Nations Unies A/CN.9/891

Assemblée générale

Distr. générale
3 mai 2016
Français
Original: anglais

Commission des Nations Unies pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Quarante-neuvième session
New York, 27 juin-15 juillet 2016

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

Note du Secrétariat

Table des matières

V.16-02635 (F)

I. Introduction

1. À sa quarante-huitième session, en 2015, la Commission a chargé le Secrétariat de mener des travaux préparatoires sur la gestion de l'identité et les services de confiance, y compris en organisant des colloques et des réunions d'experts, en vue des travaux que le Groupe de travail pourrait conduire à la suite des activités en cours consacrées aux documents transférables électroniques, sur le fondement d'une proposition qui serait soumise à la Commission pour qu'elle l'examine (A/CN.9/854)[1].

2. 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[2].

3. Comme suite à cette demande, le colloque de la CNUDCI sur les questions juridiques liées à la gestion de l'identité et aux services de confiance a été organisé à Vienne les 21 et 22 avril 2016. En outre, le Secrétariat a participé à une conférence consacrée à des questions ouvertes sur le commerce électronique et l'identité électronique, organisée par l'Université de Bologne (10 juin 2015, Bologne (Italie)); à une réunion internationale sur le droit et la politique de la gestion de l'identité, organisée conjointement par l'American Bar Association (ABA) et la Banque mondiale (Washington (États-Unis d'Amérique), 14 janvier 2016); et à une conférence sur la gestion de l'identité et les services de confiance depuis le règlement eIDAS, organisée par l'Université de Namur (Namur (Belgique), 18 mars 2016))[3].

4. La présente note résume les débats tenus au colloque et lors d'autres réunions pertinentes. Les documents utilisés pour les présentations faites au colloque sont disponibles sur le site Web de la CNUDCI[4].

5. La Commission voudra peut-être noter qu'un document donnant un aperçu de la gestion de l'identité a été soumis au Groupe de travail IV (Commerce électronique) à sa quarante-sixième session (A/CN.9/WG.IV/WP.120) et que des observations supplémentaires sont consignées dans un document présenté au Groupe de travail III (Règlement des litiges en ligne) à sa trente-deuxième session (A/CN.9/WG.III/WP.136). Le rapport sur un précédent colloque concernant le commerce électronique, auquel ont participé des experts en gestion de l'identité, est également disponible (A/CN.9/728, par. 9 à 28).

---

[1] *Documents officiels de l'Assemblée générale*, *soixante-dixième session*, *Supplément n° 17* (A/70/17), par. 354, 355 et 358.

[2] Ibid., par. 358.

[3] Les actes de cette conférence ont été publiés: Hervé Jacquemin (dir.), *L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, 2016.

[4] Ces documents, présentés tels qu'ils ont été soumis par les orateurs, sont disponibles (en anglais) à l'adresse suivante: http://www.uncitral.org/uncitral/en/commission/colloquia/dm2016-programme.html.

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

A. Cadre juridique actuel de la gestion de l'identité et des services de confiance

6. La gestion de l'identité électronique est une question essentielle pour l'utilisation de moyens électroniques. La vérification de l'identité de parties éloignées géographiquement est souvent une préoccupation fondamentale, notamment pour déterminer qui cherche à accéder à une base de données en ligne contenant des informations délicates, qui essaie d'initier un transfert de fonds en ligne à partir d'un compte, qui a signé un contrat électronique, qui a autorisé à distance un envoi de produits, qui cherche à accéder à des services publics en ligne, ou qui a envoyé un courrier électronique. Concrètement, la gestion de l'identité vise à répondre aux questions de base suivantes: "Qui cherche à prouver l'identité?" et "Avec quel degré de fiabilité l'identité est-elle prouvée?" dans un environnement électronique[5].

7. À cet égard, il convient de noter que la vérification fiable de l'identité se fait obligatoirement de manière différente selon qu'il s'agit d'une partie éloignée géographiquement dans un environnement électronique ou d'une partie présente dans un environnement physique. Par exemple, la gestion de l'identité peut être utilisée à distance et simultanément dans de nombreuses applications, ce qui n'est pas le cas des moyens d'identification traditionnels.

8. Les documents d'identité papier sont utilisés depuis des siècles pour identifier les individus et les pratiques sont désormais bien établies, de sorte que les utilisateurs de ces documents connaissent leur fiabilité comme outils d'identification et les risques associés à leur usage. À l'inverse, la gestion de l'identité étant un dispositif relativement nouveau qui nécessite que les informations sur l'identité soient corrélées avec une personne qui n'est pas physiquement présente, les pratiques commerciales concernées ne sont pas encore pleinement établies et l'évaluation des risques varie. En conséquence, si l'on veut renforcer la confiance dans l'utilisation des systèmes de gestion de l'identité, il convient notamment de préciser divers volets techniques et juridiques, y compris les questions de responsabilité.

9. Compte tenu de son importance généralisée, la gestion de l'identité peut avoir des incidences sur l'intégration culturelle, politique, économique et sociale[6]. Elle a diverses implications pour les objectifs de développement durable, car elle concerne directement l'objectif 16.9 (garantir à tous une identité juridique, notamment grâce à l'enregistrement des naissances, d'ici à 2030) et peut faciliter la concrétisation d'un certain nombre d'autres objectifs, tels que l'objectif 1.4 (faire en sorte que les pauvres aient accès aux ressources économiques, y compris à la propriété et aux services financiers), l'objectif 10.c (baisser les coûts des envois de fonds) et l'objectif 16.5 (réduire la corruption).

---

[5] A/CN.9/WG.IV/WP.120, par. 6 et 8.

[6] D'une manière générale, voir le programme de la Banque mondiale concernant l'identification pour le développement, à l'adresse suivante: www.worldbank.org/en/programs/id4d (en anglais).

10. La transition en cours vers des économies en ligne et pilotées par les données fait appel à la gestion de l'identité à de nombreuses fins commerciales et sociales. Des décideurs proposent l'adoption de modèles de gestion de l'identité centrés sur l'utilisateur, dans lesquels ce dernier peut choisir les titres d'identité et le niveau d'assurance qui lui conviennent[7].

11. Dans l'environnement juridique actuel, les systèmes de gestion de l'identité et les services de confiance sont soumis, d'une part, à des obligations prévues dans des textes conçus à d'autres fins (par exemple, code commercial et civil; lois sur la vie privée) et, d'autre part, à des accords contractuels (généralement nommés "règles de système", "règles de schéma" ou "cadres de confiance"), qui visent à assurer leur bon fonctionnement et à garantir leur fiabilité en définissant les obligations des parties.

12. Bien que la majorité des pays aient adopté des lois sur les opérations et les signatures électroniques (comportant généralement des dispositions applicables à la gestion de l'identité et aux services de confiance[8]), seules certaines d'entre elles portent spécifiquement sur l'utilisation de la gestion de l'identité et les services de confiance[9]. Des dispositions législatives supplémentaires peuvent répondre aux besoins de secteurs particuliers, comme celles qui sont destinées au secteur bancaire et applicables aux services de paiement[10].

13. Plusieurs États ont indiqué qu'ils envisageaient d'élaborer une législation sur la gestion de l'identité ou qu'ils avaient déjà commencé à le faire. Ces initiatives se fondent sur différentes stratégies et différentes notions. En conséquence, il existe un besoin évident, fort et urgent de fournir aux législateurs des directives qui proposent des options souhaitables et permettent de prévenir le manque d'harmonisation.

Portée des systèmes de gestion de l'identité

14. Différents modèles de gestion de l'identité sont actuellement utilisés pour remplir plusieurs fonctions, qui peuvent varier de manière non négligeable quant à leur objet et leurs prescriptions. Dans la mesure où les systèmes de gestion de l'identité peuvent concerner différentes sortes d'applications, de services et d'utilisateurs, il importe que leur analyse juridique ne se limite pas à certains types d'opérations (par exemple les opérations commerciales). Il en va de même pour les services de confiance.

15. Les systèmes de gestion de l'identité peuvent servir à identifier des personnes physiques ou morales, ainsi que des objets physiques ou numériques. Toutefois, toutes ces entités ne bénéficient pas de la même attention dans l'étude des questions

---

[7] OCDE, Digital Identity Management: Enabling Innovation and Trust in the Internet Economy, Paris, 2011, p. 7 et suiv.

[8] Pour un aperçu de l'état actuel de la législation sur les opérations électroniques et les signatures électroniques, voir l'outil de suivi mondial de la CNUCED en matière de cyberdroit à l'adresse suivante (en anglais): http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx.

[9] Par exemple, Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur; loi de 2015 de l'état de Virginie sur la gestion de l'identité électronique (SB 814).

[10] Voir les dispositions pertinentes de la Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

juridiques concernant ces systèmes. En particulier, les travaux menés sur les volets juridiques de l'identification des objets semblent nécessiter une attention supplémentaire. À cet égard, il convient de noter que certaines technologies (par exemple, les balises radio-identification (RFid) ou d'autres technologies sans contact) peuvent être mieux adaptées que d'autres à l'identification d'objets, et en conséquence offrir des exemples de mise en œuvre qui peuvent être utiles pour engager cette analyse.

16. Les utilisateurs commerciaux de la gestion de l'identité mènent généralement des analyses des avantages et des coûts associés aux technologies et méthodes mises en œuvre dans le cadre de leurs activités commerciales et, en conséquence, ont besoin d'une grande souplesse, ainsi que de clarté et de prévisibilité dans la répartition des obligations et de la responsabilité connexe entre les parties concernées. Les mêmes observations ne s'appliquent pas nécessairement aux systèmes de gestion de l'identité utilisés pour fournir des services publics.

17. Les systèmes de gestion de l'identité peuvent être classés en fonction de différents critères, selon par exemple qu'ils sont "gérés par des entreprises" ou "gérés par des administrations", et "centralisés" ou "décentralisés". Une autre classification distingue d'une part les systèmes fournissant l'identité fondamentale ou de base (à savoir, des caractéristiques identitaires qui généralement ne changent pas, telles que le nom ou la date de naissance, et qui sont censées être à fins multiples) et, d'autre part, les systèmes donnant une identité fonctionnelle (c'est-à-dire des caractéristiques identitaires établies à des fins particulières).

18. Si les impératifs commerciaux représentent un moteur essentiel de la conception de systèmes de gestion de l'identité au niveau mondial, l'importance des systèmes publics ne doit pas être sous-estimée. Il convient de noter que, traditionnellement, un certain nombre de fonctions liées à la gestion de l'identité dans le monde physique sont exercées par les registres et statistiques de l'état civil. Ces registres sont, notamment depuis deux siècles, gérés par les administrations. Dans le cadre de l'exercice des fonctions concernant les registres et statistiques de l'état civil, les administrations limitent généralement leur responsabilité conformément au régime juridique applicable aux activités gouvernementales et garantissent la fiabilité des informations consignées dans les registres au moyen d'autres mécanismes juridiques (par exemple, dispositions du droit pénal concernant la présentation ou la création de fausses informations relatives à l'identité).

19. Les pratiques commerciales concernant l'identification des parties se sont forgées au fil des siècles à partir des informations sur l'identité consignées dans les registres et statistiques de l'état civil et d'autres registres, et de leur cadre juridique connexe. À ce jour, ces registres jouent un rôle important pour fournir des informations utilisées dans la gestion de l'identité. En particulier, ils peuvent être utilisés comme le fondement de "documents sources" sur lesquels les systèmes commerciaux se reposent pour établir l'identité de personnes physiques ou morales.

20. Par ailleurs, les systèmes de gestion de l'identité gérés par des administrations peuvent être conçus pour prolonger et moderniser les registres et statistiques de l'état civil traditionnels. Ils peuvent être axés sur la sécurité et d'autres caractéristiques utiles à leur raison d'être. En outre, conformément à la conception classique des opérateurs des registres et statistiques de l'état civil, leurs prestataires n'agissent pas nécessairement dans le cadre d'un régime de pleine responsabilité en cas de non-fonctionnement ou de fonctionnement partiel de leurs services.

21. Des titres d'identité commerciaux établis à différentes fins peuvent se fonder sur un même document d'identité de base. Toutefois, ces différents titres d'identité peuvent offrir un niveau de fiabilité variable et être utilisés avec différentes méthodes et technologies. En conséquence, l'analyse juridique des rapports entre les divers titres d'identité et le document d'identité de base nécessite un examen attentif.

22. Les observations ci-dessus montrent qu'il n'existe pas de modèle ou de solution unique pour la gestion de l'identité. Au contraire, de nombreux systèmes de gestion de l'identité, ayant différents objets, coexistent. De même, les obligations et la responsabilité des parties participant à ces systèmes peuvent varier. Toutefois, cela ne semble pas exclure la possibilité de trouver des éléments communs sur lesquels faire fond pour promouvoir l'interopérabilité juridique.

Interaction et interopérabilité des systèmes de gestion de l'identité

23. Les systèmes de gestion de l'identité sont souvent fédérés. Selon ce modèle, les informations relatives à l'identité vérifiées par une entité sont mises à la disposition, de manière convenue et contrôlée, de nombreuses parties qui en ont besoin pour diverses raisons[11]. Les systèmes fédérés assurent l'interopérabilité entre leurs participants en utilisant un cadre technique et juridique commun défini par un ensemble de règles de système. La fédération d'un système contribue à l'augmentation du nombre d'utilisateurs et d'applications, et peut aider à modérer les coûts liés à la gestion de l'identité.

24. Toutefois, la plupart des systèmes de gestion de l'identité fonctionnent actuellement de manière autonome, avec peu d'interaction, voire aucune, en raison d'obstacles à la fois techniques et juridiques. En particulier, les règles juridiques applicables aux systèmes de gestion de l'identité sont très variables. Cependant, la valeur d'un système de ce type est proportionnelle au nombre de parties qui s'en servent et au nombre et à la diversité des applications dans lesquelles il peut être utilisé. En conséquence, idéalement, les systèmes de gestion de l'identité devraient interagir de manière harmonieuse, en s'appuyant à la fois sur l'interopérabilité technique et la reconnaissance juridique réciproque (c'est-à-dire l'"interopérabilité juridique").

25. Dans la mesure où la fédération seule ne saurait régler toutes les questions que pose la gestion de l'identité, les systèmes de ce type tireraient parti d'un cadre juridique harmonisé. La question de savoir si la fédération de systèmes de gestion de l'identité en tant que telle pose des difficultés juridiques particulières doit être examinée plus avant.

26. Des problèmes supplémentaires faisant obstacle à l'interopérabilité technique et juridique peuvent apparaître au niveau régional, où des tendances particulières peuvent exister et où les capacités et les ressources disponibles ne sont pas toujours suffisantes.

27. Un certain nombre d'organisations visent à promouvoir l'élaboration de systèmes de gestion de l'identité et le renforcement de leur utilisation[12]. Cet objectif

---

[11] A/CN.9/WG.IV/WP.120, par. 10.

[12] Voir A/CN.9/WG.IV/WP.120, par. 5, pour une liste de plusieurs organisations actives dans ce domaine.

nécessite la combinaison de décisions politiques, d'évolutions techniques et de dispositions juridiques. La prévisibilité des règles juridiques applicables – ainsi que, dans la mesure du possible, leur harmonisation – et la sécurité juridique qui en découle pourraient grandement contribuer à lever les obstacles qui entravent la mise en œuvre de la gestion de l'identité d'un système à l'autre et de part et d'autre de frontières nationales.

Services de confiance

28. Les services de confiance englobent différents actes qui visent à promouvoir la confiance en matière d'opérations électroniques, notamment, mais pas exclusivement: l'archivage numérique; l'horodatage; les signatures prouvant l'origine et l'intégrité du message; les accusés de réception; la garantie de l'existence à un moment donné; les sceaux numériques; l'authentification de l'adresse électronique (par exemple, releveur uniforme des ressources) et du compte séquestre.

29. Les textes de la CNUDCI relatifs au commerce électronique comprennent un certain nombre de dispositions applicables aux services de confiance, notamment des dispositions sur les signatures électroniques, ainsi que sur l'intégrité, l'archivage et l'attribution des messages de données. Ces textes ayant été largement adoptés dans le monde[13], un nombre significatif de lois uniformes existe dans ce domaine.

30. Les services de confiance et ceux de gestion de l'identité peuvent avoir des éléments en commun. Toutefois, il existe également des différences notables, en particulier compte tenu de l'objet de chaque service de confiance. Il reste à déterminer s'il serait possible et souhaitable d'examiner conjointement les volets juridiques des services de confiance et de ceux de gestion de l'identité.

B. Promouvoir la confiance en matière de gestion de l'identité et de services de confiance

31. Il est essentiel d'assurer la confiance dans le fonctionnement des systèmes de gestion de l'identité et des services de confiance afin de promouvoir leur utilisation (voir par. 6 à 8 ci-dessus). La confiance peut être définie comme la croyance ferme en la fiabilité de quelque chose[14]. Il s'agit donc d'une opinion qui influence le comportement et la volonté de compter sur quelqu'un ou quelque chose. Dans le cas de la gestion de l'identité et des services de confiance, la confiance est l'opinion sur la fiabilité du service proposé.

32. La fiabilité peut quant à elle se définir comme la bonne qualité systématique de l'exécution[15] et est le résultat d'un processus, plutôt qu'un produit.

33. Le manque de clarté concernant la responsabilité des parties est un obstacle majeur à la promotion de la confiance dans l'utilisation de la gestion de l'identité et des services de confiance. Les parties doivent pouvoir évaluer les droits et

---

[13] Pour l'état de l'adoption des textes de la CNUDCI relatifs au commerce électronique, voir www.uncitral.org/uncitral/fr/uncitral_texts/electronic_commerce.html.

[14] Oxford English Dictionary Online, "Trust", sub. 1.

[15] Oxford English Dictionary Online, "Reliability", sub. 1.

obligations et répartir les risques de manière claire. Actuellement, ces termes peuvent être précisés dans des accords contractuels (figurant généralement dans les règles de système), dont la teneur peut sensiblement varier. En outre, la loi peut attribuer la responsabilité, éventuellement sur le fondement de règles générales, en l'absence de tout accord, ou également prévaloir sur de tels accords. Les dispositions sur la limitation de la responsabilité figurant dans la loi et les clauses contractuelles sont également applicables pour déterminer la répartition des risques. L'existence d'assurances commerciales est également pertinente pour ce qui est de couvrir les risques liés à l'utilisation de la gestion de l'identité et des services de confiance.

34. Il importe grandement que les dispositions législatives et contractuelles visant à promouvoir la confiance soient centrées sur l'issue du processus, par exemple en prévoyant des services fiables, plutôt que sur la prescription de processus particuliers, ce qui pourrait contrevenir à la neutralité en matière de technologie ou de systèmes d'identité. Cela a d'importantes conséquences pratiques, par exemple pour ce qui est de garantir que les règles n'empêchent pas l'utilisation de la gestion de l'identité au moyen de toute technologie ou méthode particulière, telle que les appareils mobiles. De même, les obligations législatives concernant la fiabilité peuvent renvoyer à des normes techniques; toutefois, la prudence s'impose pour éviter de favoriser des technologies, méthodes ou processus particuliers, ou d'empêcher l'adaptabilité.

35. La loi peut spécifiquement promouvoir la confiance dans la fiabilité des systèmes de gestion de l'identité et des services de confiance en valorisant le respect de certaines obligations concernant cette fiabilité.

36. En particulier, la loi peut assortir de présomptions légales l'utilisation de systèmes de gestion de l'identité et de services de confiance qui satisfont à certaines exigences. Ces présomptions peuvent déplacer la charge de la preuve concernant l'origine, l'intégrité, la date d'envoi et de réception, etc., lorsque les opérations électroniques sont réalisées à l'aide de systèmes de gestion de l'identité ou de services de confiance conformes. Les parties sont libres de choisir si ces systèmes et services sont pertinents et utiles pour leurs activités commerciales, assurant ainsi la flexibilité voulue.

37. À défaut, la loi peut prévoir la limitation ou l'exclusion de la responsabilité de certaines parties à des systèmes de gestion de l'identité ou des services de confiance si elles se conforment aux obligations prévues dans la législation ou les accords contractuels. Elle peut également prévoir que les accords contractuels ne peuvent pas écarter ou modifier la responsabilité en cas de négligence grave ou de faute intentionnelle.

38. Une meilleure compréhension des obligations des diverses parties à un système d'identité et de la répartition entre elles des risques en matière de responsabilité a pour avantage non négligeable d'améliorer l'évaluation des besoins en matière de cybersécurité, ce qui permet, par voie de conséquence, d'allouer les ressources connexes plus efficacement, en fonction des besoins réels des parties.

Utilisation internationale de la gestion de l'identité et des services de confiance

39. Un environnement juridique propice à la gestion de l'identité et aux services de confiance doit également tenir pleinement compte des volets transfrontières de leur utilisation. Ces volets peuvent poser des difficultés supplémentaires en l'absence d'un cadre juridique uniforme favorisant la reconnaissance réciproque du statut juridique des systèmes de gestion de l'identité et des services de confiance. Pour ce qui est de l'examen de ces aspects, l'attention voulue doit être portée aux dispositions sur la reconnaissance juridique réciproque des méthodes d'authentification prévues dans les instruments internationaux tels que les accords de libre-échange[16].

40. Actuellement, la reconnaissance juridique transfrontière peut se concrétiser sur le fondement d'accords contractuels privés stipulant les conditions du service ainsi que les spécifications techniques[17]. Toutefois, ce modèle est soumis aux limites prévues par la loi nationale en matière de liberté contractuelle et ne s'applique pas aux parties qui ne sont pas liées par un contrat.

41. Selon une autre conception de la reconnaissance juridique transfrontière des systèmes de gestion de l'identité et des services de confiance, on peut prévoir la mise en œuvre d'un système d'accréditation centralisé procédant à des évaluations dont le résultat déterminerait le statut juridique du système de gestion ou du service et lierait les États participants. L'évaluation de la conformité des systèmes et des services se ferait avant leur utilisation effective et selon des catégories générales. Ce modèle serait particulièrement utile s'il était appliqué dans le cadre de l'intégration économique régionale car les États qui s'emploient à réaliser cette intégration auraient intérêt à s'y rattacher.

42. Selon une troisième possibilité, on élaborerait des dispositions juridiques uniformes visant la reconnaissance transfrontière, de préférence sur une base multilatérale. Dans cette hypothèse, il serait possible de ne procéder à l'évaluation de la fiabilité que si un différend survenait et au cas par cas[18].

43. Il convient de noter que tout texte juridique uniforme doit interagir avec les règles juridiques internationales privées. Une attention particulière pourrait devoir être prêtée à l'analyse de cette interaction.

C. Questions pertinentes pour de futurs travaux

44. Diverses parties prenantes saluent la décision qu'a prise la CNUDCI d'engager des travaux sur les volets juridiques de l'utilisation de systèmes de gestion de l'identité et de services de confiance et proposent qu'elle élabore des dispositions donnant des directives législatives particulières. Le texte renforcerait la confiance des parties dans l'utilisation des systèmes de gestion de l'identité et des services de confiance et promouvra l'interopérabilité entre ces systèmes. D'une part, il

---

[16] Voir, par exemple, l'article 14.6 du Partenariat transpacifique.

[17] Ce modèle est utilisé par l'Alliance panasiatique pour le commerce électronique.

[18] Cette conception est celle qui a été retenue au paragraphe 3 de l'article 9 de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux.

comblerait les lacunes entre la législation générale et les règles de système et, d'autre part, il garantirait l'uniformité de la législation future.

45. Dans la conduite de ces travaux futurs, il semble particulièrement important d'assurer la coordination avec les organisations compétentes s'occupant des volets juridiques et techniques des systèmes de gestion de l'identité et des services de confiance. Cela permettra de centrer ces travaux sur des questions concrètes, en se fondant sur l'expérience et l'expertise existantes et en soulignant les éléments communs des lois en vigueur et futures.

46. En ce qui concerne la forme des futurs travaux de la CNUDCI, on peut envisager l'élaboration d'une législation type à adopter au niveau national, mais un texte international pourrait être plus adapté pour englober les volets transfrontières. Des textes non législatifs (notamment des dispositions contractuelles types) pourraient utilement traiter de certaines questions. Des textes se renforçant mutuellement pourraient être élaborés.

47. Pour ce qui est de la teneur des dispositions sur les systèmes de gestion de l'identité et les services de confiance, les principes généraux qui sous-tendent les textes de la CNUDCI sur l'utilisation des communications électroniques (neutralité technologique, non-discrimination des communications électroniques, équivalence fonctionnelle) et d'autres principes généraux du droit commercial uniforme (liberté contractuelle) sont pertinents pour définir le cadre juridique de l'utilisation de systèmes de gestion de l'identité et de services de confiance.

48. En outre, plusieurs dispositions figurant dans les textes de la CNUDCI sur le commerce électronique (par exemple, dispositions sur les signatures électroniques et l'archivage) et dans certains autres textes[19] sont directement applicables aux systèmes de gestion de l'identité et aux services de confiance et peuvent donner des orientations utiles. Une analyse approfondie de ces textes pourrait faciliter la préparation des futurs travaux de la CNUDCI dans ce domaine.

49. À cet égard, il semble particulièrement utile de clarifier encore la relation entre, d'une part, les systèmes de gestion de l'identité et les services de confiance et, d'autre part, les signatures électroniques. Cette analyse doit tenir compte du fait que les signatures électroniques nécessitent un élément identitaire associé qui permette aux parties de se fier à la signature en identifiant le signataire de manière fiable. Il convient également de prendre en compte l'utilisation de certains types de signatures électroniques dans la prestation de services de confiance.

50. Il pourrait être utile, pour clarifier les diverses notions et garantir l'uniformité de leur interprétation, d'élaborer des définitions des termes les plus importants en ce qui concerne les systèmes de gestion de l'identité et les services de confiance. Il conviendrait, ce faisant, de prendre en compte les normes techniques existantes et les définitions qu'elles comprennent[20].

51. Compte tenu de ce qui précède, il paraît souhaitable que la portée du projet législatif englobe tous les types de systèmes de gestion de l'identité et de services de confiance, indépendamment de la nature du prestataire et de l'objet, la fonction

---

[19] Par exemple, paragraphe 2 de l'article 5 de la Loi type de la CNUDCI sur les virements internationaux (1992).

[20] Voir documents ISO/IEC 24760-1:2011 (en anglais seulement) et ISO/IEC 24760-2:2015 (en anglais seulement) pour des exemples de définitions concernant la gestion de l'identité.

ou l'utilisation principaux visés. Le projet devrait également couvrir toutes les entités possibles susceptibles d'être identifiées par un système de gestion de l'identité et tous les rôles possibles. Enfin, il devrait traiter à la fois de l'utilisation des systèmes de gestion de l'identité et des opérations entre ces systèmes.

52. Pour ce qui est des sujets particuliers à examiner en matière de gestion de l'identité, les principaux sont les suivants: droits et obligations des parties; fiabilité dans les diverses étapes du cycle de la gestion de l'identité; conséquences de la fiabilité sur la responsabilité; règles de système et autres accords contractuels (tels que les accords de prestation de service); reconnaissance juridique réciproque et autres questions relatives à l'interopérabilité juridique.

53. Un volet important de la gestion de l'identité concerne la protection de la vie privée et des données. Il s'agit d'un sujet complexe, dont les approches peuvent varier sensiblement et que plusieurs initiatives visent à concilier. En pratique, la législation en vigueur en matière de gestion de l'identité prend acte de l'existence de textes particuliers sur la vie privée et renvoie à leur application. Dans ces conditions, et afin que les travaux sur les systèmes de gestion de l'identité et les services de confiance restent dans les limites du mandat de la CNUDCI[21], il est peu probable que celle-ci puisse efficacement se pencher de près sur ces questions pour l'instant.

54. Un autre volet à analyser plus avant concerne l'utilisation de systèmes de gestion de l'identité et de services de confiance dans l'informatique en nuage. Les services infonuagiques peuvent être utilisés pour assurer la gestion de l'identité (identité en tant que service). En outre, la gestion de l'identité (par exemple, sous la forme d'une authentification multifactorielle) est généralement utilisée pour accéder aux services infonuagiques, en particulier pour garantir la conformité aux exigences réglementaires, notamment en matière de vie privée. Toutefois, une étude approfondie s'impose pour déterminer si ces utilisations posent des questions juridiques particulières.

55. En ce qui concerne les méthodes de travail, il paraît particulièrement souhaitable d'encourager une large participation de toutes les régions aux travaux futurs de la CNUDCI, afin de mieux évaluer l'état actuel des systèmes de gestion de l'identité et des services de confiance, et de déterminer quelles sont les tendances particulières au niveau régional[22]. Un moyen d'y parvenir est de distribuer des questionnaires. Il est également possible de coopérer et se coordonner avec des organisations régionales compétentes, telles que l'Organisation arabe des technologies de l'information et de la communication (AICTO)[23].

---

[21] *Documents officiels de l'Assemblée générale*, *soixante-dixième session*, *Supplément n° 17* (A/70/17), par. 355.

[22] Pour de plus amples informations sur les États membres de l'Association des nations de l'Asie du Sud-Est (ASEAN), voir le document de l'Electronic Transactions Development Agency intitulé "Secure Transactions Framework Final Report" (Bangkok, juillet 2014).

[23] En particulier, le mandat du Groupe de travail III de l'AICTO (Certification électronique et cybersécurité) peut englober la gestion de l'identité.