



Assemblée générale

Distr. limitée
16 septembre 2019
Français
Original : anglais

**Commission des Nations Unies
pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Cinquante-neuvième session
Vienne, 25-29 novembre 2019**

Projet de dispositions relatives à la reconnaissance internationale de la gestion de l'identité et des services de confiance

Note du Secrétariat

Table des matières

	<i>Page</i>
I. Introduction.	2
Annexe I. Projet de dispositions relatives à la reconnaissance internationale de la gestion de l'identité et des services de confiance	3



I. Introduction

1. Le projet révisé de dispositions relatives à la reconnaissance internationale de la gestion de l'identité et des services de confiance figurant dans l'annexe du présent document tient compte des délibérations menées par le Groupe de travail à sa cinquante-huitième session (New York, 8-12 avril 2019), ainsi que des résultats des consultations que le Secrétariat a menées auprès d'experts, comme le Groupe de travail le lui avait demandé ([A/CN.9/971](#), par. 67). Pour ce faire, le Secrétariat a convoqué une réunion d'experts (Vienne, 22-23 juillet 2019) chargée d'étudier des normes et des procédures qui permettent d'assurer la reconnaissance juridique des systèmes de gestion de l'identité ainsi que d'autres questions traitées dans le projet de dispositions, notamment la fiabilité des systèmes de gestion de l'identité et les obligations et la responsabilité des prestataires de services de gestion de l'identité.
2. On trouvera un historique des travaux en cours du Groupe de travail IV dans le document [A/CN.9/WG.IV/WP.159](#), (par. 6 à 17).

Annexe I

Projet de dispositions relatives à la reconnaissance internationale de la gestion de l'identité et des services de confiance

Chapitre I. Dispositions générales

Article premier. Définitions

Aux fins du présent [instrument] :

- a) Par « attribut », on entend une donnée ou un élément d'information associé à un sujet¹ ;
- b) Par « message de données », on entend l'information créée, transmise, reçue ou conservée par des moyens électroniques, magnétiques ou optiques ou des moyens analogues ;
- c) Par « identification », on entend le processus consistant à réunir, à vérifier et à valider suffisamment d'attributs pour établir et confirmer l'identité d'un sujet dans un contexte donné² ;
- d) Par « identité », on entend un ensemble d'attributs qui [permet d'identifier le sujet de manière suffisante] [décrit le sujet [de façon unique]] dans un contexte donné³ ;
- e) Par « justificatifs d'identité », on entend [un ensemble de données présenté comme preuve d'une identité déclarée] [les données, ou l'objet matériel sur lequel elles se trouvent, qu'un sujet peut présenter pour permettre de vérifier ou d'authentifier son identité dans un environnement en ligne]^{4, 5} ;
- f) Par « services de gestion de l'identité », on entend des services consistant à gérer l'identification de sujets dans un environnement en ligne ;
- g) Par « prestataire de services de gestion de l'identité », on entend une personne [qui fournit des services de gestion de l'identité] [qui fournit des services liés à des systèmes de gestion de l'identité] [responsable d'un système de gestion de l'identité]^{6, 7} ;

¹ Voir [A/CN.9/WG.IV/WP.150](#), par. 13.

² Voir [A/CN.9/WG.IV/WP.150](#), par. 29. Le Groupe de travail voudra peut-être se demander si cette définition reflète avec exactitude l'utilisation du terme « identification » qui est faite dans le projet de dispositions (eu égard, en particulier, au projet d'article 9) ou si elle devrait être révisée afin d'inclure d'autres processus de gestion de l'identité tels que l'inscription et la délivrance de justificatifs d'identité.

³ Voir [A/CN.9/WG.IV/WP.150](#), par. 38. Lorsqu'il examinera la définition du terme « identité », le Groupe de travail voudra peut-être se demander s'il est nécessaire de poser l'exigence de l'unicité aux fins de ses travaux étant donné que : a) l'unicité est un attribut de l'identité fondamentale, et b) l'identité fondamentale est actuellement exclue du champ de ses travaux ([A/CN.9/965](#), par. 10).

⁴ Cette définition est inspirée de la définition qui figure aux articles 59.1 à 550 de la loi de l'État de Virginie sur la gestion de l'identité électronique (Titre 59.1, Chap. 50 du Code de l'État de Virginie).

⁵ Voir [A/CN.9/WG.IV/WP.150](#), par. 21. L'expression « justificatifs d'identité » est pratiquement synonyme de celle de « moyens d'identification électronique » telle qu'elle est définie au paragraphe 2 de l'article 3 du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (règlement eIDAS), à savoir « élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne ».

⁶ Le Groupe de travail est convenu d'utiliser le terme « prestataire de services de gestion de l'identité » de préférence à « opérateur de système de gestion de l'identité » ([A/CN.9/971](#), par. 97).

⁷ Le Groupe de travail voudra peut-être se demander si cette définition devrait être conservée sous sa forme actuelle au vu des définitions du terme « fournisseur d'identité » qui figurent au

- h) Par « système de gestion de l'identité », on entend un ensemble de processus servant à gérer l'identification de sujets dans un environnement en ligne⁸ ;
- i) Par « partie utilisatrice », on entend une personne susceptible d'agir en se fiant à des services de gestion de l'identité ou à des services de confiance ;
- j) Par « sujet », on entend la personne ou l'objet identifié dans un contexte donné⁹ ;
- k) Par « service de confiance »¹⁰, on entend un service électronique qui offre un certain niveau de fiabilité en ce qui concerne la qualité des données ;
- l) Par « prestataire de services de confiance », on entend une personne qui fournit un ou plusieurs services de confiance.

Article 2. Champ d'application

Le présent [instrument] s'applique à l'utilisation et à la reconnaissance internationale de systèmes de gestion de l'identité et de services de confiance dans le cadre d'activités commerciales¹¹ et de services [publics]¹² touchant au commerce¹³.

paragraphe 37 du document [A/CN.9/WG.IV/WP.150](#), à savoir : a) une entité chargée d'identifier des personnes, entités juridiques, appareils et/ou objets numériques, de délivrer les justificatifs d'identité correspondants et de gérer ces informations pour le compte des sujets ; et b) une entité qui crée, maintient et gère des informations d'identité sécurisées pour d'autres entités (utilisateurs/abonnés, organisations et dispositifs, par exemple) et propose des services fondés sur l'identité basés sur une relation de confiance, commerciale ou d'autres natures.

⁸ Voir [A/CN.9/WG.IV/WP.150](#), par. 35. À la cinquante-septième session du Groupe de travail, il a été dit que cette définition semblait impliquer que la référence cumulée à l'« identification », à l'« authentification » et à l'« autorisation » était indispensable pour définir le concept visé, alors que l'un ou l'autre des éléments énumérés y suffirait. Certains ont déclaré, pour cette raison, que la définition du terme « identification électronique » qui figure dans le règlement eIDAS serait préférable ([A/CN.9/965](#), par. 91). Au paragraphe 1 de l'article 3 du règlement eIDAS, l'« identification électronique » est définie comme « le processus consistant à utiliser des données d'identification personnelle [c'est-à-dire des “justificatifs d'identité” tels qu'ils sont définis dans le présent document] sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale ».

⁹ Voir [A/CN.9/WG.IV/WP.150](#), par. 38.

¹⁰ Le Groupe de travail voudra peut-être examiner la question de savoir s'il convient de faire référence, en anglais, à « trusted service » pour éviter toute ambiguïté quant à la notion juridique bien établie de « trust » ([A/CN.9/965](#), par. 14 et 101).

¹¹ Comme convenu par le Groupe de travail à sa cinquante-huitième session, cette disposition a été reformulée de façon à associer des éléments des deux options proposées pour le paragraphe 1 de l'article premier dans le document [A/CN.9/WG.IV/WP.157](#) ([A/CN.9/971](#), par. 23). À sa cinquante-deuxième session, la Commission a noté qu'à ce stade précoce du projet, le Groupe de travail devrait s'attacher à élaborer un instrument qui pourrait s'appliquer à l'utilisation des systèmes de gestion de l'identité et des services de confiance à l'échelle tant interne qu'internationale ([A/74/17](#), par. 172). Ce point de vue se reflète dans le fait que la disposition mentionne à la fois l'« utilisation » et la « reconnaissance » des systèmes de gestion de l'identité et des services de confiance.

¹² Le Groupe de travail voudra peut-être se demander si la présence du mot « publics » est nécessaire, ou s'il suffirait d'une référence générale aux « services touchant au commerce » pour bien rendre l'idée d'opérations qui présentent un lien avec le commerce, mais ne sont pas de nature commerciale, comme l'interaction avec un guichet unique électronique pour les opérations douanières.

¹³ Le Groupe de travail est convenu que l'instrument devrait prévoir la possibilité d'utiliser le produit des travaux pour répondre à des besoins en dehors d'un cadre purement commercial ([A/CN.9/971](#), par. 23). À sa cinquante-deuxième session, la Commission a noté que les résultats des travaux auraient des incidences sur certaines questions qui sortaient du cadre des opérations commerciales ([A/74/17](#), par. 172).

*Article 3. Caractère volontaire de l'utilisation de systèmes de gestion de l'identité et de services de confiance*¹⁴

1. Aucune disposition du présent [instrument] n'exige d'un sujet qu'il [utilise un système de gestion de l'identité] [accepte des justificatifs d'identité] ou recoure à un service de confiance sans son consentement.
2. Aux fins du paragraphe 1, le consentement d'un sujet peut être déduit de son comportement¹⁵.

*Article 4. Interprétation*¹⁶

1. Pour l'interprétation du présent [instrument], il est tenu compte de son caractère international et de la nécessité de promouvoir l'uniformité de son application ainsi que d'assurer le respect de la bonne foi [dans le commerce international].
2. Les questions concernant les matières régies par le présent [instrument] qui ne sont pas expressément tranchées par lui sont réglées selon les principes généraux dont il s'inspire, en particulier la non-discrimination à l'égard de l'utilisation de moyens électroniques, la neutralité technologique et l'équivalence fonctionnelle [et (...)]¹⁷ [ou, à défaut de ces principes, conformément à la loi applicable en vertu des règles du droit international privé]¹⁸.

Chapitre II. Gestion de l'identité

*Article 5. Reconnaissance juridique de la gestion de l'identité*¹⁹

1. [L'utilisation] [de justificatifs d'identité] [de systèmes de gestion de l'identité] n'est pas privée d'effets juridiques, de validité, de force exécutoire ou de caractère probant au seul motif que :
 - a) [Les résultats de la vérification²⁰ d'identité] [les systèmes de gestion de l'identité] se présentent sous une forme électronique ; ou
 - b) Les systèmes de gestion de l'identité ne sont pas des systèmes de gestion de l'identité désignés conformément à l'article 11.
2. Aucune disposition du présent [instrument] n'oblige quiconque à identifier un sujet ou à utiliser un service de gestion de l'identité particulier.

¹⁴ La teneur du projet d'article 2 qui figure dans le document [A/CN.9/WG.IV/WP.157](#), intitulé « Questions sur lesquelles le présent [projet d'instrument] est sans incidence », est maintenant intégrée aux projets d'articles 5 et 13. Le Groupe de travail voudra peut-être se demander si la teneur de l'actuel projet d'article 3 devrait de même être intégrée aux projets d'articles 5 et 13.

¹⁵ Si le sujet est un objet matériel ou numérique qui n'est pas capable d'un comportement autonome, le consentement sera attribuable à la personne physique ou morale qui en est juridiquement responsable ([A/CN.9/965](#), par. 109).

¹⁶ À sa cinquante-huitième session, le Groupe de travail n'a pas examiné le projet de disposition relative à l'interprétation de l'instrument (projet d'article 5 figurant dans le document [A/CN.9/WG.IV/WP.157](#)), qui s'inspire de dispositions similaires énoncées dans d'autres textes de la CNUDCI. Il voudra peut-être se demander si cette disposition devrait faire référence à la « bonne foi » et, le cas échéant, préciser « dans le commerce international ».

¹⁷ Le Groupe de travail voudra peut-être se demander s'il conviendrait de mentionner des principes généraux supplémentaires, notamment celui de transparence (voir [A/CN.9/936](#), par. 88).

¹⁸ L'ajout du membre de phrase « ou, à défaut de ces principes, conformément à la loi applicable en vertu des règles du droit international privé » pourrait s'avérer particulièrement utile dans un contexte international.

¹⁹ Le paragraphe 1 du projet d'article 5 suit le même schéma que le projet d'article 13, qui lui-même reflète les délibérations tenues par le Groupe de travail à sa cinquante-huitième session. Cette disposition établit les effets juridiques de l'identification par des moyens électroniques, indépendamment de l'existence d'une procédure d'identification hors ligne. Les paragraphes 2 à 4 s'inspirent du projet d'article 2 qui figure dans le document [A/CN.9/WG.IV/WP.157](#).

²⁰ En ce qui concerne l'alinéa a), si la première option est choisie, le Groupe de travail voudra peut-être envisager d'ajouter une référence à l'« authentification » de l'identité, par souci de cohérence avec le libellé de la définition du terme « justificatifs d'identité » qui figure à l'article premier.

3. Sous réserve de ce que prévoient ses dispositions, rien, dans le présent [instrument], n'a d'incidence sur l'application aux services de gestion de l'identité des règles de droit applicables [, y compris celles applicables au respect de la vie privée et à la protection des données]²¹.

4. Aucune disposition du présent [instrument] n'a d'incidence sur une exigence légale selon laquelle un sujet doit être identifié suivant une procédure définie ou prescrite par la loi²².

Article 6. Obligations incombant aux prestataires de services de gestion de l'identité

Les prestataires de services de gestion de l'identité sont tenus [au minimum]²³ :

- a) D'inscrire les sujets, en ayant notamment soin :
 - i) De collecter et d'enregistrer les attributs ;
 - ii) De contrôler et de vérifier l'identité ; et
 - iii) D'attacher les justificatifs d'identité au sujet ;
- b) D'actualiser les attributs ;
- c) De gérer les justificatifs d'identité conformément aux règles qui régissent les systèmes de gestion de l'identité, en ayant notamment soin :
 - i) D'émettre, de délivrer et d'activer les justificatifs ;
 - ii) De suspendre, de révoquer et de réactiver les justificatifs ; et
 - iii) De renouveler et de remplacer les justificatifs ;
- d) D'authentifier les sujets, en ayant notamment soin :
 - i) De gérer les facteurs d'authentification ; et
 - ii) De gérer les mécanismes d'authentification ;
- e) De garantir la disponibilité en ligne et le bon fonctionnement des systèmes de gestion de l'identité ; et
- f) D'assurer un accès raisonnable aux règles qui régissent les systèmes de gestion de l'identité²⁴.

Article 7. Obligations incombant aux prestataires de services de gestion de l'identité en cas de violation des données

1. En cas d'atteinte à la sécurité ou de perte d'intégrité ayant une incidence [importante] sur un système de gestion de l'identité, notamment sur les attributs qui y sont gérés, les prestataires de services de gestion de l'identité sont tenus :

- a) D'informer immédiatement [l'autorité de contrôle] [les sujets affectés et les parties utilisatrices] de l'atteinte à la sécurité ou de la perte d'intégrité ;
- b) De remédier à l'atteinte à la sécurité ou à la perte d'intégrité ;
- c) De suspendre [les justificatifs d'identité] affectés jusqu'à ce qu'il ait été remédié à l'atteinte à la sécurité ou à la perte d'intégrité ;

²¹ La référence au respect de la vie privée et à la protection des données reflète l'importance que le Groupe de travail attache à ces questions, bien qu'il soit entendu qu'elles sortent du cadre de son mandat (A/CN.9/965, par. 125).

²² Cette nouvelle disposition vise à répondre à une préoccupation soulevée à la cinquante-deuxième session du Groupe de travail (A/CN.9/971, par. 30).

²³ Ces obligations fondamentales des prestataires de services de gestion de l'identité ont été déterminées avec l'aide d'experts.

²⁴ L'alinéa f) a été inséré afin de tenir compte du principe de transparence dans le cadre de la prestation de services de gestion de l'identité (voir également le projet d'article 12, par. 2 b)). À sa cinquante-sixième session, le Groupe de travail a considéré le principe de transparence comme pertinent en vue de débats futurs sur la gestion de l'identité (A/CN.9/936, par. 88).

- d) De rétablir [les justificatifs d'identité] affectés dans les meilleurs délais ; et
 - e) De révoquer [les justificatifs d'identité] affectés s'il ne peut être remédié à l'atteinte à la sécurité ou à la perte d'intégrité [dans les délais prévus].
2. Si un sujet leur notifie une atteinte à la sécurité ou une perte d'intégrité, les prestataires de services de gestion de l'identité sont tenus :
- a) D'examiner l'éventuelle atteinte à la sécurité ou perte d'intégrité ; et
 - b) De prendre toute autre mesure appropriée conformément au paragraphe 1^{25, 26}.

Article 8. Obligations incombant aux sujets et aux parties utilisatrices

1. Les sujets se conforment aux instructions raisonnables communiquées par le prestataire de services de gestion de l'identité afin d'empêcher tout usage non autorisé des justificatifs d'identité ou des processus d'authentification.
2. Les sujets informent le prestataire de services de gestion de l'identité si :
 - a) Ils savent que les justificatifs d'identité ou les processus d'authentification du système de gestion de l'identité concerné ont été compromis ; ou
 - b) Des circonstances dont ils ont connaissance engendrent un risque important que les justificatifs d'identité ou les processus d'authentification aient été compromis.
3. Les parties utilisatrices informent le prestataire de services de gestion de l'identité si :
 - a) Elles savent que les justificatifs d'identité ou les processus d'authentification du système de gestion de l'identité concerné ont été compromis ; ou
 - b) Des circonstances dont elles ont connaissance engendrent un risque important que les justificatifs d'identité ou les processus d'authentification aient été compromis.

²⁵ Ce paragraphe met en œuvre la proposition tendant à ce que le projet de dispositions impose aux prestataires de services de gestion de l'identité l'obligation d'agir lorsqu'ils se voient notifier une atteinte à la sécurité (A/CN.9/971, par. 88).

²⁶ Le projet de disposition comporte, entre crochets, des éléments facultatifs qui visent à prévoir le délai dans lequel la notification doit être effectuée, à désigner les parties qui doivent être informées et à établir le niveau d'incidence sur les services ou les données à caractère personnel à partir duquel se déclenche l'obligation d'information.

Article 9. Identification au moyen de systèmes de gestion de l'identité

Lorsque la loi ou une partie exige l'identification d'un sujet [selon une certaine méthode] [selon un certain principe], cette exigence est satisfaite dans le cas de la gestion de l'identité si [une méthode] [un système de gestion de l'identité] fiable est employé[e] pour identifier ce sujet^{27, 28, 29}.

Article 10. Facteurs pertinents pour déterminer la fiabilité³⁰

1. Pour déterminer la fiabilité [de la méthode] [du système de gestion de l'identité], toutes les circonstances pertinentes sont prises en considération, notamment :

a) Le respect, par le prestataire de services de gestion de l'identité, des obligations énoncées à l'article 6 ;

b) La conformité des règles qui régissent l'exploitation du système de gestion de l'identité aux normes et procédures internationales reconnues, notamment au cadre relatif aux niveaux de garantie, une attention particulière étant accordée aux règles qui régissent :

- i) La gouvernance ;
- ii) La publication d'avis et l'information des utilisateurs ;
- iii) La gestion de la sécurité de l'information ;
- iv) La conservation des documents ;
- v) Les installations et le personnel ;
- vi) Les contrôles techniques ; et
- vii) Le contrôle et l'audit ;.

c) Toute supervision ou toute certification fournie concernant le système de gestion de l'identité ; et

d) Tout accord entre les parties.

2. Pour déterminer la fiabilité [de la méthode] [du système de gestion de l'identité], il n'est pas tenu compte :

a) Du lieu où le système de gestion de l'identité est exploité ; ni

²⁷ Cette disposition se fonde sur le projet de libellé dont le Groupe de travail est convenu à sa cinquante-huitième session (A/CN.9/971, par. 49). Celui-ci voudra peut-être se demander s'il conviendrait de faire référence à un « système de gestion de l'identité fiable » plutôt qu'à une « méthode fiable ».

²⁸ L'utilisation d'une méthode (ou d'un système de gestion de l'identité) fiable pour l'identification est l'élément essentiel du régime de reconnaissance juridique de la gestion de l'identité établi par le projet d'instrument. Celui-ci prévoit, pour déterminer la fiabilité, deux mécanismes : le projet d'article 10, qui dresse une liste indicative de facteurs pertinents pour la détermination *ex post* de la fiabilité ; et le projet d'article 11, qui prévoit la mise en place d'un mécanisme pour la désignation *ex ante* de méthodes (ou de systèmes de gestion de l'identité) fiables. À la suite de consultations tenues avec des experts, la disposition traitant d'une présomption de fiabilité (projet d'article 10 figurant dans le document A/CN.9/WG.IV/WP.157) a été supprimée dans un souci de simplification du projet d'instrument. La teneur du paragraphe 2 du projet d'article 10 qui figure dans le document A/CN.9/WG.IV/WP.157 a été intégrée au paragraphe 5 du projet d'article 11.

²⁹ Le Groupe de travail voudra peut-être se demander si le projet d'article 9 traite des cas dans lesquels une équivalence fonctionnelle doit être établie entre l'identification hors ligne et l'identification en ligne. Dans la négative, il pourrait être inséré, à cette fin, une nouvelle disposition libellée comme suit ou dans des termes similaires : « Lorsqu'une règle de droit exige ou permet l'identification d'un sujet, cette règle est satisfaite si un système de gestion de l'identité fiable est utilisé. »

³⁰ Le titre de cette disposition reflète ce dont le Groupe de travail est convenu à sa cinquante-huitième session (A/CN.9/971, par. 59).

b) Du lieu où se trouve l'établissement du prestataire de services de gestion de l'identité³¹.

Article 11. Désignation des systèmes de gestion de l'identité fiables

1. [Toute personne, tout organe ou toute autorité, de droit public ou privé, indiqué[e] par l'État adoptant comme compétent[e] en la matière] peut désigner les [méthodes] [systèmes de gestion de l'identité] qui sont fiables aux fins de l'article 9^{32, 33}.

2. Toute désignation arrêtée en vertu du paragraphe 1 doit être conforme aux normes et procédures internationales reconnues de détermination de la fiabilité des systèmes de gestion de l'identité, notamment aux cadres relatifs aux niveaux de garantie^{34, 35}.

3. Pour désigner [une méthode] [un système de gestion de l'identité], il n'est pas tenu compte :

a) Du lieu où le système de gestion de l'identité est exploité ; ni

b) Du lieu où se trouve l'établissement du prestataire de services de gestion de l'identité³⁶.

4. L'identification d'un sujet au moyen de justificatifs d'identité délivrés par un système de gestion de l'identité désigné conformément au paragraphe 1 est reconnue comme une preuve fiable de l'identité du sujet.

5. Le paragraphe 4 ne limite pas la possibilité pour quiconque :

a) D'établir par tout autre moyen la fiabilité [d'une méthode] [d'un système de gestion de l'identité] aux fins de l'article 9 ; ou

b) D'apporter des preuves de la non-fiabilité [d'une méthode] [d'un système de gestion de l'identité] désigné[e] en vertu du paragraphe 1.

³¹ Le paragraphe 2 est une disposition de non-discrimination géographique inspirée de l'article 12 de la Loi type de la CNUDCI sur les signatures électroniques (LTSE), dont l'objet est de permettre la reconnaissance internationale des système de gestion de l'identité.

³² Cette disposition a été révisée afin de tenir compte des modifications dont le Groupe de travail est convenu à sa cinquante-huitième session (A/CN.9/971, par. 76), hormis pour ce qui est de l'insertion d'un renvoi à l'article 9, en raison des modifications apportées à cette disposition à la suite de consultations tenues avec des experts. Il a plutôt été choisi d'insérer les mots « qui sont fiables aux fins de l'article 9 ».

³³ Le Groupe de travail voudra peut-être se demander si l'instrument devrait traiter de la responsabilité pour des dommages causés par l'utilisation d'un système désigné comme fiable en vertu du projet d'article 11.

³⁴ Cette disposition a été révisée afin de tenir compte des modifications dont le Groupe de travail est convenu à sa cinquante-huitième session (A/CN.9/971, par. 76).

³⁵ Le Groupe de travail voudra peut-être préciser si et comment les éléments énumérés au projet d'article 10 s'appliquent à la désignation d'un système de gestion de l'identité fiable conformément au projet d'article 11 (c'est-à-dire, si la personne, l'organe ou l'autorité qui procède à la désignation est tenu de prendre en compte les circonstances visées au paragraphe 1 de l'article 10).

³⁶ Le paragraphe 3 est une disposition de non-discrimination géographique inspirée de l'article 12 de la LTSE, dont l'objet est de permettre la reconnaissance internationale des système de gestion de l'identité.

Article 12. Responsabilité des prestataires de services de gestion de l'identité

1. Les prestataires de services de gestion de l'identité sont tenus responsables des dommages causés intentionnellement ou par négligence à quiconque en raison de manquements aux obligations qui leur incombent [dans le cadre de la prestation de leurs services] [en vertu de l'article 6]³⁷.

2. Nonobstant les dispositions du paragraphe 1, les prestataires de services de gestion de l'identité ne sont pas tenus responsables des dommages découlant d'une utilisation d'un système de gestion de l'identité dans la mesure où :

a) Cette utilisation dépasse les limitations fixées [en ce qui concerne l'objet ou la valeur des transactions pour lesquelles le système de gestion de l'identité peut être utilisé] ; et

b) Ils ont fourni [[aux utilisateurs³⁸ ou] aux tiers]³⁹ des moyens raisonnablement accessibles de déterminer ces limitations⁴⁰.

3. Les prestataires de services de gestion de l'identité ne sont pas tenus responsables des dommages causés à quiconque en raison de l'utilisation d'un système de gestion de l'identité désigné en vertu de l'article 11 si [la délivrance du justificatif d'identité ou l'attribution d'un attribut] est conforme :

a) Aux obligations qui leur incombent dans le cadre de la prestation de services de gestion de l'identité, notamment à celles énoncées à l'article 6 ;

b) Aux règles qui régissent le fonctionnement du système de gestion de l'identité, notamment à celles énoncées à l'article 10-1 b) ; et

c) À tout accord entre les parties.

[4. Le paragraphe 3 ne s'applique pas si les dommages sont imputables à un acte ou à une omission de la part du prestataire de services de gestion de l'identité qui constitue [une négligence grave ou une faute intentionnelle].]⁴¹

³⁷ Cette disposition se fonde sur le projet de libellé dont le Groupe de travail est convenu à sa cinquante-huitième session (A/CN.9/971, par. 101). Ce projet a été modifié afin de préciser la cause des dommages pour lesquels la responsabilité est imposée.

³⁸ En cas d'emploi du terme « utilisateur », le Groupe de travail voudra peut-être envisager de le définir.

³⁹ Le Groupe de travail voudra peut-être se demander s'il conviendrait de mentionner, dans le projet d'article, les parties qui devraient être en mesure de déterminer les limitations et, le cas échéant, si ces parties devraient correspondre à celles devant lesquelles les prestataires de services de gestion de l'identité peuvent être tenus responsables.

⁴⁰ Cette disposition est inspirée de l'article 9-1 d) ii) de la LTSE.

⁴¹ Ce paragraphe reproduit le paragraphe 4 du projet d'article 13 qui figure dans le document A/CN.9/WG.IV/WP.157. Le Groupe de travail voudra peut-être se demander si le paragraphe 4 pourrait être supprimé, eu égard au paragraphe 1.

Chapitre III. Services de confiance⁴²

Article 13. Reconnaissance juridique des services de confiance^{43, 44}

1. Des [informations] [données]⁴⁵ dont l'échange, la vérification ou l'authentification sont assurés ou facilités au moyen d'un service de confiance [qui satisfait aux exigences prévues au [présent chapitre]] ne sont pas privées de leurs effets juridiques, de leur validité ou de leur force exécutoire [, ou de leur caractère probant]⁴⁶ au seul motif que :

- a) Elles se présentent sous forme électronique ; ou
- b) Elles ne sont pas associées à un service de confiance fiable désigné conformément à l'article 24.

2. Aucune disposition du présent [instrument] n'oblige quiconque à utiliser un service de confiance particulier⁴⁷.

3. Sous réserve de ce que prévoient ses dispositions, rien, dans le présent [instrument], n'a d'incidence sur l'application aux services de confiance des règles de droit relatives aux services de confiance [, y compris celles applicables au respect de la vie privée et à la protection des données]⁴⁸.

Article 14. Obligations incombant aux prestataires de services de confiance

1. Les prestataires de services de confiance veillent à la disponibilité et au bon fonctionnement des services de confiance qu'ils fournissent.

2. En cas d'atteinte à la sécurité ou de perte d'intégrité ayant une incidence [importante] sur des services de confiance, les prestataires de services de confiance sont tenus :

- a) De suspendre la fourniture des services affectés, [soit jusqu'à ce qu'il ait été mis fin à l'atteinte ou à la perte, soit jusqu'à ce qu'un nouveau processus de certification ou un processus similaire ait été mis en place]] ; et

⁴² Le chapitre portant sur les services de confiance a été révisé. Il comporte désormais une disposition générale sur la reconnaissance juridique des services de confiance (projet d'article 13) ; une norme de fiabilité générale assortie d'une clause de non-discrimination géographique destinée à faciliter la reconnaissance internationale (projet d'article 23) ; un mécanisme de désignation *ex ante* des services de confiance fiables (projet d'article 24) ; et une liste des services de confiance (projets d'articles 16 à 22) à utiliser comme « éléments de base », y compris en les associant les uns aux autres, pour fournir une assurance quant à certaines qualités de données. Plus particulièrement, les signatures électroniques ont trait à la personne qui est à l'origine des données (« qui ») et à la motivation qu'elle a de les créer (« pourquoi ») ; les horodatages électroniques concernent le moment où ont lieu certains événements en rapport avec les données (« quand ») ; une nouvelle disposition sur l'intégrité traite de la garantie que les données n'ont pas été modifiées depuis un moment déterminé (« quoi ») ; et les services d'envoi concernent l'emplacement de messages de données dans le cyberspace (« où »).

⁴³ Cette disposition a été insérée afin de tenir compte de ce dont le Groupe de travail est convenu à sa cinquante-huitième session (A/CN.9/971, par. 112 à 115).

⁴⁴ Le Groupe de travail voudra peut-être se demander si cette disposition de non-discrimination devrait porter sur les informations (ou les données) qui sont échangées, vérifiées ou authentifiées, ou plutôt sur la méthode utilisée pour les vérifier et les authentifier. Un libellé antérieur de cette disposition, dans lequel était adoptée la seconde approche, se lisait comme suit : « Les services de confiance ne sont pas privés de leurs effets juridiques, de leur validité, de leur force exécutoire ou de caractère probant au seul motif qu'ils se présentent sous une forme électronique. » (par. 2 de l'article 6 figurant dans le document A/CN.9/WG.IV/WP.157).

⁴⁵ Le Groupe de travail voudra peut-être se demander s'il conviendrait d'employer le mot « données » afin d'aligner cette disposition sur la définition du terme « service de confiance ».

⁴⁶ Il est proposé d'insérer les mots « ou de leur caractère probant » de façon à aligner cette disposition sur le projet d'article 5.

⁴⁷ Les paragraphes 2 et 3 s'inspirent du projet d'article 2 qui figure dans le document A/CN.9/WG.IV/WP.157.

⁴⁸ La référence au respect de la vie privée et à la protection des données reflète l'importance que le Groupe de travail attache à ces questions, bien qu'il soit entendu qu'elles sortent du cadre de son mandat (A/CN.9/965, par. 125).

- b) De remédier à l'atteinte à la sécurité ou à la perte d'intégrité.

3. Les prestataires de services de confiance notifient [à l'autorité de contrôle] [à leurs clients⁴⁹ affectés et aux parties utilisatrices], dans les meilleurs délais [et en tout état de cause dans les [...] jours après en avoir eu connaissance], toute atteinte à la sécurité ou perte d'intégrité ayant une incidence [importante] sur les services de confiance fournis ou sur les données à caractère personnel qui y sont conservées^{50, 51}.

Article 15. Obligations incombant aux utilisateurs de services de confiance en cas de violation des données

Les utilisateurs⁵² d'un service de confiance informent le prestataire du service de confiance si :

- a) Les données de création des services de confiance ont été compromises ; ou
- b) Des circonstances dont ils ont connaissance engendrent un risque important que les données de création des services de confiance aient été compromises.

Article 16. Signatures électroniques

Lorsqu'une règle de droit exige ou permet la signature [d'une personne] [d'un sujet], cette règle est satisfaite [dans le cas d'un message de données] si une méthode fiable⁵³ est utilisée pour :

- a) Identifier la personne ; et
- b) Indiquer la volonté de cette personne concernant l'information qui figure dans le message de données⁵⁴.

⁴⁹ Le Groupe de travail voudra peut-être envisager de définir la notion de « client ».

⁵⁰ Ce paragraphe reproduit le paragraphe 2 du projet d'article 17 qui figure dans le document [A/CN.9/WG.IV/WP.157](#). Le Groupe de travail voudra peut-être se demander si l'obligation qui y est énoncée ne pourrait pas plutôt figurer en tant qu'alinéa c) du paragraphe 2, dans un souci d'harmonisation avec le projet d'article 7.

⁵¹ Le projet de disposition comporte, entre crochets, des éléments facultatifs qui visent à prévoir le délai dans lequel la notification doit être effectuée, à désigner les parties qui doivent être informées et à établir le niveau d'incidence sur les services ou les données à caractère personnel à partir duquel se déclenche l'obligation d'information.

⁵² En cas d'emploi du terme « utilisateur », le Groupe de travail voudra peut-être envisager de le définir.

⁵³ De même que pour l'évaluation de la fiabilité des systèmes de gestion de l'identité, le projet de dispositions prévoit, pour déterminer la fiabilité des services de confiance, deux mécanismes : le projet d'article 23, qui dresse une liste indicative de facteurs pertinents pour la détermination *ex post* de la fiabilité ; et le projet d'article 24, qui prévoit la mise en place d'un mécanisme pour la désignation *ex ante* de services de confiance fiables. Toujours selon une approche similaire à celle suivie pour les systèmes de gestion de l'identité, la disposition traitant d'une présomption de fiabilité (projet d'article 15 figurant dans le document [A/CN.9/WG.IV/WP.157](#)) a été supprimée dans un souci de simplification du projet d'instrument. La teneur du paragraphe 2 du projet d'article 15 qui figure dans le document [A/CN.9/WG.IV/WP.157](#) a été intégrée au paragraphe 5 du projet d'article 24.

⁵⁴ À la cinquante-huitième session du Groupe de travail, il a été proposé d'insérer les mots « de telle manière qu'un tiers puisse vérifier ultérieurement cette volonté » afin que soit prise en compte la fonction de « perpétuation » des signatures électroniques (voir [A/CN.9/971](#), par. 122). Il a cependant été jugé inutile d'insérer ces mots étant donné que les signatures électroniques se caractérisaient obligatoirement par la possibilité d'effectuer une vérification ultérieure (*ibid.*).

*Article 17. Cachets électroniques*⁵⁵

Lorsqu'une règle de droit exige ou permet qu'une personne appose un cachet, cette règle est satisfaite [dans le cas d'un message de données] si une méthode fiable est utilisée pour :

- a) Identifier la personne ; et
- b) Détecter toute altération du message de données après le moment de l'apposition.

Article 18. Horodatages électroniques

Lorsqu'une règle de droit exige ou permet que [certains documents, documents d'activité ou certaines informations ou données⁵⁶] soient accompagnés d'une indication de date et d'heure, cette règle est satisfaite [dans le cas d'un message de données] si une méthode fiable est utilisée pour :

- a) Indiquer la date et l'heure, en précisant notamment le fuseau horaire ; et
- b) Associer au message de données la date et l'heure indiquées⁵⁷.

*Article 19. Assurance de l'intégrité*⁵⁸

Lorsqu'une règle de droit exige ou permet d'assurer l'intégrité [d'un document, d'un document d'activité, d'informations ou de données], [en conservant le document dans sa forme originale, en l'archivant ou d'une autre façon,] cette règle est satisfaite dans le cas d'un message de données si une méthode fiable est utilisée pour détecter toute altération du message de données après sa création, exception faite de l'ajout de tout endossement et de toute modification intervenant dans le cours normal de la communication, de la conservation et de l'exposition⁵⁹.

*Article 20. Archivage électronique*⁶⁰

Lorsqu'une règle de droit exige ou permet que [certains documents, documents d'activité ou certaines informations] soient conservés, cette règle est satisfaite si ce sont des messages de données qui sont conservés, sous réserve que :

- a) L'information que contient le message de données soit accessible pour être consultée ultérieurement ;
- b) Le message de données soit conservé :
 - i) Sous la forme sous laquelle il a été créé, envoyé ou reçu ; ou

⁵⁵ Cette disposition reflète le fait que le Groupe de travail est convenu d'insérer une disposition autonome sur les cachets électroniques (A/CN.9/971, par. 128). Conformément à l'approche rationalisée expliquée à la note de bas de page 42, le Groupe de travail voudra peut-être se demander si une disposition autonome est nécessaire ou si la fonction visée par l'utilisation de cachets électroniques peut être remplie au moyen de signatures électroniques (pour ce qui est de l'identification) ou de l'assurance de l'intégrité (pour ce qui est de la détection d'altérations).

⁵⁶ L'insertion du mot « données » reflète ce dont est convenu le Groupe de travail (A/CN.9/971, par. 130).

⁵⁷ L'insertion des mots « en précisant notamment le fuseau horaire » reflète ce dont est convenu le Groupe de travail (A/CN.9/971, par. 132).

⁵⁸ Cette disposition a pour objet d'introduire, en ce qui concerne l'intégrité des messages de données, une règle générale qui établit l'équivalent fonctionnel de la notion d'« original » dans l'environnement papier. Elle est présentée au Groupe de travail comme solution de substitution à l'article 20, qui traite de l'archivage électronique. Ainsi formulée, elle décrit clairement ce en quoi consiste le service de confiance (à savoir, fournir une méthode fiable pour la détection d'altérations).

⁵⁹ Le Groupe de travail voudra peut-être envisager d'ajouter une exigence selon laquelle l'information que contient le message de données doit être « accessible pour être consultée ultérieurement » (voir également projet d'article 20 a)).

⁶⁰ Si le projet d'article 19 est conservé, le Groupe de travail voudra peut-être se demander s'il conviendrait de supprimer le projet d'article 20 pour cause de redondance.

- ii) Sous une forme dont il peut être démontré qu'elle représente avec précision les informations créées, envoyées ou reçues ; et
- c) Les informations qui permettent de déterminer l'origine et la destination du message de données, ainsi que les indications de date et d'heure de l'envoi ou de la réception, soient conservées si elles existent⁶¹.

Article 21. Services d'envoi recommandé électroniques

Lorsqu'une règle de droit exige ou permet la preuve de l'expédition et de la réception [d'un certain document, document d'activité ou de certaines informations], cette règle est satisfaite [dans le cas d'un message de données] si une méthode fiable est utilisée pour fournir l'assurance que le message a quitté un système d'information ou y est entré⁶².

*Article 22. Authentification de site Internet*⁶³

Lorsqu'une règle de droit exige ou permet l'identification du propriétaire d'un site Internet, cette règle est satisfaite si une méthode fiable est utilisée pour identifier la personne qui possède le site Internet et pour associer celle-ci audit site.

*Article 23. Norme de fiabilité pour les services de confiance*⁶⁴

1. Aux fins des articles [16 à 22], la méthode visée doit être :
 - a) Une méthode suffisamment fiable pour remplir la fonction pour laquelle elle est utilisée, à la lumière de toutes les circonstances pertinentes, qui peuvent englober :
 - i) Toute règle de fonctionnement applicable au service de confiance ;
 - ii) Toute norme sectorielle applicable ;
 - iii) La sûreté du matériel et des logiciels ;
 - iv) Les ressources financières et humaines, y compris l'existence d'avoirs ;
 - v) La régularité et l'étendue des audits réalisés par un organisme indépendant ;
 - vi) L'existence d'une déclaration faite par un organisme de contrôle, un organisme d'accréditation ou un programme volontaire concernant la fiabilité de la méthode ; et
 - vii) Toute convention en la matière ; ou
 - b) Une méthode dont il est démontré dans les faits qu'elle a rempli les fonctions associées au service de confiance considéré.
2. Aux fins des articles [16 à 22], pour déterminer la fiabilité de la méthode, il n'est pas tenu compte :
 - a) Du lieu où le service de confiance est exploité ; ou

⁶¹ Cette condition ne s'étend pas aux informations qui n'ont d'autre objet que de permettre l'envoi ou la réception du message de données (voir la Loi type de la CNUDCI sur le commerce électronique, art. 10, par. 2).

⁶² Ce libellé reflète le fait que le Groupe de travail est convenu d'intégrer, dans le projet de dispositions, des éléments de l'article 10 de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (A/CN.9/971, par. 141).

⁶³ Conformément à l'approche rationalisée expliquée à la note de bas de page 42, le Groupe de travail voudra peut-être se demander si les fonctions visées par l'authentification de sites Internet pourraient être remplies par l'identification d'objets numériques, y compris de sites Internet, au moyen de signatures électroniques.

⁶⁴ Les éléments énumérés au paragraphe 1 a) sont inspirés de l'article 10 de la LTSE et de l'article 12 a) de la Loi type de la CNUDCI sur les documents transférables électroniques, qui énonce une norme de fiabilité générale pour la méthode utilisée.

b) Du lieu où se trouve l'établissement du prestataire de services de confiance⁶⁵.

Article 24. Désignation des services de confiance fiables^{66, 67}

1. [Toute personne, tout organe ou toute autorité, de droit public ou privé, indiqué[e] par l'État adoptant] peut désigner les [méthodes] [services de confiance] qui sont fiables aux fins des articles [16 à 22].

2. Toute désignation arrêtée en vertu du paragraphe 1 doit être conforme aux normes et procédures internationales reconnues de détermination de la fiabilité des services de confiance, notamment aux cadres relatifs aux niveaux de garantie⁶⁸.

3. Pour désigner [une méthode] [un service de confiance], il n'est pas tenu compte :

a) Du lieu où le service de confiance est exploité ; ou

b) Du lieu où se trouve l'établissement du prestataire de services de confiance⁶⁹.

4. L'utilisation d'un service de confiance désigné conformément au paragraphe 1 est reconnue comme une preuve de [la qualité des données qui lui sont associées].

5. Le paragraphe 4 ne limite pas la possibilité pour quiconque :

a) D'établir par tout autre moyen la fiabilité [d'une méthode] [d'un service de confiance] aux fins des articles [16 à 22] ; ou

b) D'apporter des preuves de la non-fiabilité [d'une méthode] [d'un service de confiance] désigné[e] en vertu du paragraphe 1.

Article 25. Responsabilité des prestataires de services de confiance

1. Les prestataires de services de confiance sont tenus responsables des dommages causés intentionnellement ou par négligence à quiconque en raison de manquements aux obligations qui leur incombent [dans le cadre de la prestation de leurs services] [en vertu [de l'article 14] [du présent instrument]].

2. Nonobstant les dispositions du paragraphe 1, les prestataires de services de confiance ne sont pas tenus responsables des dommages découlant d'une utilisation d'un service de confiance dans la mesure où :

a) Cette utilisation dépasse les limitations fixées [en ce qui concerne l'objet ou la valeur des transactions pour lesquelles le service de confiance peut être utilisé] ; et

b) Ils ont fourni [[aux utilisateurs⁷⁰ ou] aux tiers]⁷¹ des moyens raisonnablement accessibles de déterminer ces limitations⁷².

⁶⁵ Le paragraphe 2 est une disposition de non-discrimination géographique fondée sur l'article 12 de la LTSE, dont l'objet est de permettre la reconnaissance internationale des services de confiance.

⁶⁶ Ce projet de disposition ménage la possibilité de mener une évaluation *ex ante* de la fiabilité des services de confiance.

⁶⁷ Le Groupe de travail voudra peut-être préciser si et comment les éléments énumérés au projet d'article 23 s'appliquent à la désignation d'un service de confiance fiable conformément au projet d'article 24 (c'est-à-dire, si la personne, l'organe ou l'autorité qui procède à la désignation est tenu(e) de prendre en compte les circonstances visées au paragraphe 1 a) de l'article 23).

⁶⁸ Cette disposition a été révisée afin de tenir compte des modifications dont le Groupe de travail est convenu à sa cinquante-huitième session (A/CN.9/971, par. 76).

⁶⁹ Le paragraphe 3 est une disposition de non-discrimination géographique fondée sur l'article 12 de la LTSE, dont l'objet est de permettre la reconnaissance internationale des services de confiance.

⁷⁰ En cas d'emploi du terme « utilisateur », le Groupe de travail voudra peut-être envisager de le définir.

⁷¹ Le Groupe de travail voudra peut-être se demander s'il conviendrait de mentionner, dans le projet d'article, les parties qui devraient être en mesure de déterminer les limitations et, le cas échéant, si ces parties correspondraient à celles devant lesquelles les prestataires de services de confiance peuvent être tenus responsables.

⁷² Cette disposition est inspirée de l'article 9-1 d) ii) de la LTSE.

Chapitre IV. Aspects internationaux

*Article 26. Reconnaissance internationale de la gestion de l'identité et des services de confiance*⁷³

1. [Les systèmes de gestion de l'identité exploités] [Les justificatifs d'identité délivrés] ou les services de confiance fournis en dehors [de l'État adoptant] ont les mêmes effets juridiques dans [l'État adoptant] que [les systèmes de gestion de l'identité exploités] [les justificatifs d'identité délivrés] ou les services de confiance fournis dans [l'État adoptant], s'ils offrent [un niveau de fiabilité substantiellement équivalent] [le même niveau de fiabilité]^{74, 75}.

2. Pour déterminer si [des justificatifs d'identité] [un système de gestion de l'identité] ou un service de confiance offrent [un niveau de fiabilité substantiellement équivalent] [le même niveau de fiabilité], il est tenu compte [des normes internationalement reconnues].

Article 27. Coopération

[Toute personne, tout organe ou toute autorité, de droit public ou privé, indiqué[e] par l'État adoptant] [coopère] [peut coopérer] avec des entités étrangères en échangeant des informations, des données d'expérience et des bonnes pratiques ayant trait à la gestion de l'identité et aux services de confiance, notamment en ce qui concerne :

- a) La certification des systèmes de gestion de l'identité et des services de confiance ; et
- b) La définition des niveaux de garantie des systèmes de gestion de l'identité et des niveaux de fiabilité des services de confiance.

⁷³ Cette disposition reproduit les paragraphes 2 et 3 du projet d'article 19 qui figure dans le document [A/CN.9/WG.IV/WP.157](#). Le Groupe de travail voudra peut-être se demander s'il conviendrait de la conserver, compte tenu de l'insertion de paragraphes sur la non-discrimination géographique aux articles 10, 11, 23 et 24.

⁷⁴ Dans la mesure où cette disposition est inspirée du paragraphe 2 de l'article 12 de la LTSE, le terme « niveau de fiabilité » n'y revêt pas nécessairement le même sens que dans d'autres projets de dispositions de l'instrument.

⁷⁵ Le Groupe de travail voudra peut-être se demander si cette disposition suppose l'application au système de gestion de l'identité ou au service de confiance étranger de l'ensemble des règles de droit de l'État adoptant, y compris les dispositions du projet d'instrument et les règles qui régissent les limitations de responsabilité prévues par des dispositions législatives ou contractuelles.