jurídico general aplicable tanto a los servicios de gestión de la identidad como a los servicios de confianza, con disposiciones adecuadas que faciliten la interoperabilidad jurídica y técnica transfronteriza a nivel internacional.
- Contribuir a que las administraciones públicas y las empresas, que no son siempre conscientes de las cuestiones jurídicas en juego, se familiaricen con el comercio electrónico y sus operaciones a fin de que aumente la confianza en ellos.
- Completar los documentos ya elaborados por la CNUDMI, ofreciendo soluciones pragmáticas con ese fin. Más concretamente, el objetivo sería redactar disposiciones legislativas que permitan cumplir de manera “práctica y concreta” los requisitos “abstractos” establecidos en esos textos de la CNUDMI. La existencia de normas jurídicas claras beneficiaría a las empresas, al permitirles mejorar la gestión de sus riesgos en el ámbito del comercio electrónico internacional y garantizar la seguridad jurídica de sus operaciones de manera sencilla y eficaz.

14. Dada la estrecha interacción que existe entre los dos temas, la labor debería centrarse desde el principio tanto en la gestión de la identidad como en los servicios de confianza. La determinación del alcance de la labor y la definición de los conceptos

deberían por tanto abarcar estos dos temas indisociables. Este enfoque no impide que posteriormente se trabaje sobre estos temas de manera secuencial.

III. Determinación de los principios generales aplicables y posibles orientaciones

15. Los principios generales reconocidos tradicionalmente por la CNUDMI deberían orientar la labor relativa a la gestión de la identidad y los servicios de confianza. Cabe mencionar en particular los siguientes:

- El principio de la autonomía de las partes. La utilización de los instrumentos previstos debe seguir siendo facultativa y respetar plenamente la autonomía de las partes en una operación. Las partes también deben tener la posibilidad de elegir libremente el nivel de fiabilidad que habrán de utilizar. Los proveedores deben ser libres de ofrecer uno o más servicios de gestión de la identidad y de confianza y de proponer al respecto uno o más niveles de fiabilidad. En síntesis, el conjunto de normas jurídicas previstas debe considerarse una “caja de herramientas jurídicas” que se pone a disposición de los agentes del mercado.
- El principio de la neutralidad tanto tecnológica como respecto de los modelos económicos. La formulación de normas jurídicas no debe en modo alguno limitar la innovación ni las oportunidades comerciales mediante la introducción de reglas estrictas que favorezcan una solución técnica o un modelo económico en detrimento de otros.
- El principio de no discriminación. Los efectos jurídicos y la admisibilidad como prueba en la esfera judicial de un servicio de identificación electrónica o un servicio de confianza no deben negarse por el mero hecho de que el servicio se preste en forma electrónica o no cumpla los requisitos relativos al nivel de fiabilidad.
- El principio de la equivalencia funcional, según el cual las funciones jurídicas deben ser equivalentes, tanto en el entorno físico como en el entorno electrónico.

16. Las cuestiones que deberían abordarse al redactar las normas jurídicas, tanto respecto de la gestión de la identidad como de los servicios de confianza, son las siguientes:

a) Definición de distintos niveles de fiabilidad sobre la base de criterios objetivos: La fiabilidad de la gestión de la identidad y de los servicios de confianza es con frecuencia un elemento crucial. En algunos casos puede ser fundamental definir y medir la fiabilidad. ¿Qué es la fiabilidad de un servicio o sistema de gestión de la identidad o de un servicio de confianza? La falta de elementos objetivos que permitan juzgar la calidad y la fiabilidad reales de un servicio puede constituir un grave problema para las partes interesadas, especialmente en el marco de su política de gestión de los riesgos. Un modelo flexible que permita establecer distintos niveles de exigencia aplicables a los servicios de gestión de la identidad y de confianza y a sus proveedores es una vía respetuosa de la diversidad de los sistemas en todo el mundo.

b) Atribución de efectos jurídicos diferentes en función del nivel de fiabilidad: Deberían definirse los efectos jurídicos de la identificación y la autenticación electrónicas y de varios servicios de confianza. El objetivo es determinar los efectos jurídicos que se atribuyen a la identificación electrónica y a los servicios de confianza en función de cada uno de los niveles de fiabilidad definidos. Las partes interesadas podrían así gestionar eficazmente sus riesgos jurídicos al optar por el nivel de fiabilidad y los efectos jurídicos más acordes con sus necesidades. A la hora de definir esos distintos efectos jurídicos, se podría en particular tener en cuenta, si fuese

oportuno, el principio de no discriminación, el principio de asimilación, el principio de reconocimiento mutuo, determinadas presunciones y/o mecanismos de inversión de la carga de la prueba. Cuanto mayor sea el nivel de fiabilidad, más favorables serán los efectos jurídicos para el usuario del servicio.

c) Determinación del régimen de responsabilidad según el nivel de fiabilidad:
Se debe definir el régimen de responsabilidad de los proveedores de sistemas de identificación electrónica y servicios de confianza a fin de aportar a los agentes la claridad y la previsibilidad necesarias. Este régimen variaría de acuerdo con el nivel de fiabilidad ofrecido por cada proveedor.

17. En lo que respecta a los servicios de gestión de la identidad, deberían tenerse en cuenta las siguientes orientaciones:

- En virtud de la aplicación del principio de la autonomía de las partes, cada proveedor de un servicio en línea puede optar por exigir o no la identificación y la autenticación electrónicas para que se pueda acceder a su servicio y es libre de elegir el nivel de fiabilidad que eventualmente pudiera requerirse.
- Aplicación del principio de reconocimiento mutuo transfronterizo de los medios de identificación electrónica que sean de un nivel igual o superior al exigido para acceder al servicio en línea. Este principio se fundaría en la definición de los diferentes niveles de fiabilidad de los medios de identificación electrónica. Cada nivel se determinaría de acuerdo con criterios objetivos armonizados.
- A fin de determinar los sistemas de gestión de la identidad que se tendrán en cuenta en nuestra labor, es más importante saber cuál es la finalidad o el propósito de la utilización del medio de identificación electrónico (es decir, si el medio se va a utilizar — total o parcialmente — para operaciones comerciales o no), que averiguar quién es el proveedor del medio de identificación electrónica (si es el sector público, el privado, o ambos). Dado que la utilización puede tener una finalidad comercial, todos los medios de identificación electrónica - incluso los suministrados total o parcialmente por el sector público - deberían examinarse como parte de nuestra labor.
- Nuestra labor debería centrarse, como cuestión de prioridad, en la identificación de las personas físicas y jurídicas, dejando de lado en una primera etapa la cuestión de la identificación de los objetos materiales (por ejemplo, servidores, teléfonos inteligentes, terminales, etc.) o digitales (por ejemplo, programas informáticos). Puesto que se trata de formular normas jurídicas, se debe dar prioridad a la identificación del sujeto de derecho (persona física o jurídica) que **es titular de derechos y obligaciones y asume la responsabilidad** (por ejemplo, el propietario de un sitio web, el **titular de derechos de autor o el propietario de un servidor**). Los objetos materiales o digitales están siempre vinculados a una persona física o jurídica. La identificación de los objetos es, en esencia, una cuestión de carácter técnico y de seguridad, más que jurídica.
- Los medios de identificación electrónica de mayor nivel de fiabilidad deberían por lo menos estar vinculados a datos de identificación personal emitidos o administrados por una **f fuente fidedigna**.
- En el caso de los niveles de fiabilidad superiores, se debería establecer la obligación del proveedor de un medio de identificación electrónica de notificar todo quebrantamiento de la seguridad de su sistema y, si fuera necesario, suspender el funcionamiento de este. El proveedor debería efectuar esa notificación de conformidad con lo dispuesto en la legislación nacional y, en vista del contexto transfronterizo, la información debería ponerse a disposición del público.

- Se podría establecer la presunción de que se han respetado los criterios objetivos que definen los niveles de fiabilidad y se han cumplido los requisitos legales si el proveedor se ajusta a las normas técnicas determinadas por una autoridad internacional.

18. En el marco de la determinación de los niveles de garantía vinculados a la gestión de la identidad, se podrían fijar tres niveles: a) un nivel de garantía bajo; b) un nivel de garantía suficiente, y c) un nivel de garantía alto.

- Los niveles de garantía se describirían de acuerdo con especificaciones técnicas, normas y procedimientos conexos.
- Se podría prever un mecanismo de cooperación y un marco de interoperabilidad para definir los criterios en que se basarían los niveles de garantía, así como para intercambiar la información relativa a los medios de identificación electrónica y sus respectivos niveles de garantía.
- Se consagraría el principio de reconocimiento mutuo transfronterizo para los medios de identificación que tuvieran un nivel de garantía equivalente (a partir del nivel de garantía suficiente) o superior.

19. En relación con los servicios de confianza, deberían tenerse en cuenta las siguientes orientaciones:

- En el marco de la definición y armonización de los niveles de fiabilidad de los servicios de confianza, se fijarían por lo menos dos niveles:
 1. servicios de confianza no calificados;
 2. servicios de confianza calificados.
- Los efectos jurídicos variarían según el nivel de fiabilidad del servicio de confianza:
 1. Si el servicio de confianza no es calificado: los efectos jurídicos se limitarían a la cláusula de no discriminación.
 2. Si el servicio de confianza es calificado: los efectos jurídicos serían favorables y abarcarían la asimilación, la presunción, la inversión de la carga de la prueba.
- Se consagraría el principio de reconocimiento mutuo transfronterizo para los servicios de confianza que tuvieran un nivel de fiabilidad equivalente.
- Se establecería una obligación general de garantizar la seguridad, proporcional al nivel de riesgo, para todos los proveedores (calificados o no).
- Se preverían requisitos específicos para los proveedores calificados de servicios de confianza y para cada servicio de confianza calificado a fin de garantizar un alto nivel de fiabilidad.
- El régimen de responsabilidad de los proveedores de servicios de confianza variaría según si el proveedor es calificado o no.
- Se podría exigir a todos los proveedores (o por lo menos a los calificados) que notificaran cualquier quebrantamiento de la seguridad de sus sistemas y, de ser necesario, que suspendieran el funcionamiento de estos. Los proveedores deberían efectuar esa notificación de conformidad con lo dispuesto en la legislación nacional y, en vista del contexto transfronterizo, la información debería ponerse a disposición del público.

- Se podría establecer la presunción de que se han respetado los criterios objetivos que definen los niveles de fiabilidad y se han cumplido los requisitos legales si el proveedor se ajusta a las normas técnicas determinadas por una autoridad internacional.

IV. Determinación de los conceptos y propuestas de definición

20. A fin de contribuir a los debates sobre la gestión de la identidad y los servicios de confianza, se propone la siguiente lista (no exhaustiva) de conceptos y definiciones:

- **Identificación electrónica:** proceso mediante el cual se utilizan datos de identificación personal en forma electrónica que distinguen de manera exclusiva a una persona física o jurídica, o a una persona física que representa a una persona jurídica;
- **Medio de identificación electrónica:** elemento material o inmaterial que contiene datos de identificación personal y que se utiliza para autenticar a la persona que desea acceder a un servicio en línea;
- **Datos de identificación personal:** conjunto de datos que permiten determinar la identidad de una persona física o jurídica, o de una persona física que represente a una persona jurídica;
- **Sistema de identificación electrónica:** sistema de identificación electrónica mediante el cual se proporcionan medios de identificación electrónica a personas físicas o jurídicas, o a personas físicas que representen a personas jurídicas;
- **Autenticación:** proceso electrónico que permite confirmar la identificación electrónica de una persona física o jurídica, o el origen y la integridad de un dato existente en forma electrónica;
- **Fuente fidedigna:** cualquier fuente que, independientemente de su forma, sea fiable para obtener datos, información u otros elementos de identificación exactos que puedan utilizarse para demostrar la identidad;
- **Servicio de confianza:** servicio electrónico (normalmente prestado a cambio de una remuneración), que consiste:
 1. en la creación, la verificación y la validación de firmas electrónicas, precintos electrónicos o sellos electrónicos de fecha y hora, servicios electrónicos de envío certificado y certificados relacionados con esos servicios; o
 2. en la creación, la verificación y la validación de certificados para la autenticación de sitios web; o
 3. en la conservación de firmas electrónicas, precintos o sellos electrónicos o certificados relacionados con esos servicios;
- **Servicio de confianza calificado:** servicio de confianza que cumple los requisitos establecidos en el presente texto [convención, ley modelo];
- **Firma electrónica:** datos en forma electrónica adjuntados o asociados lógicamente a otros datos en forma electrónica, que el firmante utiliza para firmar;
- **Firmante:** persona física que crea una firma electrónica;

- ***Precinto electrónico***: datos en forma electrónica que se adjuntan o se asocian lógicamente a otros datos en forma electrónica para garantizar el origen y la integridad de estos últimos;
- ***Sello electrónico de fecha y hora***: datos en forma electrónica que vinculan otros datos en forma electrónica a un determinado momento y constituyen prueba de que estos últimos datos existían en ese momento;
- ***Servicio electrónico de envío certificado***: servicio que permite transmitir datos entre terceros por vía electrónica y aporta pruebas sobre el tratamiento de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente al riesgo de pérdida, hurto, alteración o cualquier modificación no autorizada;
- ***Certificado de autenticación de sitios web***: certificado que permite autenticar un sitio web y vincularlo a la persona física o jurídica a quien se ha entregado el certificado;
- ***Documento electrónico***: cualquier contenido almacenado en forma electrónica, en particular un texto o una grabación sonora, visual o audiovisual;
- ***Validación***: proceso de verificación y confirmación de la validez de una firma o un precinto electrónicos;
- ***Usuario***: persona física o jurídica que se fía de una identificación electrónica o de un servicio de confianza.

V. Vínculos con la práctica

A fin de comprender mejor el alcance de la labor, los conceptos y los vínculos con la práctica, se sugiere que durante el o los períodos de sesiones del Grupo de Trabajo IV se presenten ponencias sobre proyectos concretos existentes en distintos países o regiones. Se podría presentar una ponencia sobre las infraestructuras de servicios digitales de identificación electrónica (eID DSI) de Connecting Europe Facility (CEF) y sobre el programa informático eIDAS-Node para mostrar cómo funcionan y cómo los están aplicando los Estados miembros de la Unión Europea.