Nations Unies A/CN.9/WG.IV/WP.144

Assemblée générale

Distr. limitée
30 janvier 2017
Français
Original: anglais/français

Commission des Nations Unies pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Cinquante-cinquième session
New York, 24-28 avril 2017

Travaux dans le domaine du commerce électronique – Questions juridiques relatives à la gestion de l'identité électronique et aux services de confiance

Proposition de l'Autriche, de la Belgique, de la France, de l'Italie, du Royaume-Uni et de l'Union européenne

Note du Secrétariat

Les Gouvernements de la Belgique, de la France, de l'Italie et du Royaume-Uni, la délégation autrichienne ainsi que l'Union européenne ont soumis au Secrétariat un document afin que le Groupe de travail l'examine à sa cinquante-cinquième session. Le texte reçu par le Secrétariat est reproduit en annexe à la présente note.

V.17-00409 (F)

Merci de recycler

Annexe

Proposition de l'Autriche, de la Belgique, de la France, de l'Italie, du Royaume-Uni et de l'Union européenne

Date: 26 janvier 2017

Proposition des Gouvernements de la Belgique, de la France, de l'Italie et du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, de la délégation autrichienne ainsi que de l'Union européenne: travaux dans le domaine du commerce électronique – questions juridiques relatives à la gestion de l'identité électronique et aux services de confiance

I. Introduction

1. Conformément au mandat de la quarante-quatrième 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 électroniques[1]. Dans le cadre de la quarante-neuvième session de la Commission, le Groupe de travail IV a rendu compte de ses travaux réalisés lors de ses cinquante-deuxième et cinquante-troisième sessions. Le travail sur les dispositions types pour les documents transférables électroniques est en voie de finalisation.

2. Lors de la quarante-quatrième 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 IV[2]. À sa quarante-huitième session en 2015, la Commission a demandé au Secrétariat de mener des travaux préparatoires sur la gestion de l'identité et les services de confiance, l'informatique en nuage et le commerce mobile, y compris en organisant des colloques et des réunions de groupes d'experts, en vue des travaux que le Groupe de travail IV pourrait mener à la suite des travaux en cours consacrés aux documents transférables électroniques. À la même session, la Commission a également prié le Secrétariat de communiquer les résultats de ces travaux préparatoires au Groupe de travail IV afin d'obtenir des recommandations sur leur portée exacte, la méthodologie et les priorités qui pourraient être envisagées, afin qu'elle les examine à sa quarante-neuvième session[3].

3. Suite à cette demande, le Secrétariat a présenté à la Commission lors de sa quarante-neuvième session une note relative aux questions juridiques liées à la gestion de l'identité et aux services de confiance qui résume les débats tenus au colloque et lors d'autres réunions pertinentes sur ce sujet[4].

4. À sa quarante-neuvième session en 2016, la Commission a réaffirmé le mandat confié au Groupe de travail IV d'achever l'élaboration du projet de loi type sur les documents transférables électroniques et de la note explicative qui l'accompagnait 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), A/66/17, par. 238.

[2] Ibid., par. 236.

[3] Rapport de la Commission des Nations Unies pour le droit commercial international sur les travaux de sa quarante-huitième session (2015), A/70/17, par. 358.

[4] Document A/CN.9/891.

d'examiner les sujets de la gestion de l'identité et des services de confiance, ainsi que de l'informatique en nuage, une fois qu'il aurait terminé l'élaboration du projet de loi type[5].

5. Conformément à la réaffirmation de ce mandat, la cinquante-quatrième session du Groupe de travail IV a été mise à profit pour finaliser le projet de loi type sur les documents transférables électroniques et démarrer les travaux notamment sur la gestion de l'identité et les services de confiance. Suite aux discussions fructueuses sur ce dernier sujet[6], le Groupe de travail IV a décidé que sa prochaine session serait mise à profit notamment en vue de préciser les objectifs du projet sur la gestion de l'identité et les services de confiance, de préciser sa portée, d'identifier les principes généraux applicables, de lister les concepts à définir et faire une première ébauche de définition de ceux-ci[7].

6. Dans ce contexte, la présente proposition vise à fournir au Groupe de travail IV une contribution sur les points visés au paragraphe précédent permettant de soutenir les discussions lors de la cinquante-cinquième session de ce Groupe, tout en restant ouvert à des propositions complémentaires qui puissent alimenter les discussions.

II. Contexte, portée et objectifs du projet

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

8. 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. De plus, bon nombre d'exigences applicables au commerce électronique prévues par les textes de la CNUDCI peuvent être facilitées par l'utilisation d'un ou plusieurs services de confiance fournis par des prestataires de service. Un "service de confiance" peut inclure le service de création 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, de transmission sécurisée d'un document entre les parties (envoi recommandé électronique), ou d'authentification de site Internet.

9. Une gestion de l'identité fiable ainsi que l'utilisation de services de confiance fiables sont devenues des exigences essentielles pour les activités commerciales effectuées électroniquement du fait de l'importance et de la sensibilité croissantes des transactions exécutées en ligne.

10. Dans de nombreuses transactions électroniques effectuées via l'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

---

[5] Rapport de la Commission des Nations Unies pour le droit commercial international sur les travaux de sa quarante-neuvième session (2016), A/71/17, par. 353.

[6] Rapport du Groupe de travail IV (Commerce électronique) sur les travaux de sa cinquante-quatrième session (31 octobre-4 novembre 2016), A/CN.9/897, par. 107 à 123.

[7] Ibid., par. 120.

s'identifient à l'entame des négociations. En sus, la signature électronique de l'accord définitif peut également réclamer d'identifier les différents signataires, de s'assurer qu'ils ont exprimé leur consentement sur un contenu qui conservera son intégrité ainsi 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.

11. 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 coût. Dans ce contexte, 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 et des services de confiance.

12. 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 nombreuses et 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.

13. Les travaux dans le domaine de la gestion de l'identité et des services de confiance poursuivent différents objectifs:

- Ils veillent à faciliter le développement du droit commercial international et répondent à la nécessité de donner aux acteurs économiques des outils pour assurer la sécurité juridique de leurs transactions électroniques.

- Ils visent à contribuer à l'harmonisation des aspects juridiques émergeant des projets des divers groupes nationaux et internationaux traitant, à l'heure actuelle, isolément de ces questions. L'objectif serait de fournir un cadre juridique général applicable tant aux services de gestion de l'identité qu'aux services de confiance, en ce compris des dispositions appropriées afin de faciliter l'interopérabilité juridique et technique transfrontalière internationale.

- Ils poursuivent également l'objectif de familiariser les États et les entreprises, pas toujours conscients des questions juridiques en jeu, dans l'optique de renforcer la confiance dans le commerce et les transactions électroniques.

- Ils complètent et fournissent des solutions pragmatiques aux documents existants développés par la CNUDCI. Plus précisément, il s'agit d'élaborer des dispositions législatives consistant à réaliser de manière "concrète et opérationnelle" les exigences "abstraites" consacrées par les textes de la CNUDCI précités. Les entreprises bénéficieront ainsi de règles juridiques claires 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.

14. Vu les interactions étroites entre les deux thématiques, les travaux doivent porter d'emblée tant sur la gestion de l'identité que sur les services de confiance. La définition du champ d'application des travaux ainsi que des concepts doit donc inclure ces deux thématiques indissociables. Une telle approche n'empêche pas de travailler par la suite sur ces thématiques de manière séquentielle.

III. Identification des principes généraux applicables et orientations possibles

15. Les principes généraux traditionnels de la CNUDCI devraient guider les travaux sur la gestion de l'identité et les services de confiance. Sont notamment visés:

- *Le principe de l'autonomie de la volonté*. L'utilisation des outils mis en place doit demeurer facultative et respecter pleinement l'autonomie de la volonté des parties à une transaction. Les parties doivent également garder le choix quant au niveau de fiabilité utilisé. Les prestataires doivent rester libres d'offrir un ou plusieurs services de gestion d'identité ainsi que de confiance, et parmi ceux-ci de proposer un ou plusieurs niveaux de fiabilité. Pour résumer, les règles juridiques envisagées doivent être considérées comme une "boîte à outils juridiques" mise à la libre disposition des acteurs du marché.

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

- *Le principe de non-discrimination*. L'effet juridique et la recevabilité comme preuve en justice d'un service d'identification électronique ou d'un service de confiance ne devraient pas être refusés au seul motif que ce service se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences relatives aux niveaux de fiabilité.

- *Le principe de l'équivalence fonctionnelle* qui vise à assurer des fonctions juridiques équivalentes, que l'on agisse dans l'environnement physique ou électronique.

16. Les questions qui devraient être abordées dans le développement des règles juridiques, tant pour la gestion de l'identité que pour les services de confiance, sont les suivantes:

a) La définition de différents niveaux de fiabilité sur la base de critères objectifs: 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. Qu'est-ce que la fiabilité d'un service ou système de gestion d'identité ou de tel service 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, particulièrement dans le cadre de leur politique de gestion de risques. Un modèle flexible permettant d'introduire différents niveaux d'exigence applicables aux services et aux prestataires de service de gestion de l'identité et/ou de confiance constitue une voie respectueuse de la diversité des systèmes dans le monde.

b) Attribution d'effets juridiques distincts en fonction du niveau de fiabilité: Les effets juridiques de l'identification et de l'authentification électroniques ainsi que ceux de bon nombre de services de confiance devraient être définis. L'objectif consiste à déterminer les effets juridiques attribués à l'identification électronique et aux services de confiance en fonction de chaque niveau de fiabilité défini. Les parties prenantes pourraient ainsi gérer efficacement leurs risques juridiques, en optant pour le niveau de fiabilité et l'effet juridique le plus adéquat au regard de leurs besoins. Pour définir ces différents effets juridiques, on pourrait notamment tenir compte – lorsque c'est opportun – du principe de non-discrimination, du principe d'assimilation, du principe de reconnaissance mutuelle, de présomptions particulières

et/ou de mécanismes de renversement de la charge de la preuve. Plus le niveau de fiabilité est élevé, plus l'effet juridique serait favorable à l'utilisateur du service.

c) Détermination de régimes de responsabilité en fonction du niveau de fiabilité: Définir le régime de responsabilité des fournisseurs de systèmes d'identification électronique et des prestataires de service de confiance en vue d'apporter la clarté et prévisibilité nécessaires aux acteurs. Ce régime varierait en fonction du niveau de fiabilité qu'ils offrent.

17. Pour les services de gestion d'identité en particulier, les orientations suivantes devraient être suivies:

- Par application du principe de l'autonomie de la volonté, chaque fournisseur d'un service en ligne conserve la liberté d'exiger ou pas une identification et une authentification électroniques pour l'accès à son service ainsi que le choix du niveau de fiabilité éventuel exigé.

- Application du principe de reconnaissance mutuelle transfrontière des moyens d'identification électronique qui ont un niveau égal ou supérieur à celui exigé pour l'accès au service en ligne. Ce principe se fonderait sur la définition des différents niveaux de fiabilité des moyens d'identification électronique. Chaque niveau serait déterminé par des critères objectifs harmonisés.

- Afin de déterminer les systèmes de gestion de l'identité à prendre en compte dans nos travaux, il convient de s'intéresser en priorité à la finalité/destination d'utilisation du moyen d'identification électronique (celui-ci est-il destiné à être utilisé – totalement ou en partie – pour des opérations commerciales ou pas), et moins de savoir qui a délivré ces moyens d'identification électronique (que ce soit le secteur public, privé ou les deux). Dès lors que la finalité d'utilisation peut être commerciale, le moyen d'identification électronique devrait être examiné dans nos travaux, même s'il est délivré totalement ou partiellement par le secteur public.

- Nos travaux devraient se focaliser en priorité sur l'identification des personnes physiques et morales, en laissant de côté dans un premier temps la question de l'identification des objets matériels (serveur, smartphone, terminal …) ou numériques (logiciels …). Dès lors qu'il est question d'établir des règles de droit, la priorité doit être mise sur l'identification du sujet de droit (personne physique ou morale) **qui est titulaire de droits et d'obligations et qui assume les responsabilités** (le propriétaire d'un site Web, **le titulaire des droits d'auteur**, **le propriétaire d'un serveur** …). Les objets matériels ou numériques seront systématiquement liés à une personne physique ou morale. L'identification des objets est essentiellement une question d'ordre technique et de sécurité, plutôt que juridique.

- Les moyens d'identification électronique appartenant aux niveaux de fiabilité les plus élevés devraient au moins se raccrocher à des données d'identification personnelle issues/gérées par une source **faisant autorité**.

- Pour les niveaux supérieurs de fiabilité, on devrait consacrer une obligation pour le prestataire d'un moyen d'identification électronique de notifier toute atteinte à la sécurité de son système et, si nécessaire, de suspendre celui-ci. Le prestataire devrait notifier conformément aux dispositions prévues dans la législation nationale et, au vu du contexte transfrontalier, rendre l'information publiquement disponible.

- On pourrait envisager une présomption selon laquelle les critères objectifs définissant les niveaux de fiabilité ainsi que les exigences légales seraient

respectés si le prestataire se conforme à des normes techniques déterminées par une autorité internationale.

18. Pour la gestion de l'identité, dans le cadre de la détermination des niveaux de garantie y associés, on pourrait consacrer trois niveaux : a) le niveau de garantie faible; b) le niveau de garantie substantiel; c) le niveau de garantie élevé.

- Les niveaux de garantie seraient caractérisés sur la base de spécifications techniques, de normes et de procédures y afférents.
- Un mécanisme de coopération et un cadre d'interopérabilité pourraient être prévus afin de définir les critères sous-jacents des niveaux de garantie ainsi que d'échanger les informations relatives aux moyens d'identification et aux niveaux de garantie y afférents.
- On consacrerait un principe de reconnaissance mutuelle transfrontière pour les moyens d'identification qui ont un niveau de garantie équivalent (à partir du niveau substantiel) ou supérieur.

19. Pour les services de confiance, les orientations suivantes devraient être suivies :

- Dans le cadre de la définition et l'harmonisation des niveaux de fiabilité des services de confiance, on consacrerait au moins deux niveaux :
  1. services de confiance NON qualifiés;
  2. services de confiance QUALIFIÉS.
- Les effets juridiques seraient différents selon le niveau de fiabilité du service de confiance:
  1. Si le service de confiance est NON qualifié: effet juridique limité à la clause de non-discrimination.
  2. Si le service de confiance est QUALIFIÉ: effet juridique favorable => assimilation, présomption, renversement de la charge de la preuve.
- On consacrerait un principe de reconnaissance mutuelle transfrontière pour les services de confiance qui ont un niveau de fiabilité équivalent.
- On consacrerait une obligation générale de sécurité, adaptée au niveau de risque, pour l'ensemble des prestataires (qualifiés ou non).
- On consacrerait des conditions spécifiques pour les prestataires qualifiés de service de confiance ainsi que pour chaque service de confiance qualifié particulier afin d'assurer un haut niveau de fiabilité.
- Le régime de responsabilité des prestataires de service de confiance varierait selon que le prestataire est qualifié ou non.
- On pourrait obliger tout prestataire (au moins qualifié) de notifier toute atteinte à la sécurité de son système et/ou ses services et, si nécessaire, de suspendre ceux-ci. Le prestataire devrait notifier conformément aux dispositions prévues dans la législation nationale et, au vu du contexte transfrontalier, rendre l'information publiquement disponible.
- On pourrait envisager une présomption selon laquelle les critères objectifs définissant les niveaux de fiabilité ainsi que les exigences légales seraient respectés si le prestataire se conforme à des normes techniques déterminées par une autorité internationale.

IV. Identification des concepts et tentative de définition

20. En vue de soutenir les discussions sur la gestion de l'identité et les services de confiance, la liste suivante (non exhaustive) des concepts et définitions est proposée :

- ***Identification électronique***: le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale;
- ***Moyen d'identification électronique***: un élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne;
- ***Données d'identification personnelle***: un ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale;
- ***Schéma d'identification électronique***: un système pour l'identification électronique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes physiques ou morales, ou à des personnes physiques représentant des personnes morales;
- ***Authentification***: un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique;
- ***Source faisant autorité***: toute source, quelle que soit sa forme, à laquelle on peut se fier pour obtenir des données, des informations et/ou des éléments d'identification exacts pouvant être utilisés pour prouver l'identité;
- ***Service de confiance***: un service électronique (normalement fourni contre rémunération) qui consiste:
  1. en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services; ou
  2. en la création, en la vérification et en la validation de certificats pour l'authentification de site Internet; ou
  3. en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services;
- ***Service de confiance qualifié***: un service de confiance qui satisfait aux exigences du présent texte [Convention, loi modèle];
- ***Signature électronique***: des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer;
- ***Signataire:*** une personne physique qui crée une signature électronique;
- ***Cachet électronique***: des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières;
- ***Horodatage électronique***: des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant;

- ***Service d'envoi recommandé électronique***: un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée;
- ***Certificat d'authentification de site Internet***: une attestation qui permet d'authentifier un site Internet et associe celui-ci à la personne physique ou morale à laquelle le certificat est délivré;
- ***Document électronique***: tout contenu conservé sous forme électronique, notamment un texte ou un enregistrement sonore, visuel ou audiovisuel;
- ***Validation:*** le processus de vérification et de confirmation de la validité d'une signature ou d'un cachet électronique;
- ***Partie utilisatrice***: une personne physique ou morale qui se fie à une identification électronique ou à un service de confiance.

V. Liens avec la pratique

Afin de mieux comprendre la portée des travaux, les concepts et les liens avec la pratique, il est proposé que des projets concrets mis en place dans différents pays ou régions fassent l'objet d'une présentation lors de la (ou des) session(s) du Groupe de travail IV. Nous pourrions par exemple assurer une présentation du CEF eID DSI et du node eIDAS afin de montrer comment cela fonctionne et est mis en place par les États membres de l'Union européenne.