Naciones Unidas A/CN.9/WG.IV/WP.153

Asamblea General

Distr. limitada
6 de septiembre de 2018
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
Grupo de Trabajo IV (Comercio Electrónico)
57º período de sesiones
Viena, 19 a 23 de noviembre de 2018

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

Nota de la Secretaría

Índice

V.18-05871 (S) 280918 280918

I. Introducción

1. En la presente nota se exponen determinados aspectos de algunos de los temas que el Grupo de Trabajo consideró pertinentes para su examen de las cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza (A/CN.9/936, párr. 58) a fin de facilitar la continuación de los debates. El propósito de esta nota es, en particular, poner de relieve las cuestiones fundamentales que se plantean y sugerir posibles soluciones, sin restringir la posibilidad de que se analicen otros temas o de que algunos temas se examinen en forma conjunta, según proceda. En el documento A/CN.9/WG.IV/WP.154 se describen algunos aspectos de otros temas que el Grupo de Trabajo señaló como pertinentes para su examen de las cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza.

2. En el documento A/CN.9/WG.IV/WP.152, párrafos 6 a 17, se proporciona información sobre los antecedentes de la labor del Grupo de Trabajo en lo que respecta a las cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza. En el documento A/CN.9/WG.IV/WP.152, párrafo 18, figura una lista de otros documentos pertinentes.

II. Cuestiones de interés para la labor futura sobre los aspectos jurídicos de la gestión de la identidad y los servicios de confianza

A. Alcance de la labor

3. La Comisión solicitó al Grupo de Trabajo, en atención a lo recomendado por este, que se ocupara de estudiar las cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza con miras a preparar un texto que facilitara el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza. La solicitud de la Comisión se formuló en términos suficientemente amplios como para abarcar otros aspectos del régimen jurídico de la gestión de la identidad y los servicios de confianza, además de los ya señalados (véase el párr. 1 *supra*).

4. Los mecanismos jurídicos de reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza son un elemento fundamental de un marco jurídico propicio para la economía digital; la falta de esos mecanismos puede contribuir a ampliar aún más la brecha digital. En vista de ello, el Grupo de Trabajo tal vez desee estudiar las consecuencias que podría tener su labor a un nivel más amplio, en lo que respecta a reducir la brecha digital.

5. En ese contexto, el Grupo de Trabajo podría quizás analizar si la falta de un marco jurídico nacional que haga posible utilizar sistemas de gestión de la identidad y servicios de confianza puede ser un obstáculo para el reconocimiento jurídico transfronterizo de esos sistemas y servicios. En ese caso, el Grupo de Trabajo tal vez desee determinar las disposiciones legales que deberían incorporarse al derecho interno para hacer plenamente posible el reconocimiento jurídico transfronterizo de la gestión de la identidad y los servicios de confianza, y deliberar sobre el tipo de texto jurídico (por ejemplo, un tratado, una ley modelo, o ambos) más apropiado para lograr ese objetivo.

6. Además, el reconocimiento jurídico de la identidad a través de fronteras tiene elementos en común con el reconocimiento jurídico de la identidad entre distintos sistemas de gestión de la identidad, independientemente de los elementos extranjeros. Por lo tanto, el Grupo de Trabajo quizás desee plantearse si debería examinar un mecanismo que permita el reconocimiento jurídico entre distintos sistemas de gestión de la identidad, teniendo en cuenta, cuando proceda, los elementos extranjeros. En ese caso, el resultado de la labor del Grupo de Trabajo podría servir de orientación en materia de gestión de la identidad, tanto a nivel nacional como internacional.

1. Identidad básica e identidad adquirida

7. El Grupo de Trabajo tal vez recuerde que se sugirió hacer una distinción entre determinación primaria y secundaria de la identidad (A/CN.9/WG.IV/WP.149, párr. 29).

8. La determinación primaria de la identidad, o identidad básica, se refiere a la atribución de identidad en el contexto y en el momento en que se origina esa identidad. En tal sentido, la identidad básica es normalmente única e irreemplazable. Algunos ejemplos de determinación primaria de la identidad son: la inscripción de una persona física en el registro civil o de estadísticas vitales de un Estado; la inscripción de una persona jurídica en un registro llevado a tal efecto por el organismo competente, por ejemplo, un registro de sociedades comerciales; y la atribución a un objeto digital de un identificador de objetos digitales.

9. La determinación secundaria de la identidad, o identidad adquirida, se refiere a la utilización de la identidad para cumplir una función específica (por ejemplo, celebrar un contrato; extraer dinero de un cajero automático; expedir un certificado por un organismo público).

10. Si bien es posible que la identidad básica no se utilice comúnmente como tal en las operaciones comerciales, los proveedores de identidad pueden utilizarla para establecer la identidad adquirida. Por ejemplo, las normas de la CNUDMI sobre firmas electrónicas exigen que se identifique al firmante. En algunos casos, la identificación fiable del firmante puede basarse en la utilización de una credencial de identidad y un proceso de autenticación que establece la identidad sobre la base de credenciales de identidad básica. Por lo tanto, el reconocimiento jurídico de la identidad básica a través de fronteras y entre sistemas de gestión de la identidad puede ser útil o incluso necesario.

2. Entidades pertinentes

11. El Grupo de Trabajo sostuvo un debate preliminar sobre los tipos de entidades que resultaban pertinentes para sus deliberaciones (A/CN.9/936, párrs. 63 a 65), es decir, las entidades a las que se aplicaría el resultado de su labor. En general se reconoció que eran pertinentes las personas físicas y jurídicas que se dedicaban al comercio, incluido el comercio transfronterizo. Las entidades sin personalidad jurídica propia, pero que fueran importantes para las actividades comerciales, también podrían tenerse en cuenta. Por ejemplo, los comerciantes que operan en el sector informal de los países menos adelantados pueden utilizar su identidad móvil como medio de identificación principal.

12. La participación de organismos públicos puede justificarse por el interés que revisten para el comercio internacional algunas operaciones entre empresas y el Estado y ciertas operaciones entre Estados, como las ventanillas únicas transfronterizas para actividades aduaneras. El Grupo de Trabajo tal vez desee analizar si la participación de organismos públicos en operaciones de gestión de la identidad o en servicios de confianza plantea problemas específicos, teniendo en cuenta especialmente la aplicación de los principios de neutralidad tecnológica (véanse los párrs. 38 a 40 *infra*), autonomía de las partes (véanse los párrs. 41 a 47 *infra*) y proporcionalidad entre los medios de identificación electrónica y la función para la que se utilizan (véase el párr. 46 *infra*).

13. Se han expresado distintas opiniones en cuanto a si la identificación de los objetos físicos y digitales está comprendida en el ámbito de esta labor. Según una opinión, los objetos físicos y digitales deberían quedar excluidos porque no tienen personalidad jurídica y no se les puede atribuir responsabilidad de manera autónoma. Sin embargo, también se ha expresado la opinión de que, a los efectos de la identificación, no es necesario que el objeto identificado tenga personalidad jurídica autónoma ni que se le pueda hacer incurrir en responsabilidad (A/CN.9/936, párr. 64).

14. Según otra opinión, la identificación de los objetos podría estudiarse después de que el Grupo de Trabajo haya examinado la identificación de las personas (A/CN.9/936, párr. 65). Al respecto cabe señalar que los objetos son una fuente importante de macrodatos conforme al modelo “Internet de las cosas”, y que la atribución de datos de manera fiable puede revestir especial interés en ese modelo. Por ejemplo, se hace un uso cada vez mayor de dispositivos médicos para vigilar a distancia el estado de un

paciente durante sus actividades diarias. Es fundamental que la información generada por esos dispositivos se atribuya al paciente correcto. De manera similar, la vigilancia de los medicamentos no debe referirse únicamente al momento de su utilización, sino a todo su ciclo de producción, para que los medicamentos estén correctamente identificados y se pueda garantizar su origen y contenido. También es fundamental que los medicamentos y sus componentes se identifiquen de manera fiable.

B. Definiciones

15. El Grupo de Trabajo tal vez desee remitirse al documento A/CN.9/WG.IV/WP.150, en el que figura una lista de términos y conceptos relacionados con la gestión de la identidad y los servicios de confianza que podría ser de utilidad para sus deliberaciones. Esa lista no impide que el Grupo de Trabajo delibere sobre las definiciones de los términos pertinentes a medida que avance en su labor.

16. Con respecto a la gestión de la identidad, las siguientes definiciones que figuran en el documento A/CN.9/WG.IV/WP.150 pueden resultar particularmente útiles para las deliberaciones del Grupo de Trabajo sobre las cuestiones que se plantean en la presente nota.

17. Por “identidad” se entiende: a) la información acerca de un sujeto concreto expresada en forma de uno o más atributos que permiten distinguir suficientemente a ese sujeto en un contexto en particular; b) un conjunto de atributos relativos a una persona que la describen de manera inequívoca en un contexto determinado (A/CN.9/WG.IV/WP.150, párr. 31).

18. El Grupo de Trabajo quizás desee analizar la relación existente entre esas definiciones y los conceptos de identidad básica e identidad adquirida (véanse los párrs. 7 a 10 *supra*), así como la pertinencia de esos conceptos para su labor futura. Al respecto, el Grupo de Trabajo tal vez desee aclarar si el carácter inequívoco es un atributo de la identidad básica.

19. Por “gestión de la identidad” se entiende un conjunto de procesos que permiten gestionar la identificación, autenticación y autorización de personas físicas, personas jurídicas, dispositivos u otros sujetos en un contexto en línea (A/CN.9/WG.IV/WP.150, párr. 35).

20. Por “sistema de identidad” se entiende un entorno en línea utilizado para operaciones de gestión de la identidad que se rigen por un conjunto de normas del sistema (también conocido como marco de confianza) y en el que puede haber confianza recíproca entre individuos, organizaciones, servicios y dispositivos debido a que sus respectivas identidades han sido establecidas y autenticadas por fuentes autorizadas (A/CN.9/WG.IV/WP.150, párr. 38).

21. Por “operación de identidad” se entiende cualquier operación en la que intervengan dos o más participantes y que implique establecer, verificar, emitir, aseverar, revocar o comunicar información de identidad o fiarse de ella (A/CN.9/WG.IV/WP.150, párr. 39).

22. El Grupo de Trabajo tal vez desee remitirse a los conceptos de “gestión de la identidad”, “sistema de identidad” y “operaciones de identidad” a fin de aclarar si su labor sobre el reconocimiento jurídico de la gestión de la identidad debería referirse a los sistemas de identidad, a las operaciones de identidad o a ambas cosas (véanse los párrs. 57 a 59 *infra*).

23. Por “nivel de seguridad” se entiende una designación del grado de confianza en los procesos de identificación y autenticación, es decir: a) el grado de confianza en el proceso de análisis utilizado para establecer la identidad de una entidad a la que se ha emitido una credencial, y b) el grado de confianza en que la entidad que utiliza la credencial es la entidad a la que se ha emitido esa credencial. La seguridad refleja la fiabilidad de los métodos, procesos y tecnologías empleados (A/CN.9/WG.IV/WP.150, párr. 42).

24. El Grupo de Trabajo tal vez desee remitirse a la definición de “nivel de seguridad” cuando examine ese tema (véase A/CN.9/WG.IV/WP.154, párrs. 10 a 19). Al hacerlo, el Grupo de Trabajo podría tener en cuenta también la siguiente definición de “nivel de seguridad”: “nivel de confianza en la vinculación entre una entidad y la información de identidad presentada” (A/CN.9/WG.IV/WP.150, párr. 12), así como la nota relativa a esa definición en la que se explica que los conceptos de “garantía de identidad” y “garantía de autenticación” pueden considerarse componentes independientes del concepto general de “nivel de seguridad”.

C. Principios generales

25. El Grupo de Trabajo determinó que los siguientes principios generales eran pertinentes para su labor sobre los aspectos jurídicos de la gestión de la identidad y los servicios de confianza: no discriminación contra el uso de medios electrónicos, equivalencia funcional, neutralidad tecnológica y autonomía de las partes (A/CN.9/936, párr. 67).

1. No discriminación contra el uso de medios electrónicos

26. El principio de no discriminación contra el uso de medios electrónicos está firmemente establecido en los textos de la CNUDMI. En el contexto de la gestión de la identidad y los servicios de confianza, ese principio podría formularse por ejemplo de la siguiente manera[1]:

> No se negarán efectos jurídicos, validez ni fuerza ejecutoria a la verificación de la identidad mediante el uso de [credenciales] [sistemas de gestión] de identidad y servicios de confianza por la sola razón de que [esas credenciales] [esos sistemas de gestión] de identidad estén en forma electrónica.

27. La disposición propuesta permite elegir entre “credenciales de identidad” y “sistemas de gestión de la identidad”, y la elección dependerá de si se decide hacer referencia a la utilización de credenciales para la identificación o al uso de todo el sistema de gestión de la identidad (véanse los párrs. 57 a 59 *infra*).

2. Equivalencia funcional

28. En el ámbito del comercio electrónico, el principio de equivalencia funcional establece los requisitos que debe reunir un documento, método o proceso electrónico para cumplir las mismas funciones que el concepto análogo basado en papel.

a) Gestión de la identidad

29. Una posible norma de equivalencia funcional aplicable a la gestión de la identidad podría formularse de la siguiente manera:

> Cuando la ley requiera o permita la identificación de una entidad, ese requisito se dará por cumplido con respecto a la gestión de la identidad [electrónica] [digital] si se utiliza un método fiable para [verificar los atributos [pertinentes] de la entidad].

30. El efecto que debería tener una disposición sobre equivalencia funcional aplicable a la identificación sería trasladar a un entorno electrónico los requisitos de identificación aplicables a la identificación basada en el papel. El Grupo de Trabajo tal vez desee considerar la posibilidad de insertar la palabra “[pertinentes]” a fin de indicar que, para que la identificación en línea se lleve a cabo con éxito, solo se requerirían los atributos que se solicitan para la identificación fuera de línea. El Grupo de Trabajo quizás desee también aclarar si debería hacerse referencia a la “identidad electrónica” o a la “identidad digital”.

[1] Las disposiciones propuestas se incluyen únicamente con fines ilustrativos, sin perjuicio de las recomendaciones que el Grupo de Trabajo formule a la Comisión sobre la posible forma de su labor y de las decisiones que adopte la Comisión al respecto.

31. Se podría proporcionar más orientación sobre los elementos pertinentes para determinar la fiabilidad del método, entre ellos: a) acuerdos contractuales, si están permitidos con arreglo a la ley aplicable; b) certificación por terceros y autocertificación; y c) referencia a niveles de seguridad. En particular, cuando en una disposición sobre equivalencia funcional se prevea el uso de un "método fiable" puede ser necesario utilizar un método que ofrezca un grado de fiabilidad equivalente respecto de la identificación en línea y fuera de línea.

32. Al examinar una posible norma de equivalencia funcional aplicable a la gestión de la identidad podría ser útil mencionar los casos en que se utiliza esa gestión. Al respecto cabe señalar que la identificación puede exigirse para distintos fines o funciones. Uno de ellos es el cumplimiento de la normativa. Otros ejemplos se dan en el caso de la aplicación de las normas relativas al "conocimiento del cliente" en el sector financiero, el sector de las telecomunicaciones y otros sectores empresariales, así como en la esfera de la contratación electrónica, en que es necesario identificar correctamente a los posibles proveedores y clientes para prevenir el fraude y la colusión y obtener la inhabilitación.

33. Otro fin que puede tener la identificación es determinar la validez de un documento comercial. Por ejemplo, la ley aplicable a un conocimiento de embarque puede exigir la identificación de algunas de las partes. Así lo exigen el artículo 15 del Convenio de las Naciones Unidas sobre el Transporte Marítimo de Mercancías (Hamburgo, 1978) (las "Reglas de Hamburgo")[2] y el artículo 36 del Convenio de las Naciones Unidas sobre el Contrato de Transporte Internacional de Mercancías Total o Parcialmente Marítimo (Nueva York, 2008) (las "Reglas de Rotterdam")[3].

34. Además, las partes que celebren una operación en línea pueden convenir en utilizar determinados procedimientos y métodos para identificarse mutuamente con exactitud para fines de gestión de riesgos, aunque no tengan la obligación legal de hacerlo. Esa obligación de identificarse es de origen contractual.

35. Como cuestión de política, se podría tomar la decisión de adoptar normas de identificación más rigurosas para lograr un cumplimiento más estricto de las obligaciones de identificación en los casos en que la identificación fuera de línea, a pesar de utilizarse, no sea plenamente satisfactoria. El Grupo de Trabajo tal vez desee estudiar la interacción entre la adopción de una norma de equivalencia funcional sobre la identificación y la posible introducción de requisitos para la identificación en línea que sean más estrictos que los aplicables a la identificación fuera de línea.

b) Servicios de confianza

36. En algunos textos de la CNUDMI se establecen normas de equivalencia funcional para determinados servicios de confianza, a saber, respecto de las firmas electrónicas, en el artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico ("LMCE")[4], el artículo 6 de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas ("LMFE")[5], el artículo 9, párrafo 3, de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (Nueva York, 2005) ("CCE")[6] y el artículo 9 de la Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos[7], y, en lo que respecta a la conservación y el archivo, en el artículo 10 de la LMCE. El Grupo de Trabajo tal vez desee plantearse si convendría preparar disposiciones especiales sobre el producto de cada tipo de servicio de confianza o si, en cambio, podría o debería redactarse una norma general de equivalencia funcional (véase A/CN.9/WG.IV/WP.154, párr. 58).

---

[2] Naciones Unidas, *Treaty Series*, vol. 1695, núm. 29215, pág. 3.
[3] Resolución 63/122 de la Asamblea General, anexo.
[4] Publicación de las Naciones Unidas, núm. de venta S.99.V.4.
[5] Publicación de las Naciones Unidas, núm. de venta: S.02.V.8.
[6] Naciones Unidas, *Treaty Series*, vol. 2898.
[7] Publicación de las Naciones Unidas, núm. de venta S.17.V.5.

37. El Grupo de Trabajo quizás desee analizar también si sería conveniente preparar una disposición sobre la atribución de la información de identidad, o si bastaría con la norma de equivalencia funcional, ya que la información de identidad se atribuiría a la misma entidad de igual manera que en un entorno fuera de línea y, en cualquier caso, no se atribuiría al proveedor de servicios de identidad. El artículo 13 de la LMCE es un ejemplo de disposición que trata de la atribución.

3. Neutralidad tecnológica

38. El principio de neutralidad tecnológica es una piedra angular de los textos de la CNUDMI y de muchos otros textos legislativos que tratan de la utilización de las comunicaciones electrónicas. En el contexto de la gestión de la identidad y los servicios de confianza, puede ser necesario proporcionar orientación sobre los requisitos mínimos que deben reunir los sistemas, haciendo referencia a las propiedades de los sistemas y no a determinadas tecnologías (A/CN.9/936, párr. 69). En cambio, si se opta por un criterio basado en las operaciones (véanse los párrs. 57 a 59 *infra*), puede ser necesario proporcionar orientación sobre los requisitos mínimos aplicables a las operaciones de identidad, haciendo referencia a las propiedades de las operaciones. En el ámbito de los servicios de confianza, para aplicar el principio de neutralidad tecnológica puede ser necesario definir los objetivos concretos que debe tener cada servicio de confianza, sin imponer la utilización de ninguna tecnología en particular para alcanzar esos objetivos.

39. Una disposición sobre la igualdad de tratamiento que debe darse a todas las tecnologías, métodos y sistemas de gestión de la identidad y servicios de confianza podría formularse de la siguiente manera:

> Nada de lo dispuesto en el presente [proyecto de instrumento] se aplicará de modo que excluya, restrinja o prive de efectos jurídicos a cualquier [tecnología, método o sistema] utilizada con fines de gestión de la identidad o servicios de confianza, que cumpla los requisitos mencionados en el presente [proyecto de instrumento] [, o que cumpla de otro modo los requisitos del derecho aplicable].

40. La frase “o que cumpla de otro modo los requisitos del derecho aplicable”, que figura en el artículo 3 de la LMFE, se refiere a la posibilidad de que otro régimen legal que no sea el proyecto de instrumento exija, en determinados casos, el cumplimiento de requisitos diferentes de los enunciados en el proyecto de instrumento[8].

4. Autonomía de las partes

41. Una de las consecuencias del principio de la autonomía de las partes es que el uso de servicios de identidad y de confianza es opcional. Si bien ese principio puede aplicarse plenamente a los servicios comerciales, su aplicación puede estar restringida, por razones de política, en lo que respecta al acceso a servicios prestados por organismos públicos o a la interacción con esos organismos.

42. Una posible disposición sobre la utilización opcional de los servicios de identidad y de confianza podría formularse de la siguiente manera:

> 1. Nada de lo dispuesto en el presente [proyecto de instrumento] obligará a ninguna entidad a utilizar o aceptar [credenciales de] [sistemas de gestión de la] identidad o servicios de confianza sin su consentimiento.
>
> 2. El consentimiento de una entidad respecto de la utilización de [credenciales de] [sistemas de gestión de la] identidad o servicios de confianza podrá inferirse de su conducta [y de otras circunstancias].
>
> [El párrafo 1 no será aplicable a ...]

[8] *Ley Modelo de la CNUDMI sobre las Firmas Electrónicas con la Guía para su incorporación al derecho interno* (publicación de las Naciones Unidas, núm. de venta S.02.V.8), párr. 107.

43. La disposición propuesta permite elegir entre “credenciales de identidad” y “sistemas de gestión de la identidad”, y la elección dependerá de si se decide hacer referencia a la utilización de credenciales para la identificación o al uso de todo el sistema de gestión de la identidad (véanse los párrs. 57 a 59 *infra*).

44. En el segundo párrafo de la disposición propuesta se insertaron las palabras “[y otras circunstancias]” para contemplar la situación de las entidades que no son capaces de tener una conducta autónoma (por ejemplo, los objetos físicos o digitales). En esos casos, el consentimiento no será atribuible a la entidad, sino a la persona física o jurídica que controle a esa entidad.

45. La aplicación del principio de la autonomía de las partes está sujeta a las limitaciones que emanen de normas jurídicas imperativas (A/CN.9/936, párr. 72). Esas limitaciones son particularmente importantes debido a que los requisitos legislativos que se cumplen mediante el uso de sistemas de gestión de la identidad o servicios de confianza suelen ser obligatorios. En vista de ello, se sugiere formular ese principio sobre la base de lo dispuesto en el artículo 5 de la LMFE:

> Las partes podrán establecer excepciones al presente [proyecto de instrumento] o modificar sus efectos mediante acuerdo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

46. Otra aplicación del principio de la autonomía de las partes se refiere a la libertad de elegir los servicios de identidad y de confianza más apropiados para la función que interesa a las partes (el denominado “principio de proporcionalidad”). La libertad de elección del tipo de servicio también está estrechamente relacionada con el principio de neutralidad tecnológica.

47. El principio de la autonomía de las partes también contribuye a reforzar el cumplimiento de los acuerdos contractuales, como las normas de los sistemas de gestión de la identidad y los marcos y las normas de los sistemas de los servicios de confianza. Por lo tanto, las normas de los sistemas pueden ser especialmente pertinentes en el contexto de los sistemas federados de gestión de la identidad (véase A/CN.9/WG.IV/WP.154, párr. 39). Según la definición provisional de sistema de identidad federado, se entiende por tal “un grupo de proveedores de identidad, partes receptoras, sujetos y otras personas que convienen en actuar con arreglo a las políticas, normas y tecnologías compatibles especificadas en las normas del sistema (o en un marco de confianza) con el fin de que las partes receptoras puedan comprender la información facilitada por los proveedores de identidad sobre la identidad de los sujetos y confiar en ella” (A/CN.9/WG.IV/WP.150, párr. 28).

5. Obligación de identificar

48. Otro principio general común a todos los textos de la CNUDMI sobre comercio electrónico se refiere al hecho de que esos textos no afectan al derecho sustantivo, por ejemplo, el derecho aplicable en general a las operaciones comerciales.

49. En el contexto de la gestión de la identidad y los servicios de confianza, este principio implica que la legislación relativa a la gestión de la identidad no debe introducir ninguna obligación nueva de identificar; que la legislación sobre servicios de confianza no debe introducir ninguna obligación nueva de utilizar algún tipo de servicio de confianza en particular, y que las obligaciones existentes deben mantenerse inalteradas.

50. Una posible disposición podría formularse de la siguiente manera:

> Nada de lo dispuesto en el presente [proyecto de instrumento] impondrá a ninguna de las partes la obligación de [verificar la identidad de] [identificar a] otra entidad o de utilizar un servicio de confianza.

6. Interpretación uniforme

51. Por lo general, los textos de la CNUDMI contienen una disposición en la que se menciona el origen uniforme de dichos textos y el deber de interpretarlos de manera uniforme. El propósito de esa disposición es garantizar que se mantenga la uniformidad en el momento de la interpretación y aplicación del texto legislativo.

52. Una posible disposición podría formularse de la siguiente manera:

> 1. En la interpretación del presente [proyecto de instrumento] se tendrán en cuenta su carácter internacional y la necesidad de promover la uniformidad en su aplicación y la observancia de la buena fe en el comercio internacional.
>
> 2. Las cuestiones relativas a las materias que se rigen por el presente [proyecto de instrumento] que no estén expresamente resueltas en él se dirimirán de conformidad con los principios generales en que se basa este instrumento o, en su defecto, de conformidad con la ley aplicable en virtud de las normas del derecho internacional privado.

53. En el segundo párrafo de la disposición propuesta, la referencia a “la ley aplicable en virtud de las normas del derecho internacional privado” puede resultar particularmente útil en el contexto transfronterizo.

D. Requisitos y mecanismos de reconocimiento jurídico

54. En términos generales, puede entenderse que el reconocimiento jurídico es el que define los requisitos que deben cumplirse para la adquisición de una determinada condición jurídica en una jurisdicción. Para el otorgamiento del reconocimiento jurídico en el plano nacional puede ser necesario formular normas sustantivas.

55. Puede entenderse por reconocimiento jurídico transfronterizo: a) el otorgamiento en la jurisdicción receptora de la misma condición jurídica que en la jurisdicción de origen; b) el otorgamiento de la misma condición jurídica que en la jurisdicción receptora, independientemente de cualquier elemento extranjero; o c) la definición de los efectos del reconocimiento jurídico en un instrumento sobre ese tema. Además, el reconocimiento jurídico transfronterizo puede ser mutuo, es decir, recíproco, o unilateral. En ambos casos, puede estar sometido a condiciones.

56. El reconocimiento jurídico de los sistemas de gestión de la identidad y los servicios de confianza es el tema central de la labor del Grupo de Trabajo y debería dar lugar a la admisibilidad legal de aspectos técnicos como la interoperabilidad de las credenciales de identidad y los servicios de confianza y la portabilidad de la identidad y la confianza entre los sistemas de gestión de la identidad. Como ya se señaló (párr. 6 *supra*), el reconocimiento jurídico transfronterizo de la identidad tiene elementos en común con el reconocimiento jurídico de la identidad entre distintos sistemas de gestión de la identidad, independientemente de los elementos extranjeros.

57. Pueden ser objeto de reconocimiento jurídico los sistemas de gestión de la identidad y los sistemas de servicios de confianza. En ese caso tal vez sea necesario proporcionar orientación jurídica sobre las características que deben tener esos sistemas para que se les otorgue el reconocimiento jurídico. Como consecuencia de ello, el producto generado por esos sistemas para ser utilizado en las operaciones, es decir, los medios de identificación electrónica y determinados servicios de confianza, también puede beneficiarse del reconocimiento jurídico.

58. También pueden ser objeto de reconocimiento jurídico las operaciones facilitadas por el uso de la gestión de la identidad y los servicios de confianza. En ese caso, tal vez se necesite orientación jurídica sobre las condiciones que deben cumplirse para que se otorgue el reconocimiento jurídico a las credenciales de identidad y las verificaciones y al producto de los servicios de confianza. Los textos de la CNUDMI sobre comercio electrónico se ocupan principalmente de cuestiones relacionadas con las operaciones. Por ejemplo, la LMFE trata principalmente de la utilización de las firmas electrónicas

en operaciones y solo parcialmente de las características de los sistemas de firmas electrónicas.

59. El Grupo de Trabajo tal vez desee plantearse si su labor sobre el reconocimiento jurídico debería aplicarse a los sistemas de gestión de la identidad y los servicios de confianza, a las operaciones facilitadas por el uso de la gestión de la identidad y los servicios de confianza, o a ambas cosas.

60. El Grupo de Trabajo quizás desee plantearse también si debería ocuparse solamente de prever un mecanismo de reconocimiento jurídico transfronterizo, o si debería ocuparse también del reconocimiento jurídico entre distintos sistemas de una misma jurisdicción.

1. Gestión de la identidad

a) Reconocimiento jurídico *ex ante*

61. Un mecanismo que puede utilizarse para el reconocimiento jurídico de los sistemas de gestión de la identidad consiste en establecer previamente una lista de sistemas de gestión de la identidad reconocidos y de las condiciones que debe reunir un sistema para ser incluido en esa lista. Este método requiere, por lo general, que se establezca un mecanismo institucional de evaluación y otorgamiento de permisos administrado centralmente, para que evalúe los sistemas de gestión de la identidad.

62. Este método, que también es aplicable a los servicios de confianza, puede aportar claridad y previsibilidad con respecto a los sistemas y servicios que es posible utilizar entre distintos sistemas y a través de fronteras. Sin embargo, puede dar lugar a que se deniegue el reconocimiento jurídico a los sistemas y servicios que, a pesar de utilizarse, no figuren en la lista. Este mecanismo, dependiendo de cómo se administre, quizás no reaccione ante los acontecimientos con la rapidez que podría exigir la evolución tecnológica, creando así posibles obstáculos a la innovación, y tal vez dé lugar a que se impongan requisitos vinculados a alguna tecnología en particular.

63. El mecanismo institucional necesario para aplicar este método exige que se indiquen claramente los requisitos que debe reunir la entidad evaluadora y que se definan los criterios de evaluación de los sistemas de gestión de la identidad, así como los mecanismos que deberán emplearse para actualizarlos, el proceso de adopción de decisiones relativas a la evaluación y las fuentes de financiación. La gestión de ese sistema de otorgamiento de permisos puede ser más o menos compleja y costosa, dependiendo de una serie de factores, entre ellos las disposiciones institucionales preexistentes.

64. Además, un sistema de otorgamiento de permisos administrado centralmente puede ser más eficaz cuando funciona a una escala relativamente pequeña y en el marco de iniciativas de integración económica más amplias, pero es posible que plantee dificultades si se aplica a nivel mundial, ya que puede requerir un grado importante de cooperación de los miembros.

65. Para adoptar un sistema de otorgamiento de permisos administrado centralmente a nivel mundial puede ser necesario aprobar un tratado u otro instrumento de derecho internacional igualmente vinculante. Las ventajas de un mecanismo basado en un tratado serían, entre otras, la previsibilidad y, posiblemente, una mayor facilidad para aplicarlo a los órganos públicos; las desventajas serían, entre otras, los gastos vinculados a la creación y el mantenimiento del mecanismo institucional, los gastos cobrados a los sistemas participantes y la necesidad de conseguir el apoyo de un número suficiente de Estados, sistemas y usuarios. Un mecanismo basado en un tratado podría ser particularmente idóneo para financiar el cumplimiento de las obligaciones financieras de largo plazo, aunque existiera la posibilidad de sufragar los gastos con las sumas cobradas a los usuarios.

66. En leyes aprobadas recientemente sobre el tema específico de la gestión de la identidad se prevé un mecanismo centralizado de supervisión para reconocer efectos jurídicos a los sistemas de gestión de la identidad.

67. El Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (reglamento eIDAS)[9] es el único texto legislativo que trata concretamente de cuestiones transfronterizas relacionadas con la gestión de la identidad. En particular, el artículo 6 del reglamento eIDAS permite utilizar los medios de identificación electrónica de un Estado miembro de la Unión Europea para acceder a un servicio prestado en línea por un organismo del sector público de otro Estado miembro, si se cumplen determinadas condiciones. Una de esas condiciones es que los medios de identificación electrónica se expidan a través de un sistema de identificación electrónica notificado a la Comisión Europea y cumplan los requisitos de interoperabilidad establecidos por la Comisión Europea. Como parte del proceso de notificación se realiza un examen por homólogos o revisión inter pares.

68. En otras leyes sobre gestión de la identidad se regula el tema sin mencionar concretamente las cuestiones transfronterizas. Al respecto cabe señalar que, si bien el reglamento eIDAS no afecta a los sistemas de gestión de la identidad existentes, aunque tiene por objeto lograr el reconocimiento jurídico recíproco entre esos sistemas a través de fronteras, las leyes nacionales sobre gestión de la identidad establecen las condiciones que debe cumplir un sistema de gestión de la identidad para poder operar.

69. La Ley núm. 2017-20 de Benin tiene una sección relativa a la gestión de la identidad que trata de los niveles de garantía de los sistemas de identificación electrónica, las condiciones exigidas para la notificación de los sistemas de identificación electrónica, los ataques contra la seguridad de los sistemas, la responsabilidad y la interoperabilidad. Sus disposiciones se inspiran en general en las normas correspondientes del reglamento eIDAS.

70. La Ley de Gestión de la Identidad Electrónica de Virginia[10] establece un mecanismo que permite a los operadores de marcos de confianza e identidad eximirse de responsabilidad si cumplen una serie de requisitos legales y reglamentarios (véase A/CN.9/WG.IV/WP.154, párrs. 28 y 29). En cuanto a los efectos jurídicos, cuando se utiliza una credencial de identidad o un atributo de identidad que se ajusta a las normas establecidas por el Commonwealth de Virginia, a las estipulaciones contractuales y a los reglamentos de la federación, se dan por satisfechos los requisitos exigidos por la Ley Uniforme de Operaciones Electrónicas y la Ley Uniforme de Operaciones Informáticas[11] en lo que respecta a la utilización de un procedimiento de atribución o de seguridad que sea razonable desde el punto de vista comercial.

71. La Ley núm. 205-2018 del Estado de Vermont creó un nuevo tipo específico de entidad mercantil denominada “Personal Information Protection Company” (sociedad de protección de datos personales), cuyo objeto es la gestión de información de carácter personal, a saber, el suministro a terceros de datos personales de consumidores individuales para fines relacionados con operaciones y la prestación de servicios de certificación o validación relativos a datos personales.

72. Uno de los objetivos de la Ley, enunciado expresamente, es que las sociedades de protección de datos personales actúen en interés y en beneficio de los consumidores y para protegerlos (artículo 2451, párr. 3 B)). En el artículo 2452 de la Ley núm. 205-2018 se establece que las sociedades de protección de datos personales tienen una relación fiduciaria con el consumidor cuando prestan servicios de protección de la información personal.

73. El Departamento de Reglamentación Financiera del Estado de Vermont, que tiene potestades de supervisión de las sociedades de protección de datos personales, puede dictar normas sobre el contenido de los informes que deben presentar esas sociedades y

[9] Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

[10] Ley de Gestión de la Identidad Electrónica de Virginia, Código de Virginia, artículos 2.2-436 y 2.2-437 y artículos 59.1-550 a 59.1-555.

[11] La Ley Uniforme de Operaciones Electrónicas de 1999 y la Ley Uniforme de Operaciones Informáticas de 1999, modificadas en 2000 y 2002, son leyes modelo preparadas por la National Conference of Commissioners on Uniform State Laws de los Estados Unidos de América.

el momento en que deben presentarlos. También pueden dictar normas sobre la protección y la salvaguardia de los datos personales y sobre el intercambio de esa información con terceros.

b) Reconocimiento jurídico *ex post*

74. Otra posibilidad es obtener el reconocimiento jurídico a través de un mecanismo que permita los intercambios con carácter general y evalúe la idoneidad de un sistema de gestión de la identidad o un servicio de confianza para ser utilizado, pero solo en el caso de que se plantee una controversia y sobre la base de criterios determinados de antemano. En algunos textos de la CNUDMI se ha adoptado este enfoque, por ejemplo, al aplicar la llamada prueba de fiabilidad *ex post facto* (véase, por ejemplo, el art. 9, párr. 3, de la CCE).

75. Este enfoque tiene la ventaja de ofrecer a las partes que intervengan en la operación la máxima flexibilidad en cuanto a la elección de tecnologías y métodos. Además, no hace necesario establecer un mecanismo institucional, con lo que se evitan los gastos conexos, y puede administrarse en forma descentralizada. En cambio, tiene la desventaja de que requiere un proceso decisorio con la intervención de un tercero que evalúa la idoneidad del sistema de gestión de la identidad o el servicio de confianza para ser utilizado a través de fronteras, lo que puede resultar costoso y tardar mucho tiempo, y, además, genera incertidumbre para las partes.

c) Reconocimiento jurídico basado en un cuadro comparativo

76. Se sugirió la posibilidad de elaborar un cuadro comparativo entre los sistemas de gestión de la identidad y un modelo común. Los requisitos jurídicos aplicables a dicha labor y los efectos de esta serían definidos por la jurisdicción receptora y el sistema de gestión de la identidad.

77. Al preparar el cuadro comparativo, se podría tener en cuenta la descripción genérica de los niveles de seguridad a fin de centrar la labor en los resultados, lo que, a su vez, garantizaría la aplicación del principio de neutralidad tecnológica.

78. La elaboración del cuadro comparativo no dependería de la aprobación de un organismo central, sino que podría hacerla cualquier interesado, por ejemplo, un particular o una empresa. El cuadro comparativo se publicaría en una lista fiable para su difusión al público.

79. Algunos elementos que podrían tenerse en cuenta al elaborar el cuadro comparativo son los que se señalan en el Reglamento de Ejecución de la Comisión Europea (UE) 2015/1502, aplicado en el marco del reglamento eIDAS. Esos elementos son: la inscripción, la gestión de los medios de identificación electrónica, la autenticación y la gestión y organización. Cada elemento tiene varios elementos secundarios. El Grupo de Trabajo tal vez desee estudiar en qué medida debería ofrecerse orientación sobre las especificaciones y los procedimientos aplicables a la elaboración del cuadro comparativo.

80. Quizás un ejemplo práctico permita ilustrar la forma en que podría funcionar el cuadro comparativo. Como ya se señaló, el conocimiento del cliente es un requisito que se exige con frecuencia en diversos sectores empresariales. Dependiendo de la operación que se vaya a realizar, el requisito de conocimiento del cliente por lo general se cumple mediante la utilización de credenciales cuyo nivel de seguridad sea “dos” o “alto”, o bien “tres” o “considerable” (véanse los párrs. 13 y 14 del documento A/CN.9/WG.IV/WP.154, en los que figura una descripción de los distintos niveles de seguridad).

81. Normalmente es posible que el requisito no se cumpla si se utilizan credenciales de identidad emitidas en una jurisdicción diferente en la que no existe un mecanismo de reconocimiento jurídico de los sistemas de gestión de la identidad. Al comparar las credenciales con las descripciones genéricas de los niveles de seguridad, sería posible determinar si las credenciales de identidad podrían ajustarse al nivel de seguridad necesario para demostrar el conocimiento del cliente en esas operaciones en particular.

82. Por ejemplo, el operador A del sistema de identidad podría presentar una certificación de que su sistema de identificación electrónica X se ajusta al nivel de seguridad 2 o alto y que su sistema de identificación electrónica Y se ajusta al nivel de seguridad 3 o considerable, y de ese modo inscribir los sistemas de identificación electrónica X e Y en la lista de confianza. La persona jurídica B, que desea realizar operaciones comerciales en forma electrónica con la institución financiera C, podrá utilizar credenciales emitidas por el sistema de identificación electrónica X o el sistema de identificación electrónica Y, dependiendo de los requisitos de la operación. La institución financiera C podrá verificar que los sistemas de identificación electrónica X e Y están inscritos en la lista de confianza y comprobar los niveles de seguridad correspondientes a cada uno y, en función de ello, aceptar las credenciales emitidas con arreglo a esos sistemas de identificación electrónica.

83. El ejemplo anterior puede aplicarse también en un contexto nacional si el derecho interno no establece los requisitos exigidos para el reconocimiento jurídico y la equivalencia de los sistemas de identificación electrónica.

84. El mecanismo propuesto podría basarse en dos disposiciones que trataran, respectivamente, de las condiciones aplicables a la inscripción en la lista de confianza y los efectos de esa inscripción.

85. Una posible disposición sobre las condiciones exigidas para la inscripción en la lista de confianza podría formularse de la siguiente manera:

> 1. Los proveedores de servicios de gestión de la identidad y servicios de confianza que se propongan comenzar a prestar sus servicios deberán enviar a [...] [el organismo de supervisión] una notificación de su intención de hacerlo, acompañada de una certificación.
>
> 2. En la certificación deberá indicarse, como mínimo, lo siguiente:
>
> a) tipo de informe de evaluación;
>
> b) cualificaciones de la entidad evaluadora;
>
> c) especificaciones técnicas y formatos utilizados para la prestación de los servicios, en particular con respecto a los niveles de seguridad y las normas aplicables al envío de mensajes.
>
> 3. [El órgano de supervisión] [...] deberá establecer, mantener y publicar las listas de confianza, que contendrán información sobre los proveedores de servicios de identidad y de confianza y los servicios que prestan.

86. El Grupo de Trabajo tal vez desee plantearse si la palabra “certificación”, tal como se utiliza en la disposición propuesta, podría referirse también a la autocertificación, que puede ser apropiada para servicios que ofrezcan un nivel de seguridad menor (véase A/CN.9/WG.IV/WP.154, párrs. 3 a 9).

87. Según la disposición propuesta, es necesario designar a la entidad encargada de llevar la lista de confianza. Podría ser una entidad nacional, si se establece un mecanismo para notificar a las entidades nacionales competentes.

88. Con respecto a los efectos jurídicos de la inscripción en la lista de confianza, se podrían extraer algunos elementos útiles del artículo 12 de la LMFE. Además, en una disposición sobre los efectos del reconocimiento jurídico también se podría consagrar el principio de que solo deberían reconocerse los servicios de identidad y confianza extranjeros que ofrecieran un nivel de seguridad igual o mayor al exigido en el país en que se solicitara el reconocimiento (el denominado “principio de reciprocidad”). Se podría incluir una disposición con el siguiente texto:

> Los servicios de identidad o de confianza prestados fuera del [Estado receptor] e inscritos en la lista de confianza establecida de conformidad con el artículo ... tendrán los mismos efectos jurídicos en [el Estado receptor] que los servicios de identidad o de confianza prestados en el [Estado receptor] [que ofrezcan un [nivel de seguridad] equivalente][...]].

89. El Grupo de Trabajo quizás desee estudiar la posibilidad de dar más orientación con respecto al uso del cuadro comparativo y la referencia al concepto de niveles de seguridad para determinar los efectos jurídicos de los servicios de identidad y de confianza extranjeros. En ese contexto, el Grupo de Trabajo tal vez desee plantearse si convendría hacer referencia al concepto de "grado de fiabilidad sustancialmente equivalente", mencionado en el artículo 12 de la LMFE.

90. En el marco de sus deliberaciones, el Grupo de Trabajo quizás podría analizar diversos ejemplos de utilización de sistemas de gestión de la identidad. Dado que esta cuestión puede plantearse tanto en operaciones nacionales como en operaciones transfronterizas, el Grupo de Trabajo tal vez desee examinar ambas hipótesis. En particular, quizás podría analizar las dificultades que, al parecer, suelen surgir como consecuencia de la necesidad de cumplir los requisitos obligatorios establecidos por los organismos públicos, que tal vez no sea fácil contemplar en los acuerdos contractuales. Por ejemplo, como se explicó anteriormente (párrs. 80 a 83 *supra*), es posible que un banco desee saber cuáles son los sistemas de gestión de la identidad que pueden utilizarse para cumplir los requisitos de conocimiento del cliente.

91. En síntesis, los elementos que pueden resultar pertinentes para un mecanismo de reconocimiento jurídico son, entre otros: la notificación y la inscripción en una lista de confianza; los requisitos que deben cumplirse, entre ellos los relativos a los niveles de seguridad; el uso de la certificación para demostrar el cumplimiento de los requisitos; un organismo central de supervisión y otorgamiento de permisos, y la elaboración de un cuadro comparativo.

92. El Grupo de Trabajo tal vez desee estudiar el enfoque en que debería basarse un mecanismo de reconocimiento jurídico. Al hacerlo, quizás también podría examinar en más detalle la cuestión de si ese mecanismo de reconocimiento jurídico debería aplicarse únicamente a través de fronteras o también entre distintos sistemas de una misma jurisdicción (véase el párr. 60 *supra*).

2. Servicios de confianza

93. Con respecto a los servicios de confianza, se han ideado varios mecanismos jurídicos para lograr el reconocimiento jurídico de las firmas electrónicas. En ese sentido, cabe señalar que, según una opinión, no todas las firmas electrónicas son el producto de servicios de confianza, sino que solo pueden considerarse tales las que requieren la participación de un tercero que preste esos servicios. Conforme a otra opinión, todas las firmas electrónicas son el producto de servicios de confianza. El Grupo de Trabajo podría quizás aclarar esta cuestión.

94. En lo que respecta a los textos de la CNUDMI, las normas de equivalencia funcional aplicables a las firmas electrónicas (véase el párr. 36 *supra*) prevén el reconocimiento jurídico en el plano nacional.

95. En cuanto al reconocimiento jurídico transfronterizo, el artículo 12 de la LMFE, que adopta un enfoque de "equivalencia sustancial"[12], no permite la discriminación basada en los elementos extranjeros de la firma electrónica. El artículo 9, párrafo 3, de la CCE define los requisitos necesarios para establecer la equivalencia funcional entre las firmas manuscritas y las electrónicas, pero no determina *per se* la condición jurídica de la firma en la jurisdicción en que se solicita el reconocimiento[13].

96. Otro mecanismo de reconocimiento transfronterizo de las firmas electrónicas se basa en la celebración de un acuerdo internacional específico al respecto o en la concertación, en ejercicio de facultades delegadas, de un memorando de entendimiento.

---

[12] En la publicación de la CNUDMI titulada *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas* (publicación de las Naciones Unidas, núm. de venta S.09.V.4), párrs. 158 a 161, figura más información sobre la equivalencia sustancial.

[13] *Nota explicativa de la secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales* (publicación de las Naciones Unidas, núm. de venta S.07.V.2), párr. 156.

Por ejemplo, en el artículo 14 del reglamento eIDAS se dispone que los servicios de confianza prestados por proveedores establecidos fuera de la Unión Europea serán reconocidos como legalmente equivalentes a los servicios de confianza prestados por proveedores cualificado establecidos en la Unión Europea solamente en el caso de que sean reconocidos en virtud de un acuerdo internacional. El artículo 19 de la Ley de Tecnología de la Información de 2008 de la India permite el reconocimiento de autoridades certificadoras extranjeras en las siguientes condiciones:

> "1) Con sujeción a las condiciones y restricciones establecidas o que se establezcan en la reglamentación, el Contralor podrá, previa autorización del Gobierno Central y mediante publicación de una notificación en el Diario Oficial, reconocer a cualquier autoridad certificadora extranjera como autoridad certificadora a los efectos de la presente Ley.
>
> 2) Cuando una autoridad certificadora haya sido reconocida de conformidad con el párrafo 1, todo certificado de firma electrónica que emita esa autoridad certificadora se considerará válido a los efectos de la presente Ley.
>
> 3) El Contralor, si comprobara que una autoridad certificadora ha infringido alguna de las condiciones o restricciones con sujeción a las cuales se le otorgó el reconocimiento de conformidad con el párrafo 1, podrá, por motivos que deberán hacerse constar por escrito y mediante publicación de una notificación en el Diario Oficial, revocar ese reconocimiento."

97. Otros métodos que permiten obtener el reconocimiento, ya sea a través de fronteras o entre distintos sistemas, de firmas electrónicas basadas en infraestructura de clave pública ("ICP") son el reconocimiento recíproco y la certificación recíproca [14]. El reconocimiento recíproco es un arreglo de interoperabilidad en virtud del cual la parte que confía y que se encuentre en la zona abarcada por una ICP puede utilizar información autorizada correspondiente a la zona de cobertura de otra ICP para autenticar datos en la zona abarcada por la primera ICP[15]. La certificación recíproca es la práctica de reconocer la clave pública de otro prestador de servicios de certificación por referencia a un nivel convenido de confianza, habitualmente en virtud de un contrato[16]. Estos métodos de base contractual podrían respaldarse con una disposición legal específica al respecto. Por ejemplo, en el artículo 43 de la Ley núm. 527 de 1999 de Colombia se establece que:

> "Los certificados de firmas digitales emitidos por entidades de certificación extranjeras podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley para la emisión de certificados por parte de las entidades de certificación nacionales, siempre y cuando tales certificados sean reconocidos por una entidad de certificación autorizada que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia."

98. Los mecanismos antes mencionados existen desde hace algún tiempo, pero aún no han logrado hacer realidad la plena aplicación del reconocimiento transfronterizo de las firmas electrónicas. Solo unos pocos Estados han incorporado la LMFE a su derecho interno, y a menudo sin incluir el artículo 12. La participación de los Estados en la CCE, aunque crece de manera constante, sigue siendo reducida. Los mecanismos de reconocimiento recíproco de base legal tienen un costo alto en términos de tiempo y recursos y se han utilizado en muy pocos casos. Los mecanismos de reconocimiento recíproco y certificación recíproca basados en ICP se aplican únicamente a las autoridades certificadoras que los han negociado y, si no están respaldados por disposiciones legales en todas las jurisdicciones interesadas, es posible que no cumplan los requisitos obligatorios establecidos en la legislación.

---

[14] En la publicación titulada *Fomento de la confianza en el comercio electrónico*, antes citada, párrs. 165 a 172, figura más información sobre el reconocimiento recíproco y la certificación recíproca.

[15] *Fomento de la confianza en el comercio electrónico*, op. cit., párr. 165.

[16] *Fomento de la confianza en el comercio electrónico*, op. cit., párr. 169.