Nations Unies A/CN.9/WG.IV/WP.153

Assemblée générale

Distr. limitée
6 septembre 2018
Français
Original : anglais

Commission des Nations Unies pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Cinquante-septième session
Vienne, 19-23 novembre 2018

Questions juridiques liées à la gestion de l'identité et aux services de confiance

Note du Secrétariat

Table des matières

V.18-05869 (F)

Merci de recycler

I. Introduction

1. La présente note illustre certains aspects de quelques-uns des thèmes que le Groupe de travail a jugés pertinents pour l'examen des questions juridiques liées à la gestion de l'identité et aux services de confiance (A/CN.9/936, par. 58). Destinée à faciliter la poursuite des débats, elle vise en particulier à mettre en lumière les problèmes clefs et à proposer des solutions envisageables, sans restreindre la possibilité d'examiner des thèmes supplémentaires ou d'en examiner certains conjointement, selon le cas. Le document de travail A/CN.9/WG.IV/WP.154 illustre certains aspects d'autres thèmes que le Groupe de travail a jugés pertinents pour l'examen des questions juridiques liées à la gestion de l'identité et aux services de confiance.

2. Un historique des travaux du Groupe de travail sur les questions juridiques liées à la gestion de l'identité et aux services de confiance est présenté dans le document de travail A/CN.9/WG.IV/WP.152 (par. 6 à 17). On y trouvera également une liste d'autres documents pertinents (par. 19).

II. Questions pertinentes pour de futurs travaux sur les aspects juridiques de la gestion de l'identité et des services de confiance

A. Portée des travaux

3. Comme suite à une recommandation du Groupe de travail, la Commission a prié celui-ci de mener des travaux sur les questions juridiques relatives à la gestion de l'identité et aux services de confiance, en vue d'élaborer un texte visant à faciliter la reconnaissance internationale de la gestion de l'identité et des services de confiance. Elle a formulé sa demande dans des termes suffisamment larges pour prendre en compte des aspects du traitement juridique de la gestion de l'identité et des services de confiance en plus de ceux qui ont déjà été recensés (voir ci-dessus, par. 1).

4. Les mécanismes juridiques destinés à la reconnaissance internationale de la gestion de l'identité et des services de confiance jouent un rôle essentiel dans l'instauration d'un cadre juridique favorable à l'économie numérique, tandis que leur absence peut contribuer à élargir encore la fracture numérique. Le Groupe de travail voudra donc peut-être réfléchir, dans une perspective plus large, aux incidences que ses travaux pourraient avoir sur la réduction de la fracture numérique.

5. À cet égard, il voudra peut-être se demander si l'absence d'un cadre juridique interne propice à l'utilisation de la gestion de l'identité et des services de confiance peut constituer un obstacle à leur reconnaissance juridique internationale. Le cas échéant, il voudra peut-être déterminer les dispositions juridiques qu'il conviendrait d'adopter dans la législation interne afin de permettre la pleine reconnaissance juridique internationale de la gestion de l'identité et des services de confiance, et réfléchir au type de texte juridique (traité et/ou loi type, par exemple) qui serait le plus approprié pour atteindre cet objectif.

6. Par ailleurs, la reconnaissance juridique internationale de l'identité a des points communs avec la reconnaissance juridique de l'identité entre différents systèmes de gestion de l'identité, indépendamment des éléments d'extranéité. Le Groupe de travail voudra donc peut-être se demander s'il convient d'envisager un mécanisme qui permette la reconnaissance juridique entre les systèmes de gestion de l'identité, en tenant compte, lorsqu'il y a lieu, des éléments d'extranéité. Le cas échéant, le résultat de ses travaux pourrait offrir des orientations concernant la gestion de l'identité aux niveaux tant national qu'international.

1. Identité fondamentale et identité transactionnelle

7. Le Groupe de travail voudra peut-être se rappeler qu'une distinction avait été proposée entre la détermination primaire et la détermination secondaire de l'identité (A/CN.9/WG.IV/WP.149, par. 29).

8. La détermination primaire de l'identité, où identité fondamentale, correspond à l'attribution de l'identité dans le contexte d'origine de l'entité et au moment de son origine. En tant que telle, l'identité fondamentale est généralement unique et irremplaçable. À titre d'exemple, on peut citer : l'inscription d'une personne physique par une autorité publique dans les registres et statistiques de l'état civil ; l'inscription d'une personne morale dans un registre spécialisé, comme un registre des sociétés commerciales, par l'autorité compétente ; et l'attribution à un objet numérique d'un identifiant d'objet numérique.

9. La détermination secondaire de l'identité, ou identité transactionnelle, fait référence à l'utilisation de l'identité pour remplir une fonction précise (conclusion d'un contrat, distribution d'espèces depuis un guichet automatique de banque, et délivrance d'un certificat par une autorité publique, par exemple).

10. Si l'identité fondamentale n'est pas couramment utilisée en tant que telle dans les opérations commerciales, elle peut l'être par les fournisseurs d'identité lorsqu'ils établissent une identité de transaction. Par exemple, les dispositions de la CNUDCI relatives aux signatures électroniques exigent l'identification du signataire. Dans certains cas, celle-ci peut reposer sur l'utilisation d'un processus de justification et d'authentification de l'identité qui établit l'identité sur la base de justificatifs de l'identité fondamentale. Par conséquent, la reconnaissance juridique de l'identité fondamentale entre pays et entre systèmes de gestion de l'identité pourrait se révéler utile, voire nécessaire.

2. Entités pertinentes

11. Le Groupe de travail a mené un examen préliminaire des types d'entités pertinentes pour ses travaux (A/CN.9/936, par. 63 à 65), c'est-à-dire des entités auxquelles le résultat de ses travaux pourrait s'appliquer. L'importance des personnes physiques et morales qui jouent un rôle dans le commerce, notamment au niveau international, a généralement été admise. Les entités sans personnalité morale propre, mais qui présentent une importance pour les activités commerciales, pourraient également être prises en considération. Par exemple, dans les pays les moins avancés, les commerçants du secteur informel pourraient utiliser l'identité mobile comme principal moyen d'identification.

12. La prise en compte des entités publiques peut se justifier par l'importance que revêtent pour le commerce international certaines opérations entre entreprises et États, d'une part, et entre États, d'autre part, comme les guichets uniques internationaux pour les opérations douanières. Le Groupe de travail voudra peut-être se demander si la participation des entités publiques aux opérations de gestion de l'identité ou aux services de confiance soulève des questions particulières, en gardant à l'esprit, notamment, l'application des principes de la neutralité technologique (voir ci-dessous, par. 38 à 40), de l'autonomie des parties (voir ci-dessous, par. 41 à 47) et de la proportionnalité entre les moyens d'identification électronique et la fonction recherchée (voir ci-dessous, par. 46).

13. Différents avis ont été exprimés concernant la question de savoir si l'identification des objets physiques et numériques entrait dans le champ des travaux du Groupe de travail. Selon un avis, ces objets devaient en être exclus, car ils n'avaient pas de personnalité juridique et ne pouvaient pas être tenus responsables à titre autonome. Toutefois, l'avis a aussi été exprimé que l'identification n'exigeait pas de personnalité juridique autonome ni l'attribution d'une responsabilité à l'objet identifié (A/CN.9/936, par. 64).

14. Selon un autre avis encore, le Groupe de travail pourrait se pencher sur l'identification des objets après avoir traité celle des personnes (A/CN.9/936, par. 65). Il convient à cet égard de noter que, dans le modèle de l'« Internet des objets », les objets sont une source majeure de mégadonnées, et que la fiabilité de l'attribution des données pourrait se révéler particulièrement importante dans le cadre de ce modèle. Des dispositifs médicaux, par exemple, sont de plus en plus souvent utilisés afin de surveiller à distance l'état d'un patient pendant ses activités quotidiennes. Il est essentiel de faire en sorte que les informations produites par ces dispositifs soient bien attribuées au patient auquel elles se rapportent. De même, il est nécessaire d'effectuer un suivi des médicaments non seulement au moment de leur consommation, mais aussi tout au long de leur cycle de production, afin d'en assurer la bonne identification et d'en garantir l'origine et la composition. Il est essentiel d'identifier de manière fiable aussi bien le médicament que ses composants.

B. Définitions

15. Le Groupe de travail voudra peut-être se référer au document A/CN.9/WG.IV/WP.150 où figure une liste de termes et notions relatifs à la gestion de l'identité et aux services de confiance qui pourraient lui être utiles pour ses délibérations. Cette liste ne l'empêche pas d'élaborer des définitions de termes pertinents au fur et à mesure de ses travaux.

16. En ce qui concerne la gestion de l'identité, les définitions suivantes, qui sont tirées du document susmentionné, pourraient lui être particulièrement utiles pour débattre des questions abordées dans la présente note.

17. Par « identité », on entend a) des informations relatives à un sujet donné qui, prenant la forme d'un ou plusieurs attributs, lui permettent d'être identifié de manière suffisante dans un contexte particulier ; b) un ensemble d'attributs concernant une personne qui la décrivent de façon unique dans un contexte donné (A/CN.9/WG.IV/WP.150, par. 31).

18. Le Groupe de travail voudra peut-être étudier le lien entre ces définitions et les notions d'identité fondamentale et d'identité transactionnelle (voir ci-dessus, par. 7 à 10), ainsi que l'intérêt de ces notions dans l'optique de ses futurs travaux. À cet égard, il voudra peut-être préciser si l'unicité est un attribut de l'identité fondamentale.

19. Par « gestion de l'identité », on entend un ensemble de processus appliqués pour gérer l'identification, l'authentification et l'autorisation de personnes physiques, de personnes morales, de dispositifs ou d'autres sujets dans un univers connecté (A/CN.9/WG.IV/WP.150, par. 35).

20. Par « système d'identité », on entend un environnement en ligne pour les opérations de gestion de l'identité régi par un ensemble de règles de fonctionnement (également appelé cadre de confiance) dans lequel particuliers, organisations, services et appareils peuvent se faire mutuellement confiance parce que des sources faisant autorité établissent et authentifient leur identité respective (A/CN.9/WG.IV/WP.150, par. 38).

21. Par « transaction liée à l'identité », on entend toute transaction impliquant deux ou plusieurs participants qui consiste à établir, vérifier, émettre, asserter, révoquer ou communiquer une identité, ou à s'y fier (A/CN.9/WG.IV/WP.150, par. 39).

22. Le Groupe de travail voudra peut-être examiner les notions de « gestion de l'identité », de « systèmes d'identité » et de « transaction liée à l'identité » afin de déterminer si, dans ses travaux sur la reconnaissance juridique de la gestion de l'identité, il devrait faire référence aux systèmes d'identité, aux transactions liées à l'identité, ou à ces deux notions (voir ci-dessous, par. 57 à 59).

23. Par « niveau de garantie », on entend le degré de confiance dans les processus d'identification et d'authentification, à savoir : a) le degré de confiance dans le processus de validation utilisé pour établir l'identité d'une entité à qui un justificatif a été délivré ; et b) le degré de confiance dans le fait que l'entité qui utilise le justificatif est celle à qui le justificatif a été délivré. La garantie reflète la fiabilité des méthodes, des processus et des technologies utilisés (A/CN.9/WG.IV/WP.150, par. 42).

24. Le Groupe de travail, lorsqu'il examinera la question du « niveau de garantie », voudra peut-être se référer à la définition de cette notion (voir A/CN.9/WG.IV/WP.154, par. 10 à 19). Ce faisant, il voudra peut-être également tenir compte de la définition suivante du « niveau de garantie » : « degré de confiance dans le lien qui lie une entité et l'identité présentée » (A/CN.9/WG.IV/WP.150, par. 12), ainsi que de la note se rapportant à cette définition, dans laquelle il est expliqué que les notions de « garantie d'identité » et de « garantie d'authentification » peuvent être considérées comme des composantes distinctes du concept global de « niveau de garantie ».

C. Principes généraux

25. Le Groupe de travail a recensé les principes généraux suivants comme étant pertinents pour ses travaux sur les aspects juridiques de la gestion de l'identité et des services de confiance : non-discrimination à l'égard de l'utilisation de moyens électroniques ; équivalence fonctionnelle ; neutralité technologique ; et autonomie des parties (A/CN.9/936, par. 67).

1. Non-discrimination à l'égard de l'utilisation de moyens électroniques

26. Le principe de non-discrimination à l'égard de l'utilisation de moyens électroniques est bien établi dans les textes de la CNUDCI. Dans le contexte de la gestion de l'identité et des services de confiance, ce principe pourrait être formulé comme suit[1] :

> La vérification de l'identité au moyen de [justificatifs d'] [systèmes de gestion de l'] identité et de services de confiance n'est pas privée de ses effets juridiques, de sa validité ou de sa force exécutoire au seul motif que ces [justificatifs d'][systèmes de gestion de l']identité et ces services de confiance se présentent sous une forme électronique.

27. Ce projet de disposition propose de choisir entre les « justificatifs d'identité » et les « systèmes de gestion de l'identité », selon qu'il conviendra de faire référence à l'utilisation de justificatifs ou de l'ensemble du système de gestion de l'identité aux fins de l'identification (voir ci-dessous, par. 57 à 59).

2. Équivalence fonctionnelle

28. Dans le domaine du commerce électronique, le principe de l'équivalence fonctionnelle définit les exigences auxquelles un document, une méthode ou un processus électronique doit satisfaire pour remplir les mêmes fonctions que son équivalent papier.

[1] On a inséré des projets de dispositions à des fins uniquement illustratives, sans préjuger des recommandations du Groupe de travail à la Commission concernant la forme que ses travaux pourraient prendre, ni des décisions de la Commission à cet égard.

a) Gestion de l'identité

29. Une règle d'équivalence fonctionnelle en matière de gestion de l'identité pourrait se lire comme suit :

> Lorsque la loi exige ou permet l'identification d'une entité, cette exigence est satisfaite, dans le cas de la gestion de l'identité [électronique] [numérique], si une méthode fiable est employée pour [vérifier les attributs [pertinents] de cette entité].

30. L'effet recherché dans une telle disposition serait de transposer à un environnement électronique les exigences applicables à l'identification dans un système papier. Le Groupe de travail voudra peut-être envisager d'insérer le mot « [pertinents] » afin d'indiquer que seuls les attributs qui sont exigés pour l'identification hors ligne seraient nécessaires au succès de l'identification en ligne. Il voudra peut-être également préciser s'il convient de faire référence à « l'identité électronique » ou à « l'identité numérique ».

31. On pourrait donner des orientations supplémentaires concernant les éléments à prendre en compte pour déterminer la fiabilité de la méthode, y compris : a) les accords contractuels, s'ils sont autorisés par la loi applicable ; b) la certification par un tiers et l'autocertification ; et c) les niveaux de garantie. En particulier, la référence à l'utilisation d'une « méthode fiable » dans une disposition relative à l'équivalence fonctionnelle pourrait consister à exiger l'utilisation d'une méthode qui fournisse un niveau de fiabilité équivalent lors de l'identification en ligne et hors ligne.

32. Pour établir une règle d'équivalence fonctionnelle en matière de gestion de l'identité, il pourrait être intéressant de se pencher sur les situations dans lesquelles celle-ci intervient. À cet égard, il convient de noter que l'identification peut être nécessaire à diverses fins ou fonctions. Elle a notamment pour objet le respect de la réglementation. À titre d'exemple, on peut citer l'application de la règle « Connaissez votre client » dans les domaines de la finance et des télécommunications et dans d'autres secteurs d'activité. Ce type d'usage trouve une autre illustration dans le domaine de la passation électronique des marchés, où l'identification correcte des fournisseurs et des clients potentiels est nécessaire pour prévenir la fraude et la collusion et faire appliquer les mesures d'exclusion.

33. L'identification a également pour objet d'établir la validité d'un document commercial. Par exemple, la loi applicable à un connaissement peut exiger l'identification de certaines parties, comme c'est le cas à l'article 15 de la Convention des Nations Unies sur le transport de marchandises par mer (Hambourg, 1978) (les « Règles de Hambourg »[2]) ainsi qu'à l'article 36 de la Convention des Nations Unies sur le contrat de transport international de marchandises effectué entièrement ou partiellement par mer (New York, 2008) (les « Règles de Rotterdam »[3]).

34. Par ailleurs, les parties à une opération en ligne peuvent convenir, à des fins de gestion des risques, de l'utilisation de certaines procédures et méthodes pour s'identifier mutuellement avec exactitude, en l'absence de toute obligation légale de le faire. La source de cette obligation d'identification est contractuelle.

35. On pourrait prendre une décision de principe consistant à adopter des normes plus strictes en matière d'identification, afin d'améliorer l'application des obligations dans ce domaine, dans des situations où l'identification hors ligne, même si elle est utilisée, ne donne pas pleinement satisfaction. Le Groupe de travail voudra peut-être étudier l'interaction entre l'adoption d'une disposition relative à l'équivalence fonctionnelle en matière d'identification et l'éventuelle introduction d'exigences plus

---

[2] Nations Unies, *Recueil des Traités*, vol. 1695, nº 29215, p. 3.

[3] Résolution 63/122 de l'Assemblée générale, annexe.

strictes pour l'identification en ligne que celles applicables dans l'environnement hors ligne.

b) Services de confiance

36. On trouve dans les textes de la CNUDCI des règles d'équivalence fonctionnelle pour certains services de confiance, à savoir pour les signatures électroniques, à l'article 7 de la Loi type de la CNUDCI sur le commerce électronique (LTCE)[4], à l'article 6 de la Loi type de la CNUDCI sur les signatures électroniques (LTSE)[5], à l'article 9-3 de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (New York, 2005) (CCE)[6] et à l'article 9 de la Loi type de la CNUDCI sur les documents transférables électroniques[7], ainsi que pour la conservation et l'archivage, à l'article 10 de la LTCE. Le Groupe de travail voudra peut-être se demander s'il convient d'élaborer des dispositions spécifiques pour le résultat de chaque type de services de confiance, ou s'il est possible ou souhaitable de concevoir plutôt une règle générale d'équivalence fonctionnelle (voir A/CN.9/WG.IV/WP.154, par. 58).

37. Il voudra peut-être également se demander s'il serait souhaitable d'élaborer une disposition relative à l'attribution des informations d'identité, ou si la règle d'équivalence fonctionnelle serait suffisante, dans la mesure où ces informations seraient attribuées à la même entité que dans un environnement hors ligne et où, dans tous les cas, elles ne seraient pas attribuées au fournisseur de services d'identité. L'article 13 de la LTCE offre un exemple de disposition relative à l'attribution.

3. Neutralité technologique

38. Le principe de la neutralité technologique est un élément essentiel des textes de la CNUDCI et de nombreux autres textes législatifs en rapport avec l'utilisation des communications électroniques. Dans le contexte de la gestion de l'identité et des services de confiance, il serait peut-être nécessaire de fournir des orientations concernant la configuration minimale requise en faisant référence aux propriétés du système plutôt qu'à des technologies spécifiques (A/CN.9/936, par. 69). Si l'on optait plutôt pour une approche axée sur les opérations (voir ci-dessous, par. 57 à 59), il faudrait peut-être donner des orientations au sujet des exigences minimales pour les opérations liées à l'identité en faisant référence aux propriétés des opérations. Afin d'appliquer le principe de la neutralité technologique dans le contexte des services de confiance, il pourrait être nécessaire de définir les objectifs spécifiques de chaque service de confiance, sans imposer l'utilisation d'une technologie particulière pour les atteindre.

39. Une disposition relative à l'égalité de traitement des technologies, méthodes et systèmes employés pour la gestion de l'identité et les services de confiance pourrait se lire comme suit :

> Aucune disposition du présent [projet d'instrument] n'est appliquée de manière à exclure, restreindre ou priver d'effets juridiques [une technologie, une méthode ou un système] quelconque utilisé pour la gestion de l'identité et les services de confiance satisfaisant aux exigences mentionnées dans le présent [projet d'instrument][, ou autrement satisfaisant aux exigences de la loi applicable].

---

[4] Publication des Nations Unies, numéro de vente : F.99.V.4.
[5] Publication des Nations Unies, numéro de vente : F.02.V.8.
[6] Nations Unies, *Recueil des Traités*, vol. 2898.
[7] Publication des Nations Unies eISBN 978-92-1-362735-8.

40. Les mots « ou autrement satisfaisant aux exigences de la loi applicable », qui se trouvent à l'article 3 de la LTSE[8], font référence à la possibilité qu'une loi autre que le projet d'instrument prescrive, dans certains cas précis, l'application d'exigences différentes de celles prévues dans le projet d'instrument.

4. Autonomie des parties

41. Le principe de l'autonomie des parties a notamment pour conséquence de rendre optionnelle l'utilisation de la gestion de l'identité et des services de confiance. Alors qu'il peut être pleinement mis en œuvre dans le contexte des services commerciaux, son application peut, pour des raisons politiques, être limitée pour ce qui est de l'accès aux services fournis par des entités publiques ou de l'interaction avec ces entités.

42. Une disposition relative à l'utilisation optionnelle de la gestion de l'identité et des services de confiance pourrait se lire comme suit :

> 1. Aucune disposition du présent [projet d'instrument] n'oblige une entité à utiliser ou à accepter des [justificatifs d'] [systèmes de gestion de l']identité et des services de confiance sans son consentement.
>
> 2. Le consentement d'une entité à utiliser des [justificatifs d'] [systèmes de gestion de l']identité et des services de confiance peut être déduit de son comportement [et d'autres circonstances].
>
> [Le paragraphe 1 ne s'applique pas à …]

43. Ce projet de disposition propose de choisir entre les « justificatifs d'identité » et les « systèmes de gestion de l'identité », selon qu'il conviendra de faire référence à l'utilisation de justificatifs ou de l'ensemble du système de gestion de l'identité aux fins de l'identification (voir aussi ci-dessous, par. 57 à 59).

44. Dans le second paragraphe du projet de disposition, les mots « [et d'autres circonstances] » ont été insérés afin de tenir compte des cas où l'entité n'est pas capable de comportement autonome (s'il s'agit d'un objet physique ou numérique, par exemple). En pareil cas, le consentement ne sera pas attribuable à l'entité, mais à la personne physique ou morale qui en a le contrôle.

45. L'application du principe de l'autonomie des parties est soumise à des limitations énoncées dans la loi impérative (A/CN.9/936, par. 72). Ces limitations sont particulièrement importantes, car les exigences législatives satisfaites par l'utilisation de la gestion de l'identité et des services de confiance sont souvent impératives. En conséquence, il est proposé d'adopter une formulation de ce principe basée sur l'article 5 de la LTSE :

> Il est possible de déroger aux dispositions du présent [projet d'instrument] ou d'en modifier les effets par convention, à moins que cette convention soit invalide ou sans effets en vertu de la loi applicable.

46. Une autre application du principe de l'autonomie des parties a trait à la liberté de choisir la gestion de l'identité et les services de confiance les mieux adaptés à la fonction recherchée par les parties (« principe de proportionnalité »). La liberté du choix du type de services est aussi étroitement liée au principe de la neutralité technologique.

47. Le principe de l'autonomie des parties vise également à appuyer l'exécution des accords contractuels, tels que les règles de fonctionnement relatives à la gestion de l'identité et les règles de fonctionnement et cadres relatifs aux services de confiance. Par conséquent, les règles de fonctionnement pourraient être particulièrement importantes dans le contexte de la fédération de systèmes de gestion de l'identité

[8] *Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation* (publication des Nations Unies, numéro de vente : F.02.V.8), par. 107.

(voir A/CN.9/WG.IV/WP.154, par. 39). Dans la pratique, par « fédération d'identité », on entend un groupe de fournisseurs d'identité, de parties utilisatrices, de sujets et d'autres entités qui acceptent d'opérer dans le cadre de politiques, de normes et de technologies compatibles spécifiées dans des règles de fonctionnement (ou cadre de confiance) afin que les informations communiquées par les fournisseurs d'identité puissent être comprises et utilisées en confiance par les parties utilisatrices (A/CN.9/WG.IV/WP.150, par. 28).

5. Obligation d'identification

48. Un autre principe général commun aux textes de la CNUDCI sur le commerce électronique réside dans le fait que le droit matériel, c'est-à-dire le droit généralement applicable aux opérations commerciales, n'est pas touché.

49. Dans le contexte de la gestion de l'identité et des services de confiance, ce principe signifie que la législation relative à la gestion de l'identité n'introduit aucune nouvelle obligation d'identification, que la législation relative aux services de confiance n'introduit aucune nouvelle obligation d'utiliser un type particulier de services de confiance, et que les obligations existantes demeurent inchangées.

50. On pourrait envisager le projet de disposition suivant :

> Aucune disposition du présent [projet d'instrument] n'impose à une partie l'obligation [de vérifier l'identité d'] [d'identifier] une autre entité ou d'utiliser un service de confiance.

6. Interprétation uniforme

51. Les textes de la CNUDCI comportent généralement une disposition qui fait référence à leur origine uniforme et énonce une obligation d'interprétation uniforme. Cette disposition a pour objet d'assurer le maintien de l'uniformité lors de l'interprétation et de l'application du texte législatif.

52. On pourrait envisager le projet de disposition suivant :

> 1. Pour l'interprétation du présent [projet d'instrument], il sera 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 [projet d'instrument] et qui ne sont pas expressément tranchées par lui seront réglées selon les principes généraux dont il s'inspire ou, à défaut de ces principes, conformément à la loi applicable en vertu des règles du droit international privé.

53. Dans le second paragraphe du projet de disposition, la référence à « la loi applicable en vertu des règles du droit international privé » peut être particulièrement utile dans un contexte international.

D. Exigences et mécanismes de reconnaissance juridique

54. D'un point de vue général, la reconnaissance juridique peut s'entendre comme la définition des exigences auxquelles il faut satisfaire pour obtenir un statut juridique dans un pays. L'octroi de la reconnaissance juridique au niveau interne peut nécessiter la formulation de règles de droit matériel.

55. La reconnaissance juridique internationale peut s'entendre comme : a) l'octroi dans le pays requis du même statut juridique que dans le pays d'origine ; b) l'octroi du même statut juridique que dans le pays requis, indépendamment de tout élément d'extranéité ; ou c) la définition des effets de la reconnaissance juridique dans un

instrument spécifique. Par ailleurs, la reconnaissance juridique internationale peut être mutuelle, c'est-à-dire réciproque, ou unilatérale. Dans les deux cas, elle peut être soumise à conditions.

56. La reconnaissance juridique des dispositifs de gestion de l'identité et des services de confiance est la question centrale des travaux du Groupe de travail. Elle doit permettre, sur le plan juridique, la mise en œuvre de propriétés techniques telles que l'interopérabilité des justificatifs d'identité et des services de confiance ou la portabilité de l'identité et de la confiance entre différents dispositifs de gestion de l'identité. Comme indiqué plus haut (par. 6), la reconnaissance juridique internationale de l'identité a des points communs avec la reconnaissance juridique de l'identité entre différents systèmes de gestion de l'identité, indépendamment des éléments d'extranéité.

57. La reconnaissance juridique peut porter sur les systèmes et les dispositifs de gestion de l'identité et de services de confiance. Si tel était le cas, il faudrait peut-être fournir des orientations juridiques concernant les caractéristiques que ces systèmes et dispositifs devraient présenter pour obtenir la reconnaissance juridique. En conséquence, les résultats de ces systèmes et dispositifs qui seraient utilisés dans les opérations, à savoir des moyens d'identification électronique et des services de confiance spécifiques, pourraient également bénéficier de la reconnaissance juridique.

58. La reconnaissance juridique peut également porter sur les opérations facilitées par l'utilisation de la gestion de l'identité et des services de confiance. Le cas échéant, il serait peut-être nécessaire de fournir des orientations juridiques concernant les conditions à satisfaire pour que les justificatifs et vérifications d'identité et le résultat des services de confiance puissent bénéficier de la reconnaissance juridique. Les textes existants de la CNUDCI sur le commerce électronique traitent principalement des questions liées aux opérations. Par exemple, la LTSE a surtout pour objet l'utilisation des signatures électroniques dans les opérations, et ne traite que partiellement des caractéristiques des systèmes de signatures électroniques.

59. Le Groupe de travail voudra peut-être se demander si ses travaux sur la reconnaissance juridique devraient porter sur les systèmes et dispositifs de gestion de l'identité et de services de confiance, sur les opérations facilitées par l'utilisation de la gestion de l'identité et des services de confiance, ou sur ces deux aspects.

60. Il voudra peut-être également se demander s'il devrait envisager uniquement un mécanisme de reconnaissance juridique internationale ou également s'intéresser à la reconnaissance juridique entre différents systèmes au niveau national.

1. Gestion de l'identité

a) Reconnaissance juridique *ex ante*

61. En vue d'assurer la reconnaissance juridique des dispositifs de gestion de l'identité, une solution consiste à envisager d'établir au préalable une liste des dispositifs reconnus ainsi que les conditions d'inscription sur cette liste. Ce type de démarche nécessite généralement la mise en place d'un mécanisme institutionnel d'évaluation et d'octroi de licences centralisé pour évaluer les dispositifs de gestion de l'identité.

62. Cette approche, qui serait également utilisable pour les services de confiance, pourrait permettre de savoir de manière claire et prévisible quels sont les dispositifs et services qui peuvent être utilisés par différents systèmes et dans différents pays. Toutefois, elle risquerait de priver de reconnaissance juridique des dispositifs et services qui, bien qu'étant utilisés, ne figurent pas sur la liste. De plus, selon son mode de gouvernance, elle ne permettrait pas nécessairement de réagir aussi rapidement aux faits nouveaux que l'évolution technologique pourrait l'exiger, ce qui

risquerait d'entraver l'innovation et de conduire à l'imposition d'exigences spécifiques à une technologie.

63. Pour établir le mécanisme institutionnel nécessaire à la mise en œuvre de cette approche, il faudrait définir les conditions pour devenir membre de l'entité d'évaluation, les critères d'évaluation des dispositifs de gestion de l'identité et les mécanismes d'actualisation de ces critères, le processus d'évaluation de la prise de décisions, et les sources de financement. En fonction d'un certain nombre de facteurs, notamment des arrangements institutionnels préexistants, la gouvernance du système d'octroi de licences pourrait être plus ou moins complexe et coûteuse.

64. Par ailleurs, un système d'octroi de licences centralisé pourra être plus efficace s'il fonctionne à une échelle relativement limitée et dans le cadre de larges initiatives d'intégration économique, mais pourra poser des problèmes s'il est mis en œuvre au niveau mondial, car il pourra alors nécessiter un niveau de coopération élevé de la part des membres.

65. La mise en place d'un tel système centralisé à l'échelle mondiale pourrait nécessiter l'adoption d'un traité ou autre instrument de droit international contraignant. Les avantages d'un mécanisme fondé sur un traité comprennent la prévisibilité et, éventuellement, une plus grande facilité d'application aux organismes publics ; parmi ses inconvénients figurent les coûts liés à l'établissement et au fonctionnement du mécanisme institutionnel, les frais demandés aux dispositifs participants, et la nécessité de recueillir l'appui d'un nombre suffisant d'États, de dispositifs et d'utilisateurs. Un mécanisme fondé sur un traité pourrait être particulièrement approprié pour garantir le financement des obligations financières à long terme, même s'il serait peut-être possible de recouvrer les coûts auprès des utilisateurs.

66. Les lois consacrées à la gestion de l'identité adoptées récemment prévoient l'exercice d'un contrôle centralisé pour la reconnaissance des effets juridiques des dispositifs de gestion de l'identité.

67. Le Règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (Règlement eIDAS)[9] est le seul texte de loi qui traite expressément des aspects internationaux de la gestion de l'identité. En particulier, l'article 6 de ce règlement permet l'utilisation du moyen d'identification électronique d'un État membre de l'Union européenne pour accéder à un service en ligne fourni par un organisme public d'un autre État membre, sous réserve de certaines conditions. L'une de ces conditions est que la délivrance de ce moyen d'identification électronique relève d'un schéma d'identification électronique qui soit notifié à la Commission européenne et satisfasse aux exigences d'interopérabilité énoncées par celle-ci. Le processus de notification comprend un examen par les pairs.

68. D'autres lois sur la gestion de l'identité abordent les questions qui s'y rapportent sans faire expressément mention des aspects internationaux. À cet égard, il convient de noter que, si le Règlement susmentionné n'a pas d'incidence sur les dispositifs de gestion de l'identité existants, mais vise à en assurer la reconnaissance juridique mutuelle entre États, les lois nationales sur la gestion de l'identité définissent quant à elles les conditions d'exploitation desdits dispositifs.

69. La loi béninoise nº 2017-20 comporte une section relative à la gestion de l'identité, qui traite des niveaux de garantie des schémas d'identification électronique, de l'éligibilité de ces schémas pour la notification, des atteintes à la sécurité, de la

[9] Règlement (UE) nº 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.

responsabilité et de l'interopérabilité. Les dispositions de cette section sont généralement inspirées des dispositions correspondantes du Règlement eIDAS.

70. La loi de l'État de Virginie sur la gestion de l'identité électronique[10] repose sur un mécanisme en vertu duquel les opérateurs du cadre de confiance de l'identité peuvent être exonérés de responsabilité s'ils remplissent un certain nombre d'exigences légales et réglementaires (voir A/CN.9/WG.IV/WP.154, par. 28 et 29). S'agissant des effets juridiques, l'utilisation d'un justificatif ou d'un attribut d'identité conforme aux normes établies par le Commonwealth de Virginie, aux représentations conventionnelles et aux règles de la fédération satisfait à toute exigence d'une procédure de sécurité ou d'attribution commercialement raisonnable prévue dans la loi uniforme sur les opérations électroniques et la loi uniforme sur les opérations informatiques[11].

71. La loi nº 205-2018 de l'État du Vermont porte création d'un nouveau type d'entité commerciale spécialisée, appelée « entreprise de protection des données personnelles » (Personal Information Protection Company), qui s'occupe de gérer des données personnelles, c'est-à-dire, plus précisément, de communiquer des éléments de données personnelles concernant tel ou tel consommateur à des tiers à des fins d'opérations, et de fournir des services de certification ou de validation concernant les données personnelles.

72. Cette loi énonce l'objectif selon lequel une entreprise de protection des données personnelles doit agir « au mieux des intérêts et pour la protection et le bien du consommateur » (art. 2451-3 B)). L'article 2450 dispose qu'une entreprise de ce type a une relation de confiance avec le consommateur lorsqu'elle lui fournit des services de protection des données personnelles.

73. Le Département de la régulation financière de l'État du Vermont, qui dispose d'un pouvoir de contrôle sur les entreprises de protection des données personnelles, peut adopter des règles concernant la fréquence et la teneur des rapports que ces entreprises doivent lui soumettre. Il peut également adopter des règles sur la protection et la préservation des données personnelles et sur l'échange de ces données avec des tiers.

b) Reconnaissance juridique *ex post*

74. Une autre approche consiste à envisager d'assurer la reconnaissance juridique à l'aide d'un mécanisme qui autorise généralement les échanges et ne détermine si des dispositifs de gestion de l'identité et des services de confiance sont propres à être utilisés qu'en cas de différend et sur la base de critères prédéfinis. Elle a été suivie dans les textes de la CNUDCI, comme l'illustre, par exemple, l'application du critère de fiabilité dit « a posteriori » (voir, par exemple, l'article 9-3 de la CCE).

75. Cette approche a le mérite d'offrir aux parties à l'opération un maximum de souplesse dans le choix des technologies et des méthodes. De plus, elle ne requiert pas la mise en place d'un mécanisme institutionnel, évitant ainsi les coûts susceptibles d'en découler, et permet une gestion décentralisée. Toutefois, elle a pour inconvénient de nécessiter le recours à un processus de décision par un tiers pour déterminer si un dispositif de gestion de l'identité ou un service de confiance est propre à être utilisé dans un contexte international, ce qui peut s'avérer long et coûteux et constituer pour les parties une source d'incertitude.

---

[10] *Virginia Electronic Identity Management Act*, Code de l'État de Virginie, art. 2.2-436, 2.2-437 et 59.1-550 à 59.1-555.

[11] Le *Uniform Electronic Transactions Act* (1999) et le *Uniform Computer Information Transactions Act*, adopté en 1999 et amendé en 2000 et 2002, sont des lois types établies par la National Conference of Commissioners on Uniform State Laws des États-Unis.

c) Reconnaissance juridique fondée sur l'établissement de correspondances

76. On peut également établir, à partir d'un modèle commun, des correspondances entre les systèmes de gestion de l'identité. Les exigences et les effets juridiques du processus de mise en correspondance seraient définis par le pays requis et le système de gestion de l'identité.

77. On pourrait mener ce processus en se référant aux descriptions génériques des niveaux de garantie, de manière à faire en sorte qu'il soit axé sur les résultats, ce qui, à son tour, préserverait l'application du principe de la neutralité technologique.

78. Le processus de mise en correspondance ne dépendrait pas de l'approbation d'une autorité centrale, mais pourrait être mené par toute partie intéressée, y compris des entités privées et commerciales. Son résultat serait publié sur une liste de confiance à diffusion publique.

79. Pour mener le processus de mise en correspondance, on pourrait tenir compte des éléments indiqués dans le Règlement d'exécution (UE) 2015/1502 de la Commission, qui s'inscrit dans le cadre du Règlement eIDAS. Ces éléments sont les suivants : inscription, gestion des moyens d'identification électronique, authentification, et gestion et organisation. Chaque élément comprend plusieurs sous-éléments. Le Groupe de travail voudra peut-être se demander dans quelle mesure des orientations devraient être fournies sur les prescriptions et les procédures à suivre pour mener le processus.

80. On pourrait illustrer par un exemple pratique la manière dont le processus de mise en correspondance pourrait fonctionner. Comme on l'a noté plus haut, la règle « Connaissez votre client » est largement répandue dans différents secteurs d'activité. Selon l'opération à effectuer, elle est généralement satisfaite par l'utilisation de justificatifs conformes au niveau de garantie « 2 » ou « substantiel », ou au niveau de garantie « 3 » ou « élevé » (voir A/CN.9/WG.IV/WP.154, par. 13 et 14, pour une description des différents niveaux de garantie).

81. Le plus souvent, cette règle ne pourra pas être satisfaite par des justificatifs d'identité délivrés dans un autre pays s'il n'existe pas de mécanisme de reconnaissance juridique des dispositifs de gestion de l'identité. L'établissement de correspondances entre justificatifs au regard des descriptions génériques des niveaux de garantie permettrait de vérifier si, pour une opération donnée, les justificatifs d'identité peuvent satisfaire aux exigences fixées pour le niveau de garantie nécessaire aux fins de la règle « Connaissez votre client ».

82. Par exemple, un opérateur de système d'identité A pourrait soumettre une certification selon laquelle son schéma d'identification électronique X est conforme au niveau de garantie 2 ou substantiel, et son schéma d'identification électronique Y au niveau de garantie 3 ou élevé, ce qui lui permettrait d'inscrire ces deux schémas sur la liste de confiance. La personne morale B qui souhaiterait réaliser une opération commerciale électronique avec l'institution financière C pourrait utiliser des justificatifs délivrés conformément au schéma X ou Y, selon les exigences de l'opération. L'institution financière C pourrait s'assurer que les deux schémas sont inscrits sur la liste de confiance, vérifier les niveaux de garantie correspondants, et accepter en conséquence les justificatifs délivrés conformément à ces schémas.

83. L'exemple précédent pourrait également être valable dans un contexte national, dans le cas où la législation interne ne préciserait pas les exigences applicables à la reconnaissance et à l'équivalence juridiques des schémas d'identification électronique.

84. Le mécanisme envisagé pourrait se fonder sur deux dispositions qui traiteraient, respectivement, des conditions d'inscription sur la liste de confiance et des effets de cette inscription.

85. Une disposition relative aux conditions d'inscription sur la liste de confiance pourrait se lire comme suit:

> 1. Lorsque des prestataires de services de gestion de l'identité ou de services de confiance ont l'intention de commencer à fournir leurs services, ils en notifient [...] [l'organisme de contrôle] et lui soumettent une certification.
>
> 2. Cette certification doit comporter au minimum les indications suivantes:
>
> a) Le type de rapport d'évaluation ;
>
> b) Les qualifications de l'entité d'évaluation ;
>
> c) Les spécifications techniques et formats utilisés pour la prestation de services, notamment en ce qui concerne les niveaux de garantie et les normes de messagerie.
>
> 3. [L'organisme de contrôle] [...] dresse, tient et publie des listes de confiance contenant des informations sur les prestataires de services de gestion de l'identité et de services de confiance et sur les services qu'ils fournissent.

86. Le Groupe de travail voudra peut-être se demander si, dans ce projet de disposition, le mot « certification » pourrait également faire référence à l'autocertification, ce qui serait peut-être approprié pour les services associés à un niveau de garantie faible (voir A/CN.9/WG.IV/WP.154, par. 3 à 9).

87. Le projet de disposition requiert la désignation d'une entité chargée de tenir la liste de confiance. Il pourrait s'agir d'une entité nationale, à condition d'établir un mécanisme de notification des entités nationales responsables.

88. En ce qui concerne les effets juridiques de l'inscription sur la liste de confiance, quelques éléments utiles pourraient être repris de l'article 12 de la LTSE. Par ailleurs, une disposition sur les effets de la reconnaissance juridique pourrait également intégrer le principe selon lequel des services d'identité et de confiance étrangers ne devraient être reconnus que s'ils offrent un niveau de garantie supérieur ou égal à celui exigé dans le pays où la reconnaissance est demandée (principe de réciprocité). On pourrait envisager la disposition suivante :

> Un service d'identité ou de confiance fourni à l'extérieur de [l'État requis] et inscrit sur la liste de confiance établie conformément à l'article [...] a les mêmes effets juridiques dans [l'État requis] qu'un service d'identité ou de confiance [[d'un niveau de garantie] [...] équivalent] fourni dans [l'État requis].

89. Le Groupe de travail voudra peut-être se demander s'il convient de fournir des orientations supplémentaires concernant l'utilisation du processus de mise en correspondance et de préciser la référence à la notion de niveau de garantie pour ce qui est de déterminer les effets juridiques d'un service d'identité ou de confiance étranger. À cet égard, il voudra peut-être réfléchir à l'opportunité de faire référence à la notion de « niveau de fiabilité substantiellement équivalent », qui figure à l'article 12 de la LTSE.

90. Lors de ses délibérations, le Groupe de travail voudra peut-être examiner divers exemples d'utilisation de dispositifs de gestion de l'identité. Dans la mesure où la question peut se poser à la fois pour les opérations internes et internationales, il souhaitera peut-être envisager les deux cas de figure. Il voudra peut-être se pencher, en particulier, sur les problèmes que semble souvent occasionner la nécessité de se conformer aux exigences impératives établies par les autorités publiques et parfois difficiles à intégrer dans les accords contractuels. Par exemple, comme l'illustre l'exemple ci-dessus (par. 80 à 83), une banque pourra vouloir connaître les dispositifs de gestion de l'identité dont l'utilisation permet de respecter la règle « Connaissez votre client ».

91. En résumé, les éléments qui pourraient être pertinents pour l'examen d'un mécanisme de reconnaissance juridique comprennent: la notification et l'inscription sur une liste de confiance ; les exigences à satisfaire, s'agissant notamment des niveaux de garantie ; l'utilisation d'une certification comme preuve que les exigences sont satisfaites ; un contrôle centralisé et une autorité d'octroi de licences ; un processus de mise en correspondance.

92. Le Groupe de travail voudra peut-être se demander sur quelle approche devrait se fonder le mécanisme de reconnaissance juridique. Ce faisant, il souhaitera peut-être en outre réfléchir à la question de savoir si ce mécanisme devrait s'appliquer uniquement au niveau international ou également entre différents systèmes dans un contexte national (voir ci-dessus, par. 60).

2. Services de confiance

93. En ce qui concerne les services de confiance, plusieurs mécanismes juridiques ont été conçus afin d'assurer la reconnaissance juridique des signatures électroniques. À cet égard, il convient de noter que, selon un avis, les signatures électroniques ne sont pas toutes le résultat de services de confiance, seules celles qui nécessitent l'intervention d'un tiers fournisseur de services de confiance pouvant être considérées comme tel. Selon un autre avis, toutes les signatures électroniques sont le résultat de services de confiance. Le Groupe de travail voudra peut-être éclaircir cette question.

94. Dans les textes de la CNUDCI, les règles d'équivalence fonctionnelle relatives aux signatures électroniques (voir ci-dessus, par. 36) prévoient la reconnaissance juridique au niveau interne.

95. Pour ce qui est de la reconnaissance juridique internationale, l'article 12 de la LTSE, qui se fonde sur la notion d'« équivalence substantielle »[12], prévoit que les éléments d'extranéité d'une signature électronique n'engendrent aucune discrimination. L'article 9-3 de la CCE définit des exigences pour l'établissement d'une équivalence fonctionnelle entre les signatures manuscrites et électroniques, mais ne détermine pas, en soi, le statut juridique de la signature dans le pays où la reconnaissance est demandée[13].

96. Un autre mécanisme destiné à la reconnaissance internationale des signatures électroniques repose sur la conclusion d'un accord international spécifique ou, en vertu d'une délégation de pouvoirs, d'un mémorandum d'accord. Par exemple, l'article 14 du Règlement eIDAS prévoit que les services de confiance fournis par des prestataires établis en dehors de l'Union européenne ne peuvent être reconnus comme équivalents, sur le plan juridique, à ceux fournis par des prestataires qualifiés établis dans l'Union européenne, que s'ils sont reconnus en vertu d'un accord international. Par ailleurs, l'article 19 de la loi indienne sur les technologies de l'information (2008) prévoit la reconnaissance des autorités de certification étrangères comme suit:

> « 1) Sous réserve des conditions et restrictions éventuelles prévues dans la réglementation, le Contrôleur peut, avec l'approbation préalable du Gouvernement central, et en publiant un avis dans l'*Official Gazette*, reconnaître toute autorité de certification étrangère comme autorité de certification aux fins de la présente Loi.

---

[12] Pour plus d'informations sur la notion d'équivalence substantielle, voir la publication de la CNUDCI intitulée *Promouvoir la confiance dans le commerce électronique : questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques* (publication des Nations Unies, numéro de vente : F.09.V.4), par. 158 à 161.

[13] Voir la Note explicative du secrétariat de la CNUDCI relative à la Convention sur l'utilisation des communications électroniques dans les contrats internationaux (publication des Nations Unies, numéro de vente : F.07.V.2), par. 156.

2) Lorsqu'une autorité de certification est reconnue en vertu du paragraphe 1, le certificat de signature électronique délivré par elle est valable aux fins de la présente Loi.

3) Le Contrôleur, s'il estime qu'une autorité de certification a enfreint l'une des conditions et restrictions sous réserve desquelles elle s'est vu octroyer la reconnaissance en vertu du paragraphe 1, peut, pour des raisons à consigner par écrit, et en publiant un avis dans l'*Official Gazette*, révoquer cette reconnaissance. »

97. Pour assurer la reconnaissance des signatures électroniques entre systèmes ou entre pays, on peut également faire appel à des méthodes basées sur l'infrastructure à clefs publiques (ICP), à savoir la reconnaissance croisée et la certification croisée[14]. La reconnaissance croisée est un dispositif d'interopérabilité selon lequel la partie intéressée se trouvant dans la zone couverte par une ICP peut utiliser des informations fournies par l'autorité d'une autre ICP pour procéder à une authentification dans la région de la première ICP[15]. Par certification croisée, on entend la pratique consistant à reconnaître la clef publique d'un autre prestataire de services de certification jusqu'à un degré convenu de fiabilité, normalement par contrat[16]. Ces méthodes contractuelles peuvent s'appuyer sur une disposition législative spécifique. Par exemple, l'article 43 de la loi colombienne n° 527 (1999) dispose ce qui suit:

Les certificats de signature numérique délivrés par des autorités de certification étrangères peuvent être reconnus aux mêmes conditions que celles requises par la loi pour la délivrance de certificats par les autorités de certification nationales, sous réserve que ces certificats soient reconnus par une autorité de certification nationale agréée qui garantit, de la même manière que pour ses propres certificats, l'exactitude des informations du certificat étranger, ainsi que leur validité et leur efficacité.

98. Les mécanismes ci-dessus existent depuis un certain temps, mais n'ont pas permis à ce jour la pleine reconnaissance internationale des signatures électroniques. La LTSE a été adoptée par un petit nombre d'États, souvent sans l'article 12, tandis que la participation des États à la CCE, bien qu'en constante augmentation, demeure limitée. Les mécanismes de reconnaissance mutuelle fondés sur la législation demandent beaucoup de temps et de ressources et ne sont utilisés que de manière restreinte. Enfin, la reconnaissance croisée et la certification croisée, qui reposent sur l'ICP, s'appliquent uniquement aux autorités de certification qui les négocient et elles risquent, si elles ne s'appuient pas sur des dispositions législatives dans tous les pays concernés, de ne pas satisfaire aux exigences législatives impératives.

---

[14] Pour plus d'informations sur la reconnaissance croisée et la certification croisée, voir la publication intitulée Promouvoir la confiance dans le commerce électronique, op. cit., par. 165 à 172.

[15] Ibid. par. 165.

[16] Ibid. par. 169.