

**Assemblée générale**

Distr. générale
5 mai 2015
Français
Original: anglais/français

**Commission des Nations Unies
pour le droit commercial international**
Quarante-huitième session
Vienne, 29 juin-16 juillet 2015

**Travaux futurs possibles dans le domaine du commerce
électronique – questions juridiques liées à la gestion de
l’identité et aux services de confiance**

**Proposition de l’Autriche, de la Belgique, de la France, de l’Italie
et de la Pologne**

Note du Secrétariat

Le Secrétariat a reçu la proposition de l’Autriche, de la Belgique, de la France, de l’Italie et de la Pologne. Le texte reçu est reproduit en annexe à la présente note sous la forme dans laquelle il a été reçu.

Le Secrétariat a reçu, de la Section de droit commercial de l’Association du barreau américain, une proposition, dont le contenu est identique (en anglais), avec la mention suivante “établie, puis adoptée le 18 avril 2015, par l’équipe juridique spéciale sur la gestion de l’identité de la Section de droit commercial de l’Association du barreau américain. Les opinions exprimées dans le présent document n’ont été approuvées ni par la Chambre des délégués ni par le Conseil des Gouverneurs de l’Association et ne doivent par conséquent pas être considérées comme représentant nécessairement la politique de l’Association.”



Annexe

I. Introduction

1. Conformément au mandat de la 44^e session de la Commission en 2011, le Groupe de travail IV sur le commerce électronique (ci-après le Groupe de travail IV) a mené ses travaux sur les documents transférables électroniques¹. Dans le cadre de la 48^e session de la Commission, le Groupe de travail rend compte des travaux réalisés lors de ses 50^e et 51^e sessions. Le travail progresse considérablement sur les dispositions types pour les documents transférables électroniques.

2. Lors de la 44^e session en 2011, la Commission a également constaté que l'examen des questions juridiques liées à la gestion de l'identité électronique recueillait un certain soutien, comme sujet pouvant relever du mandat Groupe de travail IV². À cet égard, il était indiqué qu'il pourrait être utile de continuer à observer la situation de manière à pouvoir mieux définir les termes d'un futur mandat éventuel du Groupe de travail³. Par ailleurs, la Commission a également convenu que l'extension du mandat du Groupe de travail IV aux autres sujets, dont celui de la gestion de l'identité, en tant que sujets distincts (et non en raison de l'incidence qu'ils peuvent avoir sur les documents transférables électroniques) serait examinée lors d'une session future⁴.

3. Depuis la 44^e session de la Commission, l'importance de la gestion de l'identité pour le commerce électronique a pris de l'ampleur, et est dorénavant considérée comme fondamentale en matière de commerce électronique. De même, l'intérêt pour l'utilisation des services de confiance pour accomplir les transactions e-commerce s'est également considérablement élargi.

4. Dans ce contexte, la présente proposition vise à fournir à la Commission les informations nécessaires concernant les domaines de la gestion de l'identité électronique et des services de confiance afin d'envisager un éventuel mandat du Groupe de travail IV dans l'optique d'engager des travaux relatifs à ses sujets.

II. Impact sur les travaux et textes de la CNUDCI

5. Les travaux proposés dans le domaine de la gestion de l'identité et des services de confiance s'inscrivent directement dans la logique des travaux réalisés par le Groupe de travail IV 1) dans le passé (notamment la loi type sur le commerce électronique, la loi type sur les signatures électroniques et la convention sur l'utilisation de communications électroniques dans les contrats internationaux), 2) actuellement (les travaux sur les documents transférables électroniques), et

¹ Rapport de la Commission des Nations Unies pour le droit commercial international sur les travaux de sa quarante-quatrième session (27 juin-8 juillet 2011), document de l'ONU A/66/17, par. 238.

² Ibid., par. 236.

³ Ibid., par. 236.

⁴ Ibid., par. 239.

3) dans le futur, sur d'autres sujets qui ont été discutés, tels le guichet unique, l'informatique nuagique ou les paiements mobiles.

6. Par essence, la gestion de l'identité est un ensemble de processus pour gérer l'identification, l'authentification et les différents attributs spécifiques des individus, entités juridiques, dispositifs ou autres sujets dans un univers connecté. Il est conçu pour fournir la réponse à deux questions simples que chaque partie à une transaction en ligne pose: "Qui êtes-vous?" et "Comment pouvez-vous me le prouver?". Grâce à une vérification fiable de l'identité, une partie à une transaction en ligne peut décider, à titre d'exemple, de conclure un contrat, de permettre à l'autre partie d'accéder à une base de données sensible, ou d'étendre les privilèges ou droits d'accès de l'autre partie. Un aperçu de la gestion de l'identité – synthétisant sa nature, son fonctionnement, et les questions juridiques qu'elle soulève – peut être trouvé dans le document "A/CN.9/WG.IV/WP.120, Vue d'ensemble de la gestion de l'identité."

7. De facto, la gestion de l'identité est une exigence fondamentale qui sous-tend la plupart des travaux développés (ou en cours de développement) par le Groupe de travail IV. Par exemple:

a) Établir l'identité du signataire est l'une des conditions requises pour la création d'une signature électronique valide. Tant l'article 7 de "la Loi type de la CNUDCI sur le commerce électronique" (1996) que "l'article 9 de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux" (2005) requièrent, comme condition préalable à la création d'une signature électronique valide, qu'une méthode soit utilisée pour identifier le signataire "dont la fiabilité est suffisante au regard de l'objet pour lequel la communication électronique a été créée ou transmise". De même, l'article 2 de "la Loi type de la CNUDCI sur les signatures électroniques" (2001) requiert que des données "pouvant être utilisées pour identifier le signataire" soient l'une des composantes d'une signature électronique;

b) Établir l'identité est également une exigence essentielle en matière de documents transférables électroniques, de guichet unique, et de paiement mobile. En particulier, plusieurs dispositions du projet sur les documents transférables électroniques requièrent d'établir l'identité du signataire du document transférable et/ou du titulaire du droit de le contrôler⁵. De même, les futurs travaux sur les processus de guichet unique devraient requérir d'établir l'identité du signataire des documents de douane, ainsi que l'identité de la personne ou entité les remplissant, tout autant que celle de la personne ou entité habilitée à les faire respecter⁶. En outre, les futurs travaux relatifs au paiement mobile requerront également (à des fins d'autorisation) d'établir l'identité de la personne censée transférer des fonds⁷.

8. Qui plus est, bon nombre d'exigences applicables au commerce électronique prévues par les textes de la CNUDCI peuvent, au libre de choix des parties à la transaction, être facilitée par l'utilisation d'un ou plusieurs services de confiance fournis par des tiers. Un "service de confiance" peut inclure le service de création

⁵ Voir A/CN.9/WG.IV/WP.132 et WP.132/Add.1, Projet de dispositions sur les documents transférables électroniques, aux Articles 9, 10, 17, 27, et 28.

⁶ Voir A/CN.9/728/Add.1, par. 42 et 45.

⁷ Voir A/CN.9/728, par. 52.

d'une signature électronique, d'application d'un cachet électronique pour garantir l'origine et l'intégrité d'un document, d'horodatage électronique d'un document afin de lui conférer date certaine, ou de transmission sécurisée d'un document entre les parties.

III. De l'importance de la gestion de l'identité et des services de confiance pour le commerce électronique

9. Une gestion de l'identité fiable est devenue une exigence essentielle pour les activités commerciales effectuées électroniquement du fait de l'importance et de la sensibilité croissantes des transactions exécutées. Une étude de l'OCDE, (ainsi que ses lignes directrices) sur la gestion des identités abonde en ce sens, arguant que "la gestion de l'identité numérique est fondamentale pour le développement futur de l'économie Internet."⁸

10. Par conséquent, de nombreuses entités, tant du secteur public que privé, développent (ou voudraient développer) des modèles économiques qui fournissent, ou font usage de, la gestion de l'identité. Ce dernier point s'applique également aux services de confiance; qui pour certains réclament aussi une gestion de l'identité.

11. Dans de nombreuses transactions électroniques effectuées via internet, il est nécessaire de vérifier l'identité du dépositaire du site internet pour s'assurer qu'il appartient et est effectivement géré par le sujet de droit qui prétend le faire fonctionner. De même, dans de nombreux cas, il est important que les parties s'identifient à l'entame des négociations. En sus, la signature électronique de l'accord définitif peut également réclamer d'identifier les différents signataires, tout autant que d'horodater le document pour lui conférer date certaine. Enfin, dans certains cas, il est important que les documents soient transmis à l'autre partie par le truchement d'un canal sécurisé qui assure la date d'envoi et de réception du document. Les services d'authentification de l'identité et de confiance contribuent de manière significative à l'émergence d'un environnement commercial sans papier, dès lors que les activités quotidiennes des entreprises et administrations publiques peuvent s'effectuer plus rapidement, efficacement et à moindre coûts.

12. Nonobstant les avantages procurés par la gestion de l'identité et les services de confiance, le secteur marchand se montre parfois réticent et prudent quant à leur utilisation. Alors que les raisons d'une telle défiance peuvent être d'ordre économique ou relatives à des défis techniques ou commerciaux, les exigences et incertitudes juridiques peuvent aussi rendre malaisées la conception, la mise-en-œuvre et l'usage de tels systèmes. La gestion de l'identité et les services de confiance étant des concepts relativement neufs, les défis juridiques peuvent inclure: i) que de nombreuses entreprises et États ne comprennent pas les problématiques juridiques y afférent, et ii) que les lois existantes ne sont souvent pas adaptées pour les transactions électroniques, établissant de facto des barrières au déploiement global des systèmes de gestion de l'identité et des services de confiance. En outre, des législations récemment adoptées dans certaines juridictions

⁸ OECD (2011) "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy — Guidance for Government Policy Makers," OECD Digital Economy Papers, No. 196, OECD Publishing, at p. 3.

sont en contradiction avec des lois similaires adoptées précédemment dans d'autres, ce qui pourrait conduire à des problèmes d'interopérabilité transfrontalière.

IV. En quoi des travaux liés à l'identification électronique et les services de confiance se révéleraient utiles

13. Vu l'importance grandissante en matière commerciale de l'identification électronique et des services de confiance et eu égard à l'accroissement de leur usage au niveau domestique et international, il semblerait opportun de mener à bien des travaux au sein de la CNUDCI quant aux problématiques juridiques y afférentes. Qui plus est, mettre en lumière les problématiques juridiques associées à l'utilisation des outils susmentionnés s'avèrerait utile aux fins de développement d'un cadre juridique international uniforme ainsi qu'aux fins d'évaluation par les parties prenantes du modèle idoïne pour mener à bien leurs activités.

14. Par ailleurs, les réflexions et initiatives nationales et régionales dans le domaine de la gestion de l'identité et/ou des services de confiance sont aujourd'hui arrivées à maturité. Bien qu'adoptant parfois des approches contradictoires, elles permettent d'identifier les questions pertinentes et peuvent éclairer le débat eu égard à la conception de cadres juridiques appropriés au niveau international, lesquels seraient transposables dans les divers systèmes juridiques existants. Les exemples d'initiatives listés ci-dessous illustrent le propos:

a) Les législations régionales ou nationales en matière de gestion de l'identité et/ou des services de confiance, notamment, l'adoption le 23 juillet 2014 du règlement européen sur l'identification électronique et les services de confiance⁹, la loi belge sur la carte d'identité électronique et le projet de loi belge sur les services de confiance¹⁰, la législation française relative à la signature électronique¹¹ ainsi qu'à l'envoi recommandé électronique¹², la réglementation italienne relative à la *posta elettronica certificata*¹³ et la Virginia [USA] Electronic Identity Management Act, en vigueur au 1^{er} juillet 2015¹⁴;

b) Les initiatives nationales et internationales émanant du secteur public, y compris la Stratégie nationale américaine des identités de confiance dans le cyberspace (NSTIC)¹⁵ et son groupe pilote sur l'écosystème des identités¹⁶, deux études de l'OCDE sur la gestion de l'identité numérique¹⁷, les projets STORK de

⁹ <http://ec.europa.eu/digital-agenda/en/trust-services-and-eid>

¹⁰ <http://www.lachambre.be/FLWB/PDF/53/2745/53K2745006.pdf>

¹¹ <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00000399095&dateTexte=&categorieLien=id>

¹² <http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023513151>

¹³ <http://qualitapa.gov.it/relazioni-con-i-cittadini/open-government/strumenti-della-pa-digitale/la-posta-elettronica-certificata/>

¹⁴ <https://leg1.state.va.us/cgi-bin/legp504.exe?151+ful+CHAP0483>

¹⁵ <http://www.nist.gov/nstic/>

¹⁶ <http://www.idecosystem.org/>

¹⁷ OECD (2011) "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy — Guidance for Government Policy Makers," OECD Digital Economy Papers, No. 196, OECD Publishing, at p. 3; and OECD (2011), "National Strategies and Policies for Digital Identity Management in OECD Countries", OECD Digital Economy Papers, No. 177, OECD Publishing.

l'UE¹⁸, et les activités effectuées au sein de plusieurs groupes de travail, dont l'UIT, le Conseil de l'identification et de l'authentification numérique du Canada (DIAC)¹⁹, et le Ministère du service numérique du Royaume-Uni²⁰; et

c) Les initiatives nationales et internationales émanant du secteur privé, y compris la "ABA Business Law Section's Identity Management Legal Task Force"²¹, l'Initiative Kantara²², la "Fast Identity Online (FIDO) Alliance"²³, la "Secure Identity Alliance"²⁴, l'"Open Identity Exchange"²⁵, le "Transglobal Secure Collaboration Program (TSCP)"²⁶, et l'"Open Group: Identity Management Forum"²⁷.

15. Les travaux proposés peuvent contribuer à l'harmonisation des aspects juridiques émergeant des travaux de la plupart des divers groupes nationaux et internationaux traitant, à l'heure actuelle, isolément de ces questions; ainsi que familiariser les États et les entreprises peu au fait des questions juridiques en jeu, dans l'optique de raffiner la confiance dans le commerce et les transactions électroniques.

16. Par ailleurs, les travaux proposés pourraient compléter ainsi que fournir des solutions pragmatiques aux documents existants développés par la CNUDCI. Plus précisément, il s'agirait d'élaborer des dispositions législatives dont l'objectif serait de réaliser de manière "concrète et opérationnelle" les exigences "abstraites" consacrées par les textes de la CNUDCI précités. Les entreprises pourraient bénéficier de cadres juridiques clairs afin de mieux gérer leurs risques dans le cadre du commerce électronique international et d'assurer la sécurité juridique de leurs transactions de manière simple et efficace.

V. Objectifs et questions ouvertes

17. L'objectif des travaux proposés serait de fournir un cadre juridique général applicable aux opérations de gestion de l'identité, en ce compris des dispositions appropriées afin de faciliter l'interopérabilité transfrontalière internationale. Par la suite, l'objectif serait de faire de même pour chaque service de confiance.

18. En tout état de cause, de tels cadres juridiques seraient assujettis à deux principes fondateurs. Tout d'abord, l'utilisation des outils mis en place doit demeurer facultative et respecter pleinement l'autonomie de volonté des parties à une transaction. Un second principe est celui de neutralité tant technologique qu'en termes de modèles économiques. Légiférer ne devrait aucunement conduire à limiter l'innovation et les opportunités commerciales par l'introduction de règles strictes

¹⁸ <https://www.eid-stork.eu>

¹⁹ www.diac.ca

²⁰ <http://digital.cabinetoffice.gov.uk/category/id-assurance/>

²¹ <http://apps.americanbar.org/dch/committee.cfm?com=CL320041>

²² <http://kantarainitiative.org/>

²³ <https://fidoalliance.org>

²⁴ <https://www.secureidentityalliance.org/>

²⁵ <http://openidentityexchange.org/>

²⁶ www.tscp.org

²⁷ <http://www.opengroup.org/>

qui favoriseraient une solution technique ou un modèle économique plutôt qu'un(e) autre.

19. Les questions qui pourraient être abordées dans le développement desdits cadres juridiques, tant pour la gestion de l'identité que pour les services de confiance, pourraient être les suivantes:

a) **Obstacles juridiques:** De même qu'il le fut pour les projets du groupe de travail IV traitant du commerce électronique, éliminer les obstacles juridiques pourrait s'avérer un élément essentiel des travaux proposés. Lesdits obstacles peuvent être liés à différentes problématiques, y compris celles liées à l'identification, la signature, l'intégrité, la date, la preuve d'envoi et de réception, de méthode fiable, etc. En sus, l'absence d'harmonisation internationale pourrait en soi constituer un obstacle important à l'usage de la gestion de l'identité et/ou des services de confiance.

b) **Fiabilité:** La fiabilité de la gestion de l'identité et des services de confiance est souvent un élément critique. Définir et mesurer la fiabilité peut s'avérer fondamental dans certains cas et être impossible dans d'autres. Bien que bon nombre de facteurs affectant la fiabilité ne soient pas de nature juridique, certaines approches juridiques peuvent être efficaces pour répondre aux préoccupations y relatives. De telles approches peuvent inclure, à titre exemplatif, des obligations d'information permettant aux parties prenantes d'évaluer précisément la situation; l'attribution d'effets juridiques distincts aux pratiques qui pourraient impacter, positivement ou négativement, la confiance; l'harmonisation transfrontalière de certaines exigences, voire l'imposition d'exigences régissant la conduite des parties prenantes afin d'assurer un haut degré de confiance.

c) **Sécurité des données:** Le niveau de sécurité des opérations de gestion d'identité ou des services de confiance peut, d'un point de vue juridique, affecter le résultat d'une transaction électronique. Actuellement, nulles normes ou législations internationales n'imposent de gestion des risques associés à la fourniture de systèmes de gestion de l'identité ou de services de confiance. L'absence d'éléments objectifs pour juger de la qualité et fiabilité réelle du service obtenu peut se révéler être un problème significatif pour les parties prenantes. Alternativement, un modèle flexible permettant d'introduire différents niveaux d'exigence applicables aux prestataires de services de gestion de l'identité et/ou de confiance pourrait également être une option. Faut-il, et si oui comment, établir des exigences appropriées en matière de sécurité par les prestataires de services de gestion de l'identité et/ou de confiance peut s'avérer une problématique centrale.

d) **Responsabilité:** Quel est le régime de responsabilité des fournisseurs de systèmes d'identification électronique et des prestataires de services de confiance? À l'heure d'engager leur responsabilité transfrontalière, l'utilisateur pourrait être confronté à des clauses contractuelles sibyllines et/ou à des lois relevant de juridictions complaisantes. Il serait dès lors opportun d'évaluer l'opportunité d'édicter des règles claires et structurées en matière de responsabilité

e) **Effet juridique:** L'effet juridique de l'identification et de l'authentification électronique ainsi que celui de bon nombre de services de confiance est souvent indéfinis. Exception faite de la signature électronique, aucun des autres services de confiance ne fait l'objet d'une définition de droit international ou ne se voit attribuer un effet juridique transfrontalier; soulevant un certain nombre

d'interrogations: Sont-ils reconnus par l'autre juridiction? Bénéficient-ils du principe de non-discrimination eu égard à leur équivalent papier? Bénéficient-ils d'autres effets juridiques? Le contrat sera-t-il considéré comme valide dans une autre juridiction? Quelles sont les possibilités en cas d'inexécution des obligations? Les travaux proposés envisageraient de déterminer les effets juridiques qui seraient attribués à l'identification électronique et aux services de confiance en vue de permettre aux parties prenantes de gérer efficacement leurs risques.

20. Ce bref exposé démontre l'importance de la gestion de l'identité et des services de confiance pour le développement du droit commercial international et la nécessité de donner aux acteurs économiques des outils pour assurer la sécurité juridique de leurs transactions électroniques.

VI. Travaux devant être menés par la CNUDCI

21. À la lumière de ce qui précède, nous proposons que la Commission donne mandat pour engager des travaux dans le domaine de la gestion de l'identité et des services de confiance et donne la priorité à ces sujets. Tenant compte des ressources disponibles et du temps limité, nous proposons de commencer par engager des travaux dans le domaine de la gestion de l'identité et d'introduire progressivement les travaux relatifs aux services de confiance.

22. Afin de tenir compte des ressources budgétaires limitées du Secrétariat, nous proposons de mettre en place un groupe d'experts informel qui appuie le secrétariat afin de préparer des propositions législatives pour démarrer les discussions en groupe de travail. Ce groupe d'experts serait ouvert à toutes les délégations qui le souhaitent. Si la nécessité de collecter des informations supplémentaires se fait ressentir, ce groupe d'experts pourrait appuyer le secrétariat dans l'organisation éventuelle d'un colloque sur le sujet.