Nations Unies A/CN.9/965

Assemblée générale

Distr. générale
23 novembre 2018
Français
Original : anglais

Commission des Nations Unies pour le droit commercial international
Cinquante-deuxième session
Vienne, 8-26 juillet 2019

Rapport du Groupe de travail IV (Commerce électronique) sur les travaux de sa cinquante-septième session (Vienne, 19-23 novembre 2018)

I. Introduction

1. 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). Comme suite à une recommandation du Groupe de travail (A/CN.9/936, par. 95), la Commission a prié celui-ci de mener des travaux sur ces questions, en vue d'élaborer un texte visant à faciliter la reconnaissance internationale de la gestion de l'identité et des services de confiance[1]. 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 par le Groupe de travail lors de sessions précédentes.

II. Organisation de la session

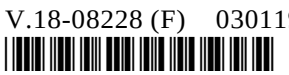
2. Le Groupe de travail, qui se compose de tous les États membres de la Commission, a tenu sa cinquante-septième session à Vienne du 19 au 23 novembre 2018. Ont assisté à la session des représentants des États membres ci-après du Groupe de travail : Allemagne, Arménie, Autriche, Bélarus, Brésil, Bulgarie, Burundi, Canada, Chine, El Salvador, Équateur, Espagne, États-Unis d'Amérique, Fédération de Russie, France, Grèce, Hongrie, Iran (République islamique d'), Italie, Japon, Kenya, Malaisie, Mexique, Ouganda, Pakistan, Pologne, République de Corée, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Singapour, Suisse, Tchéquie, Thaïlande, Turquie et Venezuela (République bolivarienne du).

3. Ont également assisté à la session des observateurs des États suivants : Algérie, Belgique, Bolivie (État plurinational de), Myanmar, Pérou, Qatar, République dominicaine, Suède, Timor-Leste et Yémen.

4. Ont aussi assisté à la session des observateurs du Saint-Siège et de l'Union européenne.

[1] *Documents officiels de l'Assemblée générale, soixante-treizième session, Supplément n° 17* (A/73/17), par. 159.

V.18-08228 (F) 030119 040119



Merci de recycler

5. Ont en outre assisté à la session des observateurs des organisations internationales suivantes :

a) *Système des Nations Unies* : Banque mondiale ;

b) *Organisations intergouvernementales* : Conseil de coopération du Golfe, Organisation internationale de la Francophonie et Secrétariat du Commonwealth ;

c) *Organisations non gouvernementales internationales* : Association Droit & Méditerranée (Jurimed), Association internationale des marques (AIM), Association juridique de l'Asie et du Pacifique (LAWASIA), Centre for International Legal Education (Université de Pittsburgh) (CILE), Chambre brésilienne de commerce électronique (camara-e.net), European Multi-channel and Online Trade Association (EMOTA), Fédération internationale des associations de transitaires et assimilés (FIATA), GSM Association (GSMA), Institut de droit et de technologie (Université Masaryk), Jerusalem Arbitration Center (JAC), Moot Alumni Association (MAA) du Concours d'arbitrage commercial international Willem C. Vis et Union internationale du notariat (UINL).

6. Le Groupe de travail a élu le Bureau suivant :

Présidente : Mme Giusella Dolores FINOCCHIARO (Italie)

Rapporteur : M. Tomas KOZAREK (Tchéquie)

7. Le Groupe de travail était saisi des documents suivants : a) ordre du jour provisoire annoté (A/CN.9/WG.IV/WP.152) ; b) notes du Secrétariat sur les questions juridiques liées à la gestion de l'identité et aux services de confiance (A/CN.9/WG.IV/WP.153 et A/CN.9/WG.IV/WP.154) ; et c) proposition de l'Allemagne comprenant un projet d'instrument relatif à la reconnaissance juridique transfrontière de la gestion de l'identité et des services de confiance et une feuille de route présentée sous forme de tableau pour l'examen des aspects juridiques de la gestion de l'identité et des services de confiance (A/CN.9/WG.IV/WP.155 et Add.1).

8. Le Groupe de travail a adopté l'ordre du jour suivant :

1. Ouverture de la session.
2. Élection du Bureau.
3. Adoption de l'ordre du jour.
4. Questions juridiques liées à la gestion de l'identité et aux services de confiance.
5. Assistance technique et coordination.
6. Questions diverses.
7. Adoption du rapport.

III. Délibérations et décisions

9. Le Groupe de travail a poursuivi l'examen des questions juridiques liées à la gestion de l'identité et aux services de confiance, en se fondant sur les documents mentionnés au paragraphe 7 ci-dessus. Il est rendu compte de ses délibérations et décisions sur ce sujet au chapitre IV du présent rapport.

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

A. Portée des travaux

10. Reconnaissant qu'il appartenait aux États d'examiner la question de l'identité fondamentale des personnes physiques et morales, le Groupe de travail a confirmé que ses travaux devraient mettre l'accent sur les questions liées à l'identité de

transaction et, dans ce contexte, sur celles liées à la reconnaissance, plutôt qu'à l'attribution de l'identité. Dans le même temps, il a reconnu que les questions liées à l'identité fondamentale pourraient être pertinentes pour ses travaux étant donné que cette identité pouvait être exigée par la loi ou utilisée par les parties contractantes pour établir l'identité de transaction.

11. Le Groupe de travail s'est demandé si ses travaux devaient s'attacher à permettre l'identification fiable tant des sujets que des objets de transactions et a confirmé qu'il faudrait maintenir une distinction claire entre les deux concepts (sujets et objets). Il a été dit que l'identification d'objets pouvait être nécessaire pour identifier les sujets de transactions, c'est-à-dire les personnes auxquelles les droits, obligations et responsabilités découlant de la transaction seraient attribués. Dans le même temps, on a déclaré qu'un objet n'avait pas de personnalité juridique et ne pouvait assumer de responsabilité.

12. On a appuyé l'avis selon lequel les questions de responsabilité ne seraient pertinentes pour les travaux du Groupe de travail que dans la mesure où elles concernaient la responsabilité découlant des services d'identification. On a notamment souligné que la question de la responsabilité des objets n'entrait pas dans le cadre de ces travaux. On a aussi exprimé l'avis selon lequel le Groupe de travail pourrait aborder les responsabilités des créateurs d'objets, notamment celle d'identifier correctement l'objet lors de sa création et d'établir un lien clair entre l'objet et la personne qui serait responsable des actions de l'objet, puisque ces responsabilités pouvaient être pertinentes pour l'identification appropriée des personnes.

13. S'agissant des paragraphes 5 et 6 du document A/CN.9/WG.IV/WP.153, on s'est inquiété de ce qu'ils tendaient à élargir le mandat du Groupe de travail concernant la gestion de l'identité. Le point de vue a été exprimé que celui-ci devait limiter les travaux qu'il mènerait sur ce thème aux questions susceptibles d'être traitées dans un délai raisonnable. On n'a pas exclu la possibilité de diviser ce thème en plusieurs sous-thèmes et de présenter les résultats des travaux correspondants de manière étalée dans le temps.

14. On s'est inquiété de l'utilisation du terme « trust services » (services de confiance en français) dans les documents de travail en anglais dont le Groupe de travail était saisi. On a exprimé une préférence pour l'utilisation d'un autre terme, tel que « trusted services providers », qui traduirait mieux le sens recherché, car le mot « trust » avait une acception juridique établie dans certains pays (voir également par. 101 ci-dessous).

15. Compte tenu des débats tenus aux sessions précédentes, on a réaffirmé que les travaux menés par le Groupe de travail sur la gestion de l'identité ne devaient pas avoir pour objet d'établir des exigences équivalentes sur le plan fonctionnel pour l'identification dans les environnements papier et électronique.

16. On a estimé que les travaux devaient avoir pour objet d'identifier les éléments des systèmes de gestion de l'identité qui facilitaient la reconnaissance, entre ces systèmes, des résultats de l'identification. On a expliqué que le Groupe de travail devrait donc s'efforcer de proposer aux parties contractantes un ensemble d'options parmi lesquelles elles pourraient effectuer leur choix en fonction de leurs besoins, sans toutefois leur imposer aucune solution.

17. Une question a été posée au sujet de la référence, au paragraphe 11 du document A/CN.9/WG.IV/WP.153, à l'identification des commerçants du secteur informel. Il a été indiqué que cette référence traduisait une inquiétude exprimée à la cinquante-sixième session du Groupe de travail (voir A/CN.9/936, par. 63), à savoir qu'en se fiant exclusivement aux justificatifs d'identité officiels, on risquait de pénaliser les commerçants qui rencontraient de graves difficultés pour obtenir une reconnaissance formelle. On a ajouté que l'inclusion économique et financière était l'une des considérations prises en compte par la CNUDCI.

18. À cela, il a été répondu qu'il ne fallait pas interpréter cette référence comme valant approbation du secteur informel, et qu'il était préférable d'encourager la transition des commerçants vers le secteur formel en tenant compte uniquement des

entités dotées de la personnalité juridique. Dans ce contexte, on a rappelé que le Groupe de travail I était chargé de mettre au point des outils juridiques pour faciliter cette transition.

19. Par ailleurs, on a noté que les travaux menés par le Groupe de travail avaient pour objet de permettre l'identification fiable des entités, que celles-ci exercent leurs activités dans le secteur formel ou informel. Dans ce contexte, on a souligné que les parties contractantes pourraient accepter divers moyens d'identification, qui n'incluraient pas nécessairement les justificatifs d'identité officiels, en fonction des risques commerciaux liés à une transaction donnée.

B. Exigences et mécanismes de reconnaissance juridique

20. On a posé la question de savoir si la reconnaissance juridique était nécessaire pour faciliter la reconnaissance des systèmes de gestion de l'identité à l'échelle internationale, ou si un autre type de reconnaissance, comme la reconnaissance technique, pourrait être suffisant. On s'est également interrogé sur la relation entre la reconnaissance juridique et la reconnaissance factuelle.

21. En réponse à cette question, il a été noté qu'avant de conclure des opérations commerciales par voie électronique, pour mieux en évaluer les risques et en réduire les coûts, il était souhaitable de disposer d'un certain niveau de confiance. Il a également été noté que les parties à une opération visant un niveau plus élevé de sécurité juridique s'efforceraient d'obtenir la reconnaissance juridique de l'identification, et que l'objectif global du Groupe de travail était de développer la confiance en ce qui concerne l'utilisation de l'identité numérique. Il a été ajouté que la reconnaissance juridique *ex ante* constituerait l'un des moyens de renforcer cette confiance.

22. Il a été indiqué que le Groupe de travail devrait s'attacher à identifier les exigences liées à la reconnaissance juridique et qu'il ne devrait pas traiter d'aspects techniques car ceux-ci évoluaient constamment. Il a en outre été indiqué que les travaux du Groupe de travail ne devraient ni introduire de nouvelles obligations en matière d'identification ni modifier celles qui existaient déjà (voir également par. 110 ci-dessous).

23. Il a été dit que la reconnaissance juridique des systèmes de gestion de l'identité pourrait réduire les coûts des opérations dans la mesure où les justificatifs délivrés dans le cadre d'un système donné seraient reconnus sans qu'il soit besoin d'autre vérification. Il a également été dit que tout mécanisme efficace de reconnaissance juridique devrait éliminer la nécessité d'une double vérification, par exemple à la fois dans le pays d'origine et dans le pays requis.

24. Il a été indiqué que la toute première question à aborder concernait l'objet de la reconnaissance juridique. Celle-ci pourrait en effet porter sur les systèmes de gestion de l'identité, les justificatifs d'identité ou les résultats du processus d'identification (voir également A/CN.9/WG.IV/WP.153, par. 57 et 58).

25. Il a été dit qu'en faisant porter la reconnaissance juridique sur les résultats du processus d'identification, on pourrait mieux prendre en compte différentes démarches en matière d'identification, en particulier dans les pays où aucune référence n'était faite à la notion de niveau de garantie. Il a été ajouté que la reconnaissance juridique des résultats était nécessaire pour surmonter les problèmes de réciprocité susceptibles de se poser à l'égard de la reconnaissance juridique des systèmes de gestion de l'identité.

26. Par ailleurs, il a été expliqué que la reconnaissance des systèmes de gestion de l'identité pourrait faciliter la reconnaissance des justificatifs, qui pourrait elle-même faciliter la reconnaissance de l'opération pour laquelle les justificatifs étaient mis en œuvre, c'est-à-dire les résultats du processus d'identification. Il a donc été indiqué qu'il y avait une complémentarité dans la reconnaissance juridique de tous ces éléments. Il a été ajouté que, lorsque la reconnaissance des systèmes de gestion de l'identité serait impossible, il devrait être possible de reconnaître les justificatifs ou les résultats du processus d'identification.

27. Il a été ajouté que les systèmes de gestion de l'identité, aussi bien publics que privés, étaient largement utilisés et qu'il était impératif de disposer d'une description harmonisée des niveaux de garantie applicables, reposant sur un ensemble de règles et de principes, pour assurer la reconnaissance juridique de ces systèmes et renforcer la confiance des partenaires commerciaux.

28. Il a été indiqué qu'une autre question préalable concernait les effets de la reconnaissance juridique. Il a été fait référence aux options énumérées au paragraphe 55 du document A/CN.9/WG.IV/WP.153. En réponse à une question, il a été expliqué que les mots « l'octroi du même statut juridique que dans le pays requis, indépendamment de tout élément d'extranéité » qui figuraient dans ce paragraphe renvoyaient au fait d'accorder la reconnaissance juridique sans tenir compte des éléments d'extranéité qui pourraient être présents (principe du « traitement national »).

29. On s'est inquiété de ce que la référence à la notion de pays d'origine qui figurait au paragraphe 55 du document A/CN.9/WG.IV/WP.153 pourrait enfreindre le principe de la neutralité des systèmes en matière de reconnaissance juridique internationale de l'identité numérique, en sous-entendant l'utilisation obligatoire de justificatifs et de systèmes de gestion de l'identité publics. À ce sujet, il a été dit que cette notion renvoyait au droit applicable au système de gestion de l'identité mis en œuvre, qui pouvait aussi être multinational, indépendamment de sa nature privée ou publique.

30. Il a été dit qu'il était préférable d'accorder un traitement national, dans la mesure où la présence d'un élément d'extranéité ne devrait pas en soit constituer un motif de discrimination dans le commerce international. Il a été ajouté que les juges et autres autorités pourraient faire face à des difficultés s'ils devaient appliquer des lois et des concepts juridiques étrangers, ce qui était une raison supplémentaire de privilégier une telle démarche.

31. Il a également été dit que, compte tenu de l'existence d'ensembles nationaux d'exigences applicables aux systèmes de gestion de l'identité, on ne pouvait aborder la reconnaissance juridique qu'en définissant ses effets juridiques dans un instrument propre.

32. Selon un autre point de vue, les effets de la reconnaissance juridique dépendraient de la fiabilité du système de gestion de l'identité mis en œuvre. À cet égard, il a été expliqué que l'utilisation d'un système respectant un niveau de garantie plus élevé faciliterait sa reconnaissance juridique internationale.

33. Il a été indiqué qu'il faudrait fournir des éclaircissements supplémentaires à propos des effets juridiques de la reconnaissance. Par exemple, il a été proposé de préciser si la limitation légale de la responsabilité d'un prestataire de services d'identité en vertu d'un droit national donné choisi par les parties à une transaction commerciale pourrait être maintenue dans un autre pays et, le cas échéant, dans quelles conditions.

34. La question a été posée de savoir quelle entité devrait mener les éventuelles évaluations nécessaires à la reconnaissance juridique. Il a été souligné que la plupart des opérations commerciales ne faisaient pas intervenir de pouvoirs publics. À ce sujet, il a été dit que les évaluations pourraient être menées par des entités publiques, par des tiers accrédités, par des organisations spécialisées ou par les parties à l'opération commerciale.

35. Il a en outre été indiqué que, si l'évaluation nécessaire à la reconnaissance juridique pouvait être menée par des parties privées, il fallait néanmoins disposer d'un cadre législatif habilitant prévoyant la reconnaissance juridique. Il a été ajouté qu'en l'absence d'un tel cadre, il se pourrait que l'accord des parties sur la loi applicable à l'identification ne puisse pas être respecté.

36. En réponse à une question, il a été précisé que les projets de dispositions figurant dans les documents de travail dont le Groupe de travail était saisi avaient un caractère illustratif (utile au début des délibérations du Groupe), sans préjudice de la possibilité qu'ils soient examinés de manière détaillée ultérieurement.

37. Il a été expliqué que la décision de reconnaître les systèmes de gestion de l'identité était fondée sur la confiance, et que les éléments essentiels nécessaires pour instaurer cette confiance constituaient la question fondamentale dont le Groupe de travail devait débattre. Il a en outre été expliqué que la confiance pouvait découler de l'expérience ou de la participation à une activité dans un climat de confiance. Il a été estimé que la mise à profit d'un climat de confiance pourrait promouvoir un niveau plus élevé de sécurité juridique et que le Groupe de travail devrait donc s'employer à créer un tel climat en définissant ses éléments essentiels. Il a été dit que ces éléments essentiels comprenaient l'ensemble minimum de règles appropriées sur la manière dont les systèmes de gestion de l'identité devraient fonctionner, notamment en matière d'audit, d'assurance, de certification, de responsabilité et de résiliation ou d'autres changements dans les niveaux de garantie, ainsi que les mécanismes visant à garantir et vérifier l'application de ces règles par les participants. Il a été indiqué qu'un tel climat de confiance permettrait aux acteurs économiques de se fier aux résultats des systèmes de gestion de l'identité et d'en tenir compte.

38. Il a été souligné que les besoins des pays en développement devraient être dûment pris en considération afin d'assurer la compatibilité de tous les résultats des travaux avec tous les systèmes économiques et juridiques et tous les niveaux de développement. Il a été rappelé que l'un des objectifs était de promouvoir le commerce électronique avec la participation des pays en développement. Il a été indiqué que l'application intégrale du principe de neutralité technologique était souhaitable pour empêcher l'adoption de prescriptions techniques trop coûteuses ou trop complexes pour les commerçants des pays en développement.

39. Il a été souligné que les systèmes de notification n'étaient pas une solution de substitution aux niveaux de garantie. Il a été expliqué que le processus de notification impliquait la notification des systèmes de gestion de l'identité selon des normes préétablies comme étape suivant la détermination d'un ensemble minimum de règles et l'évaluation des systèmes de gestion de l'identité par rapport à ces règles. Un exemple régional associant des systèmes de notification et des niveaux de garantie a été donné. Il a été expliqué que cet exemple pourrait être reproduit à des fins purement privées sans la participation des pouvoirs publics.

40. S'agissant de mécanismes de reconnaissance juridique particuliers, il a été suggéré que le Groupe de travail se concentre sur la création d'un environnement de confiance à la fois centralisé et minimal, dont les membres parviendraient à un consensus sur les règles et principes qui sous-tendraient cet environnement. Toutefois, l'avis a également été exprimé que, si cela était souhaitable en théorie, il ne serait pas réaliste de prévoir la création d'un organe supranational qui remplirait de telles fonctions.

41. Selon un autre avis, le Groupe de travail devait envisager un mécanisme de reconnaissance juridique fondé sur une mise en correspondance (aussi désignée en tant que mappage) et une liste blanche des systèmes d'accréditation publics et privés existants par rapport à des paramètres à déterminer. Il a été expliqué que de tels paramètres pour les systèmes privés pourraient inclure, par exemple, les exigences en matière d'audit et d'assurance, et que la liste des systèmes agréés ne serait pas exhaustive.

42. Les avis ont divergé sur la question de savoir s'il faudrait adopter l'approche *ex ante*, l'approche *ex post* ou l'approche fondée sur la mise en correspondance, examinées aux paragraphes 61 à 92 du document A/CN.9/WG.IV/WP.153. Les aspects positifs et négatifs de chaque approche ont été illustrés. Il a été jugé important que le Groupe de travail recense les caractéristiques de chaque approche acceptables par tous les États ainsi que les questions posant problème.

43. Selon un avis, l'approche fondée sur la mise en correspondance était préférable en raison de la souplesse qu'elle offrait en permettant une reconnaissance juridique à la fois *ex ante* et *ex post*. Selon un autre avis, il convenait de souligner les avantages de la reconnaissance *ex post*, étant donné qu'il ne serait pas facile de parvenir à l'applicabilité juridique dans les pays dépourvus d'un système de gestion de l'identité. Il a été estimé qu'en raison de considérations liées aux coûts, entre autres, les utilisateurs commerciaux dans les pays en développement pourraient favoriser des

mécanismes de reconnaissance juridique ne fonctionnant qu'en cas de litige, c'est-à-dire sur la base de l'approche *ex post*.

44. Selon l'avis qui a prévalu, il était prématuré et peu souhaitable de choisir entre ces trois approches : prématuré en raison de l'expérience insuffisante de leur utilisation, et peu souhaitable dans la mesure où toutes les options devraient être conservées afin d'offrir un choix plus large aux agents économiques.

45. En outre, ce choix a été jugé prématuré en raison également de la nécessité de recenser dans un premier temps les obstacles à la reconnaissance des systèmes de gestion de l'identité à l'échelle internationale. Il a été expliqué que, malgré l'hypothèse largement répandue selon laquelle, s'agissant des transactions, il était bénéfique et, dans certains cas, nécessaire que les partenaires commerciaux aient un niveau de confiance plus élevé dans l'identité des autres partenaires, il existait peu de mécanismes de reconnaissance internationale des systèmes de gestion de l'identité. Il a été ajouté qu'il pouvait y avoir différentes raisons à cette situation, par exemple le manque d'informations sur le système de gestion de l'identité du pays d'origine ou le fait que les résultats de l'évaluation étrangère du système de gestion de l'identité n'étaient pas comparables ou compréhensibles. Il a été jugé essentiel de mettre en évidence ces raisons pour trouver des solutions juridiques appropriées. En réponse, on s'est demandé s'il existait vraiment des obstacles ou si les partenaires commerciaux s'accommodaient du statu quo.

46. On a aussi fait valoir que toute solution devrait être non exclusive et faciliter la mise au point et l'application d'autres options, tout en respectant les prescriptions juridiques de tel ou tel pays ou région. Il a été noté que les incidences financières pourraient déterminer l'approche qui s'imposerait.

47. Il a été expliqué que ces approches ne s'excluaient pas mutuellement : par exemple, l'approche fondée sur la mise en correspondance permettait une évaluation à la fois *ex ante* et *ex post* des systèmes de gestion de l'identité par rapport à un ensemble prédéterminé de règles. Il a été ajouté que la reconnaissance juridique *ex ante* était souvent utilisée pour les niveaux de garantie supérieurs, tandis que la reconnaissance juridique *ex post* était utilisée pour les niveaux de garantie inférieurs. Il a été noté que les présomptions légales et la charge de la preuve varieraient en fonction du niveau de garantie et seraient connues des parties à l'avance pour leur permettre d'évaluer les conséquences du recours à une approche particulière.

48. Des doutes ont été exprimés sur le point de savoir si l'approche fondée sur la mise en correspondance était une approche distincte. Certaines délégations ont considéré que la mise en correspondance constituait une étape dans la reconnaissance juridique *ex ante* et *ex post*. D'autres délégations ont estimé qu'elle était une variante de l'approche *ex ante* car elle présupposait l'existence de règles communes convenues à l'avance par les participants au processus de mise en correspondance, ainsi que la participation d'une autorité centrale publique ou privée à l'évaluation.

49. Différents avis ont été exprimés sur la participation des pouvoirs publics à un mécanisme de reconnaissance juridique. Selon un avis, elle était souhaitable pour appuyer les systèmes de gestion de l'identité offrant un degré de confiance plus élevé. Il a été ajouté qu'elle pourrait être utile pour éviter que les grands acteurs du marché n'imposent des normes techniques aux plus petits. Il a également été indiqué que la mise en place d'un mécanisme de reconnaissance internationale impliquait nécessairement la participation des pouvoirs publics en raison de son caractère transnational.

50. Selon un autre avis, la participation des pouvoirs publics aux opérations commerciales ou l'adoption d'autres formes de contrôle central sur ces transactions devaient être limitées. Il a été noté qu'un commerce électronique transfrontière important s'effectuait déjà sans cette participation. Il a été proposé que soient communiquées d'autres données d'expérience pour justifier un rôle accru des pouvoirs publics dans la reconnaissance internationale des systèmes de gestion de l'identité. Il a été réaffirmé que les travaux sur la gestion de l'identité ne devaient pas partir du principe que les systèmes de gestion de l'identité et leur reconnaissance juridique seraient nécessairement ou principalement fondés sur la participation des

pouvoirs publics et que, dans le contexte du commerce interentreprises, l'accent devait plutôt être mis sur des mécanismes privés de gestion de l'identité et de reconnaissance.

51. Un appui a été exprimé en faveur de la collecte d'un plus grand nombre d'informations sur la manière dont les différentes approches fonctionnaient dans la pratique. Pour faire suite à cette remarque, il a été noté que la CNUDCI avait élaboré plusieurs textes concluants dans le domaine du commerce électronique sur la base d'une pratique commerciale limitée en raison du caractère novateur de ce domaine. Il a été ajouté qu'un texte de la CNUDCI sur les systèmes de gestion de l'identité et les services de confiance pourrait sensiblement contribuer à modifier la structure du marché et donner une nouvelle impulsion à l'utilisation de ces services.

52. Sur ce point, il a été fait observer qu'il ressortait de l'expérience de la CNUDCI que les instruments qu'elle élaborait étaient particulièrement utiles lorsqu'ils traitaient d'un problème juridique touchant les milieux d'affaires qui avait été mis en évidence à partir de connaissances empiriques plutôt que théoriques. Il a été suggéré d'établir une liste des problèmes concrets que la CNUDCI devrait s'efforcer de traiter dans le cadre de ses travaux sur la gestion de l'identité. On a notamment évoqué l'existence de lois et approches divergentes dans ce domaine, qui entraînait des coûts supplémentaires pour les entreprises, problème auquel il faudrait remédier par une harmonisation des lois, tâche qui relevait du mandat de la CNUDCI. Un autre problème cité était que, dans certains cas, une partie contractante pouvait être tenue d'utiliser un document d'identification papier pour conclure une transaction commerciale en ligne. On a ajouté qu'une identification inappropriée de la partie contractante pouvait être source de problèmes à l'étape de l'exécution du contrat. Il a également été noté que l'identification transfrontière en ligne posait problème.

53. En réponse à une question, il a été expliqué que la partie du Règlement eIDAS relative aux services de confiance était entrée en vigueur en 2016 et celle relative à la gestion de l'identité en septembre 2018. On a ajouté que, si l'on ne disposait pas encore de données sur les effets du Règlement sur le développement du marché de la gestion de l'identité, étant donné sa récente entrée en vigueur, les effets sur le développement du marché des services de confiance étaient déjà considérables.

54. En réponse à une autre question, il a été expliqué que le processus de mise en correspondance était complexe et prenait beaucoup de temps en raison notamment des difficultés qu'il y avait à comparer des systèmes de gestion de l'identité développés à partir d'ensembles de règles différents. Il a été ajouté que l'évaluation des systèmes de gestion de l'identité était également coûteuse et devait être répétée régulièrement, généralement à un rythme annuel. Il a été dit que le fréquent changement des niveaux de garantie constituait une difficulté supplémentaire. Il a en outre été mentionné que l'offre de services du secteur privé en matière d'évaluation des systèmes de gestion de l'identité ne semblait pas indiquer une forte demande pour ce genre de services. On a par conséquent émis des doutes quant à la possibilité qu'une approche fondée sur la mise en correspondance puisse fonctionner à l'échelle mondiale. Selon un autre avis, le processus de mise en correspondance que certains États effectuaient au niveau bilatéral était très utile, même s'il prenait beaucoup de temps.

55. Le Groupe de travail s'est accordé à dire que, s'il était prématuré de prendre une décision quant au mécanisme de reconnaissance juridique qu'il conviendrait de retenir, il devait poursuivre l'examen des avantages et des inconvénients de chaque modèle, individuellement et de manière groupée.

C. Niveaux de garantie

56. Le Groupe de travail a examiné divers aspects de l'utilisation des niveaux de garantie dans la gestion de l'identité. Il a été expliqué que le niveau de garantie était un indicateur du niveau de confiance dans l'identification d'une entité. On a ajouté que la référence à ces niveaux était essentielle pour permettre aux mécanismes de reconnaissance juridique de fonctionner et qu'il faudrait s'efforcer d'en harmoniser la description. Par ailleurs, on a expliqué que le nombre de niveaux de garantie à

prévoir correspondait au nombre d'effets juridiques recherchés, de sorte que, par exemple, s'il y avait deux effets associés à un système de gestion de l'identité (par exemple reconnaissance ou non-reconnaissance), il y aurait deux niveaux de garantie correspondants. On a ajouté que l'utilisation de niveaux de garantie posait des difficultés, notamment la nécessité de faire correspondre ces niveaux entre plusieurs pays et de les actualiser fréquemment.

57. Le point de vue a été exprimé qu'il était trop tôt pour examiner la définition des niveaux de garantie et que cela risquait de faire intervenir des questions techniques. Un large soutien a été exprimé en faveur de l'opinion selon laquelle ce genre de questions n'entraient pas dans le cadre des travaux du Groupe de travail. On a ajouté qu'il faudrait faire preuve de prudence car les discussions d'ordre juridique pouvaient avoir des incidences importantes sur les solutions technologiques. Il a été estimé que si l'avancement des travaux l'exigeait, on pourrait solliciter l'assistance d'organisations internationales compétentes telles que l'Union internationale des télécommunications.

58. Toutefois, il a également été dit que la mise en place d'un mécanisme de reconnaissance juridique exigerait de relier les effets juridiques aux propriétés, caractéristiques et attributs du système de la gestion de l'identité. On a ajouté que ce processus devrait être axé sur les résultats et non prescriptif, et devrait viser à assurer l'interopérabilité entre les niveaux de garantie.

59. Il a été dit qu'en examinant la question des niveaux de garantie, il faudrait préciser les conséquences juridiques de la référence à ces niveaux et que les autres conséquences n'étaient pas pertinentes pour les travaux du Groupe de travail. À cet égard, il a été indiqué que la notion de niveaux de garantie avait des conséquences juridiques différentes pour les systèmes de gestion de l'identité et les services de confiance. Il a également été indiqué que différents niveaux de garantie produisaient des effets juridiques différents, qui répondaient à différents besoins des entreprises.

60. L'avis a été exprimé qu'il fallait associer les niveaux de garantie à des effets juridiques distincts. Selon un autre avis, il n'était pas possible d'associer ces niveaux à tous les effets juridiques possibles. À cela, il a été répondu qu'il était possible et même souhaitable de définir un ensemble minimal d'effets juridiques associés à chaque niveau de garantie.

61. On s'est posé la question de savoir quels effets juridiques étaient associés à l'utilisation des niveaux de garantie. Divers exemples ont été fournis. On a indiqué que le principal effet juridique obtenu était l'association d'un niveau de garantie à la fiabilité de l'identification d'une personne ou d'un objet (c'est-à-dire identification fiable au-delà de tout doute raisonnable, identification fiable selon des critères de probabilité ou échec de l'identification), qui était la notion clef du processus d'identification.

D. Équivalence fonctionnelle

62. Il a été reconnu qu'en formulant le principe de l'équivalence fonctionnelle, la CNUDCI avait fourni une contribution importante au développement du commerce électronique, et l'avis a été exprimé qu'il conviendrait peut-être d'adapter ce principe au contexte de la gestion de l'identité. Il a été dit que, s'il était aisé d'identifier les fonctions spécifiques liées aux notions d'« écrit », d'« original » et de « signature manuscrite », il était en revanche difficile de mettre en évidence les fonctions précises visées par la gestion de l'identité. À cet égard, il a été noté que l'identification pouvait constituer une fonction en soi. La préoccupation concernant les efforts visant à établir une équivalence fonctionnelle entre l'identification hors ligne et l'identification en ligne, exprimée précédemment au cours de la session (voir par. 15 ci-dessus), a de nouveau été soulevée.

63. Il a été dit que les dispositions sur la gestion de l'identité pourraient devoir faire référence aux niveaux de garantie, au degré de fiabilité ou aux niveaux d'équivalence et qu'il faudrait donc peut-être établir, pour chaque niveau de garantie, des dispositions ayant des effets juridiques différents. Il a été souligné que la recherche

d'une solution « universelle », démarche adoptée dans les dispositions existantes de la CNUDCI établissant l'équivalence fonctionnelle, pourrait donc devoir être écartée dans le contexte de la gestion d'identité.

64. Des exemples précis ont été fournis pour illustrer la relation entre l'équivalence fonctionnelle et la référence à des niveaux de garantie dans la gestion de l'identité. Il a été expliqué que différents niveaux de garantie de l'identification pourraient être exigés, conformément soit à la loi soit à un contrat, également dans le monde hors ligne. Il a été dit qu'il n'existait pas de correspondance exacte et uniforme entre chaque niveau de garantie et l'identification hors ligne.

65. Selon un autre point de vue, les dispositions sur l'équivalence fonctionnelle ne devraient pas faire référence à des niveaux de garantie, car on touchait là à des aspects techniques qui dépassaient le mandat de la CNUDCI tel qu'il avait été examiné plus tôt durant la session (voir par. 57 ci-dessus). Conformément à l'autre opinion exprimée, il était utile de faire état de niveaux de garantie et les dispositions devraient être reformulées pour mieux faire comprendre que chaque niveau produirait des effets juridiques différents.

66. On s'est demandé si les dispositions relatives à l'équivalence fonctionnelle auraient pour objet d'établir l'équivalence du statut juridique des processus de gestion de l'identité en ligne et hors ligne. Il a été souligné que, pour parvenir à cette équivalence, il faudrait peut-être maintenir dans les dispositions un lien avec les processus de gestion de l'identité hors ligne. Les avis ont divergé sur les moyens d'établir ce lien.

67. Le point de vue a été exprimé que, contrairement aux dispositions sur l'équivalence fonctionnelle figurant dans des textes existants de la CNUDCI qui mettaient l'accent soit sur une chose (signature, écrit ou original) soit sur une situation (possession), les dispositions sur l'équivalence fonctionnelle dans le contexte de la gestion de l'identité devraient peut-être porter sur le processus lui-même. Il a été ajouté que, si les dispositions actuelles de la CNUDCI sur l'équivalence fonctionnelle visaient à confirmer la validité, il pourrait être utile, dans le contexte de la gestion de l'identité, non seulement de rechercher une réponse binaire à la question de la reconnaissance juridique, mais aussi de clarifier les effets juridiques de cette reconnaissance.

68. On s'est demandé si le fait de formuler des dispositions spécifiques sur l'équivalence fonctionnelle pour chaque niveau de garantie reviendrait à établir des règles sur la gestion de l'identité et irait donc au-delà du principe de l'équivalence fonctionnelle. Il a été estimé que le projet de disposition figurant au paragraphe 29 du document A/CN.9/WG.IV/WP.153 pourrait avoir cet effet.

69. Un certain soutien a été exprimé en faveur de l'opinion selon laquelle il était prématuré d'examiner des dispositions sur l'équivalence fonctionnelle tant que la portée des travaux sur la gestion de l'identité n'aurait pas été précisée, en particulier tant que l'on n'aurait pas déterminé si ces travaux visaient à obtenir la reconnaissance juridique des processus de gestion de l'identité ou des résultats de ces processus. Il a été noté que les dispositions en matière d'équivalence fonctionnelle ne s'appliqueraient que si la gestion de l'identité était pertinente pour l'environnement papier. En outre, il a été proposé de faire porter les débats sur une méthode d'identification acceptable plutôt que d'essayer d'élaborer des dispositions étroites en matière d'équivalence fonctionnelle avec les documents ou les processus d'identification de l'environnement papier. On a également fait valoir que l'examen de toute proposition rédactionnelle devrait se faire sans préjudice d'une décision du Groupe de travail sur la forme d'un éventuel texte futur sur la gestion de l'identité.

70. À titre préliminaire, il a été noté que le libellé liminaire du projet de disposition figurant au paragraphe 29 du document A/CN.9/WG.IV/WP.153 était trompeur car, dans le contexte du commerce interentreprises, le droit n'exigeait ou n'autorisait d'identification explicite qu'en de rares occasions. Il a été expliqué que les obligations de s'identifier de manière appropriée dans le contexte du commerce interentreprises pourraient être implicites ou simplement dictées par les besoins des entreprises.

71. Il a été proposé de reformuler la disposition comme suit, pour tenir compte du fait que des prescriptions juridiques et des niveaux de garantie différents pourraient s'appliquer et qu'il faudrait décider si la portée des travaux engloberait non seulement des personnes, mais aussi des objets :

> « Lorsque la loi exige ou permet l'identification d'une [entité] [personne] [d'une certaine manière], 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] [personne] [au même niveau ou de la même manière]]. »

72. On a souligné qu'il fallait définir certains des termes utilisés dans le libellé proposé, notamment « une méthode fiable ». Il a également été proposé de scinder la disposition en deux parties, dont l'une contiendrait le principe de l'équivalence fonctionnelle et l'autre traiterait de la fiabilité. Des doutes ont été exprimés quant au fait que la disposition couvrait tous les éléments de la gestion de l'identité, et la nécessité de les prendre tous en compte a été soulignée ; en effet, une défaillance de l'un quelconque des maillons de la chaîne de la gestion de l'identité risquait de compromettre le résultat.

73. Il a été proposé de reformuler comme suit le projet de disposition figurant au paragraphe 29 du document A/CN.9/WG.IV/WP.153, s'il s'agissait d'établir une équivalence fonctionnelle avec un document d'identification matériel existant dans l'environnement papier (c'est-à-dire avec une chose) :

> « Lorsque la loi exige ou permet l'identification d'une personne à l'égard d'un document matériel, cette exigence est satisfaite, dans le cas d'un processus de gestion de l'identité électronique, si une méthode fiable est employée pour vérifier les attributs pertinents de la personne contenus dans le document. »

74. Il a été indiqué que la gestion de l'identité était une notion juridique complexe et que, si les dispositions devaient établir une équivalence fonctionnelle du processus de gestion de l'identité, tous les éléments le composant (par exemple, l'identification et l'authentification) devraient être pris en compte. Il a été suggéré de reformuler le projet de dispositions contenu au paragraphe 29 du document A/CN.9/WG.IV/WP.153 comme suit, par exemple, afin d'y insérer une référence à un « niveau de garantie » requis par le droit matériel :

> « Lorsque la loi exige ou permet l'identification d'une personne selon des critères de probabilité, cette exigence est satisfaite, dans le cas d'un processus d'identification électronique, si une méthode fiable est employée pour vérifier les attributs pertinents de cette personne à un niveau équivalent. »

75. Différents avis ont été exprimés au sujet des propositions rédactionnelles contenues aux paragraphes 73 et 74 ci-dessus. D'une part, on a posé la question de savoir s'il serait souhaitable de faire expressément référence à un document matériel ou papier. On a expliqué que dans l'environnement physique, l'autorité chargée d'identifier les personnes (par exemple, un registre) ne produisait pas nécessairement de documents d'identification matériels, mais pouvait être la source faisant autorité pour les informations d'identification. On a aussi expliqué que la loi ne préciserait pas nécessairement s'il convenait d'utiliser des moyens d'identification sur papier ou d'autres moyens. D'autre part, on a estimé que la notion de « critères de probabilité » (« balance of probabilities » en anglais) n'était ni connue, ni claire. On a suggéré de la remplacer par une référence au niveau d'équivalence.

76. Certains ont jugé que la proposition énoncée au paragraphe 73 ci-dessus était trop limitée, car elle visait uniquement à établir une équivalence fonctionnelle entre les documents d'identification sur papier et les moyens d'identification électroniques. Pour ces raisons, certains ont préféré la proposition énoncée au paragraphe 74 ci-avant.

77. Compte tenu de ces commentaires, on a formulé une autre proposition rédactionnelle, qui entendait répondre aux préoccupations exprimées au sujet des projets de dispositions contenus aux paragraphes 73 et 74 ci-dessus en les fusionnant et en les reformulant :

« Lorsque la loi ou les parties exigent l'identification de l'entité ou de la personne selon une certaine méthode, cette exigence est satisfaite, dans le cas de la gestion de l'identité électronique, si une méthode fiable est employée pour vérifier les attributs pertinents de cette entité à un niveau équivalent à celui assuré par cette méthode. »

78. Une autre proposition rédactionnelle se lisait comme suit :

« Lorsque les parties souhaitent procéder à l'identification [d'une personne] [d'un sujet] ou qu'elles y sont tenues par la loi, l'application d'une procédure d'identification électronique à cet effet a un effet juridique équivalent à celui de l'application de procédures non électroniques reconnues à cet effet, pour autant que la procédure d'identification électronique emploie une méthode fiable pour vérifier les attributs [de la personne] [du sujet] qui sont pertinents à cette fin. »

79. Rappelant que certains textes de la CNUDCI contenaient déjà des règles d'équivalence fonctionnelle pour certains services de confiance, à savoir pour les signatures électroniques et pour la conservation et l'archivage, le Groupe de travail s'est demandé s'il conviendrait d'élaborer des dispositions spécifiques pour chaque type de service de confiance, ou si l'autre approche qui consisterait à rédiger une règle générale sur l'équivalence fonctionnelle de la gestion de l'identité pour l'ensemble de ces services serait possible ou souhaitable. Selon l'avis qui l'a emporté, il faudrait élaborer des dispositions d'équivalence fonctionnelle spécifiques pour chaque type de service pour tenir compte de ses fonctions particulières et, pour ce faire, établir une liste des services de confiance.

80. On a souligné l'importance de la numérisation de l'identité des personnes morales pour les transactions transfrontières. On a dit que les travaux du Groupe de travail sur la gestion de l'identité pourraient avoir pour objet non seulement d'assurer la reconnaissance transfrontière des systèmes de gestion de l'identité, mais aussi de faciliter la dématérialisation de l'identification. On a expliqué que, pour ce second sujet, l'équivalence fonctionnelle demeurait un principe important, tandis que les niveaux de garantie ou les degrés de fiabilité étaient plus pertinents pour la reconnaissance des systèmes de gestion de l'identité. Par ailleurs, on a fait valoir que l'équivalence fonctionnelle était également un concept important parce qu'elle ne demandait aucune modification des exigences de droit matériel.

81. À l'issue de la discussion, il a été décidé de continuer à étudier la question de savoir s'il convenait d'examiner les degrés d'identification ou les niveaux de garantie en parallèle avec des dispositions sur l'équivalence fonctionnelle ou des dispositions concernant une méthode d'identification fiable. On a souligné que des dispositions sur l'équivalence fonctionnelle, les niveaux de garantie et la reconnaissance mutuelle constituaient la base de tout document futur. Par ailleurs, on a dit qu'il pourrait être nécessaire de rédiger ces dispositions en tenant compte de divers éléments, y compris le respect des règlements, l'autonomie des parties, la non-discrimination entre les moyens d'identification en ligne et hors ligne et la reconnaissance transfrontière de l'identification en ligne.

82. Reconnaissant qu'il pourrait tirer parti, pour son examen des dispositions sur l'équivalence fonctionnelle en matière de gestion d'identité, d'exemples concrets dans lesquels la gestion de l'identité était utilisée, le Groupe de travail a entendu des exemples dans lesquels celle-ci était requise dans le contexte interentreprises, en particulier à des fins de respect des règlements (par exemple, le principe « Connaissez votre client »), pour établir la validité d'un document commercial et satisfaire aux obligations contractuelles. On s'est inquiété du fait que la plupart des exemples cités ne renvoyaient pas à des transactions entre entreprises, et que ceux qui y renvoyaient portaient sur des questions liées à la conformité ou au fonctionnement réglementaires dans des secteurs fortement réglementés comme les services financiers. On a en particulier exprimé des doutes quant à la pertinence, pour la gestion de l'identité dans le contexte interentreprises, de l'exemple du principe « Connaissez votre client », puisque les exigences en la matière, y compris celle d'identification du client, visaient à remplir des objectifs spécifiques qui avaient trait à la lutte contre le financement du terrorisme, le blanchiment d'argent et la corruption.

83. On s'est interrogé sur les entités pertinentes pour les travaux du Groupe de travail (voir A/CN.9/WG.IV/WP.153, par. 12). Un appui a été exprimé en faveur de l'avis selon lequel les travaux devaient mettre l'accent sur les relations entre entreprises et viser à faciliter la confiance dans l'identité des partenaires commerciaux. On a expliqué que les opérations avec des entités publiques impliquées dans le commerce (par exemple, dans le contexte de la facilitation du commerce sans papier) seraient aussi pertinentes.

84. On a rappelé que les transactions commerciales pouvaient entrer dans le champ d'application de règlements contenant une obligation d'identification. À cet égard, on a noté qu'il était vraisemblable que les exigences réglementaires aient des incidences sur l'évolution des pratiques commerciales. On a ajouté qu'il y avait peu de chances qu'un document élaboré par le Groupe de travail dans le domaine de la gestion de l'identité soit très pertinent pour les secteurs fortement réglementés.

85. On a reconnu que des systèmes de gestion de l'identité établis dans d'autres contextes que les relations entre entreprises pourraient intéresser les partenaires commerciaux et qu'il conviendrait par conséquent d'en tenir compte dans les travaux du Groupe de travail sur la gestion de l'identité. On a toutefois souligné à nouveau que celui-ci devrait se concentrer avant tout sur la gestion de l'identité dans les transactions entre entreprises.

E. Examen du projet d'instrument et de la feuille de route figurant dans la proposition de l'Allemagne (A/CN.9/WG.IV/WP.155 et Add.1)

86. On a présenté au Groupe de travail la proposition figurant dans les documents A/CN.9/WG.IV/WP.155 et Add.1, en mettant en exergue ses principaux éléments et les objectifs poursuivis. On s'est félicité de cette présentation et de la démarche globale adoptée dans les documents, qui ont été jugés utiles pour la suite des débats.

87. Des éclaircissements ont été demandés en ce qui concerne certaines dispositions présentées dans les documents qui ne semblaient pas applicables aux opérations interentreprises, notamment les exemples d'identification primaire dans le projet d'article 2 et la référence à l'authentification de sites Internet dans le projet d'article 19. On s'est également demandé si les milieux d'affaires avaient manifesté de l'intérêt pour la création et l'appui au fonctionnement du Conseil de coordination évoqué au projet d'article 5, étant entendu que celui-ci pourrait être constitué aussi bien par des acteurs non étatiques que par des États.

88. On s'est inquiété des projets de dispositions qui attribuaient des fonctions législatives au Conseil de coordination, notamment sur des questions soulevant des considérations d'ordre public. Selon un avis, les États étaient souvent réticents à déléguer l'élaboration de règles juridiques sur de tels points à des organismes privés. La question a également été posée de savoir si le mécanisme envisagé dans le document A/CN.9/WG.IV/WP.155 s'appliquerait au contexte national ou international, ou aux deux.

89. En réponse à cette question, il a été précisé que l'identification primaire servait généralement à la création d'une personne morale, tandis que les certificats de sites Internet étaient utilisés dans le contexte du commerce interentreprises, en particulier dans la chaîne de sous-traitance. S'agissant du Conseil de coordination, il a été précisé qu'un tel organisme pourrait faire l'objet d'une gestion publique ou privée. On a cité l'exemple d'un organisme créé dans un pays et jouissant d'un rayonnement international important. Il a été reconnu qu'il serait essentiel que les États participent au Conseil ou interviennent dans le cadre de la validation et de l'application de ses travaux. On a noté que différentes voies pourraient permettre d'atteindre cet objectif, par exemple la conclusion d'un accord international visant à intégrer aux législations nationales le code de conduite élaboré par le Conseil ou la mise en place de mesures incitatives pour encourager son utilisation.

F. Définitions

90. Il a été noté que, compte tenu du débat antérieur du Groupe de travail sur les objets (voir par. 11 et 12 ci-dessus), il faudrait peut-être modifier la définition du terme « identité » qui figurait au paragraphe 17 du document A/CN.9/WG.IV/WP.153. La question a été posée de savoir si cette définition, contrairement à celle du terme « identification », était nécessaire, ou si elle devrait relever du droit national. En réponse, il a été dit que la définition de l'« identité » était également utile.

91. S'agissant de la définition du terme « gestion de l'identité » qui figurait au paragraphe 19 du même document, on s'est inquiété de ce que le libellé actuel pourrait impliquer que la référence cumulée à l'identification, l'authentification et l'autorisation était indispensable pour définir ce concept, alors que l'un ou l'autre des éléments énumérés y suffirait. On a déclaré que la définition du terme « identification électronique » figurant dans le document A/CN.9/WG.IV/WP.144 était préférable.

92. Une question a été posée concernant la signification du terme « environnement », qui apparaissait dans la définition de « système d'identité » au paragraphe 20 du document A/CN.9/WG.IV/WP.153. On a indiqué que la définition du terme « schéma d'identification électronique » figurant dans le document A/CN.9/WG.IV/WP.144 était préférable.

93. Concernant la définition du terme « niveau de garantie », on a proposé de fusionner les projets de disposition figurant aux paragraphes 23 et 24 du document A/CN.9/WG.IV/WP.153 ou de revoir la définition de ce terme à partir du libellé du paragraphe 23. Selon un autre point de vue, il était inutile de définir ce terme.

94. Les avis ont divergé pour ce qui est de savoir si les travaux sur la reconnaissance juridique de la gestion de l'identité devraient concerner les processus de gestion de l'identité ou leurs résultats, ou bien les deux. Selon un avis, il faudrait distinguer les services de confiance de la gestion de l'identité : s'agissant des services de confiance, on chercherait à obtenir la reconnaissance de leurs résultats, tandis que dans le contexte de la gestion d'identité, la reconnaissance porterait sur les processus. Il a donc été proposé que, pour commencer, les travaux portent sur la reconnaissance des processus de gestion de l'identité ; on pourrait par la suite décider d'aborder la reconnaissance des opérations elles-mêmes. Un certain soutien a été exprimé en faveur du principe selon lequel on devrait mener séparément les travaux, d'une part sur la reconnaissance des processus de gestion de l'identité et, d'autre part, sur la reconnaissance des résultats des services de confiance.

95. Selon l'autre point de vue, il serait inopportun de séparer la reconnaissance des résultats de celle des processus. On a rappelé qu'il existait déjà des systèmes de gestion de l'identité mais que la mauvaise connaissance de la qualité des processus sur lesquels ils reposaient empêchait que leurs résultats soient largement reconnus à l'échelle internationale.

96. Selon un autre avis, les travaux devraient porter uniquement sur la reconnaissance des résultats des processus de gestion de l'identité. Selon une autre opinion, s'il fallait effectivement s'attacher à établir l'équivalence des résultats, on ne devait pas pour autant négliger la nécessité de garantir l'adéquation des processus.

97. Selon encore un autre point de vue, dans la pratique, il ne serait pas réaliste de chercher à faire reconnaître chaque résultat de processus de gestion de l'identité et de services de confiance. Il a donc été proposé de faire porter les travaux sur la reconnaissance des processus (c'est-à-dire des ensembles de règles) fondée sur des données factuelles, ce qui pourrait entraîner la reconnaissance automatique de tous les résultats des processus reconnus, éliminant ainsi la nécessité d'essayer d'obtenir la reconnaissance de chaque résultat particulier.

98. De l'avis général, le Groupe de travail devrait s'attacher à la reconnaissance des processus et des résultats dans le contexte aussi bien des systèmes de gestion de l'identité que des services de confiance. Il a été jugé essentiel d'établir un lien entre ce débat et la discussion sur les différentes manières d'aborder le sujet de la reconnaissance juridique (voir sect. B ci-dessus).

99. On s'est inquiété de ce que le Groupe de travail examinait des définitions avant de s'être mis d'accord sur certains points essentiels. Selon un point de vue, à ce stade des travaux, les définitions compilées dans le document A/CN.9/WG.IV/WP.150 étaient utiles et suffisantes. Selon un autre point de vue, il fallait utiliser les termes et définitions figurant dans les documents A/CN.9/WG.IV/WP.144 et A/CN.9/WG.IV/WP.155, soit à la place des termes définis dans les documents A/CN.9/WG.IV/WP.150 et A/CN.9/WG.IV/WP.153, soit en combinaison avec eux.

100. De l'avis général, il fallait parvenir dans un premier temps à une compréhension commune des termes essentiels pour les travaux sur la gestion de l'identité et les services de confiance, et il serait donc utile d'établir une liste de définitions. Par conséquent, le Secrétariat a été prié d'inclure les définitions figurant dans le document A/CN.9/WG.IV/WP.144 dans la liste des définitions essentielles, à des fins de référence. Il a aussi été prié d'inclure dans cette liste des renvois au document A/CN.9/WG.IV/WP.150 et aux définitions contenues dans le document A/CN.9/WG.IV/WP.155. En outre, il a été prié de préciser l'origine des définitions et la mesure dans laquelle le Groupe de travail les avait examinées. Il était entendu que les définitions, ainsi regroupées, seraient préliminaires et modifiées au fur et à mesure de l'avancement des travaux. Selon un avis, le Groupe de travail devrait décider rapidement de la forme du texte juridique à élaborer, afin de faciliter l'avancée des travaux, notamment en ce qui concernait les définitions, et d'éviter les discussions répétitives.

G. Services de confiance

101. Le point de vue a été réaffirmé qu'il faudrait faire référence, en anglais, aux « trusted services », pour éviter toute ambiguïté quant à la notion juridique bien établie de « trust » (voir par. 14 ci-dessus).

102. Le point de vue a été exprimé que la nécessité de créer des mécanismes transfrontières pour la reconnaissance des services de confiance était peu avérée, car ceux-ci faisaient généralement l'objet d'accords contractuels. Il conviendrait par conséquent de limiter les travaux du Groupe de travail dans ce domaine.

103. Selon un autre avis, le marché des services de confiance démontrait clairement la nécessité d'assurer un niveau plus élevé de sécurité juridique concernant l'utilisation transfrontière de ces services. Il a été ajouté que les travaux dans le domaine des services de confiance revêtaient par conséquent une grande importance, et qu'il conviendrait de les mener en parallèle avec les travaux sur la gestion de l'identité.

104. Il a été estimé qu'il faudrait établir une liste non exhaustive de services de confiance qui reposerait sur une définition commune de cette notion. Par ailleurs, on a suggéré d'utiliser la définition du terme « service de confiance » contenue dans le document A/CN.9/WG.IV/WP.144 comme hypothèse de travail pour les délibérations futures.

105. On a indiqué que les services de confiance qui étaient énumérés dans le document A/CN.9/WG.IV/WP.154 sur la base de la législation existante étaient les suivants : signatures électroniques ; cachets électroniques ; horodatages électroniques ; services d'envoi recommandé électronique ; authentification de site Internet ; et archivage électronique. Il a été suggéré d'ajouter à cette liste les services de séquestre électronique. Il a aussi été suggéré d'y ajouter les services de chaîne de blocs. À ce sujet, il a été indiqué que la chaîne de blocs était une technologie, et non un service.

106. Il a été expliqué qu'il ne fallait pas utiliser la notion de niveaux de garantie en ce qui concernait les services de confiance, car des moyens d'identification électronique offrant un niveau de garantie élevé pourraient être utilisés pour des services de confiance présentant des niveaux de fiabilité différents.

H. Autres principes généraux

107. On a souligné l'importance du principe de non-discrimination à l'égard de l'utilisation de moyens électroniques. On a noté que le projet de disposition contenu au paragraphe 26 du document A/CN.9/WG.IV/WP.153 posait problème en ce qu'il traitait de la vérification de l'identité tant pour la gestion de l'identité que pour les services de confiance. Il a été estimé qu'il faudrait modifier le libellé pour éviter toute confusion, ou élaborer deux dispositions distinctes portant respectivement sur la gestion de l'identité et les services de confiance.

108. Il a été estimé qu'il faudrait remplacer, dans les projets de dispositions relatifs à la non-discrimination, toute référence à un élément du processus par une référence aux résultats de ce processus. À cet égard, il a été estimé que les dispositions relatives à la gestion de l'identité devraient faire référence aux « résultats de la vérification de l'identité », et celles relatives aux services de confiance aux « résultats de l'application de services de confiance ».

109. S'agissant des propositions rédactionnelles relatives à l'autonomie des parties et du commentaire y relatif, on a proposé les changements suivants : a) modifier le projet de disposition contenu au paragraphe 42 du document A/CN.9/WG.IV/WP.153 pour tenir compte des réflexions du Groupe de travail au sujet de la portée des travaux (personnes ou objets ; voir par. 11 et 12 ci-dessus) ; b) remplacer l'expression « personne qui en a le contrôle », au paragraphe 44 de ce document, par les mots « personne juridiquement responsable », étant entendu que la personne qui aurait le contrôle de l'objet ne serait pas nécessairement la personne juridiquement responsable de celui-ci ; et c) identifier les règles fondamentales que les parties ne pourraient modifier et auxquelles elles ne pourraient déroger, afin d'augmenter la sécurité et la prévisibilité de la reconnaissance transfrontière de la gestion de l'identité et des services de confiance.

110. S'agissant d'une proposition rédactionnelle concernant le principe de l'absence de nouvelle obligation d'identification, on a fait observer qu'il existait un lien étroit entre cette disposition et le principe de l'autonomie des parties. Il a été expliqué que le principe de l'absence de nouvelle obligation d'identification était plus large que le principe de l'autonomie des parties, car il signifiait également qu'aucune modification du droit matériel n'était envisagée. Toutefois, on a aussi noté que de nouvelles obligations d'identification pourraient survenir du fait de l'utilisation d'un service de confiance particulier mais que, en tout état de cause, l'utilisation de ce service devrait se faire à titre volontaire (voir également par. 22 ci-dessus).

111. On a souligné l'importance des travaux sur la gestion de l'identité et les services de confiance pour permettre la production de preuves à l'échelle internationale. On a aussi mis l'accent sur le fait que les accords contractuels étaient subordonnés aux règles de droit impératives.

I. Certification des prestataires de services de gestion de l'identité et de services de confiance

112. L'avis a été exprimé que, dans le contexte du commerce interentreprises, il conviendrait d'offrir toutes les options de certification, qui comprenaient : l'absence de certification ; l'autocertification ; la certification par un tiers indépendant ; la certification par un tiers indépendant accrédité ; et la certification par un organisme public. Il a été expliqué que les partenaires commerciaux devraient être en mesure de choisir l'option la mieux adaptée à leurs besoins, étant entendu que chaque option aurait des effets juridiques différents. Il a en outre été expliqué qu'une éventuelle architecture à l'appui de cette certification volontaire n'impliquerait pas nécessairement l'intervention d'entités publiques mais pourrait reposer sur une certification indépendante.

113. Une question a été soulevée sur la manière dont les résultats de cette certification par un tiers seraient reconnus à l'échelle internationale autrement que par l'application d'une clause contractuelle. On a répondu en citant l'International

Accreditation Forum comme exemple d'organisme qui facilitait la reconnaissance des certificats.

114. On a exprimé la crainte que toute solution présupposant l'intervention d'un organisme central de certification, d'accréditation ou de supervision puisse ne pas convenir lorsque la technologie du registre distribué était utilisée dans les services de gestion de l'identité et les services de confiance, en raison des difficultés à identifier l'organisme qualifié pour demander la certification et celui chargé de l'évaluation, entre autres choses. Il a été noté que le régime de responsabilité dans ces situations n'était pas clair non plus.

115. Selon un avis, les dispositions relatives à la certification ne devaient pas imposer une charge excessive aux prestataires de services de gestion de l'identité. En outre, il a été dit que le contrôle exercé par l'État sur les activités des organismes de certification du secteur privé était essentiel pour prévenir les risques en matière de concurrence et les abus, en particulier en ce qui concernait les petits acteurs du marché. Il a été indiqué que l'accréditation des organismes de certification auprès des pouvoirs publics visait à garantir l'indépendance, l'impartialité et l'équité. À cet égard, on a estimé qu'une autorité indépendante serait peut-être mieux à même d'atteindre ces objectifs.

J. Responsabilité

116. Il a été expliqué que la question de la responsabilité pourrait être traitée de différentes manières en fonction de la portée des travaux. D'une part, si l'objectif était de faciliter la reconnaissance internationale des services de gestion de l'identité et des services de confiance, il serait nécessaire de déterminer la loi applicable. D'autre part, si l'objectif était de fournir des orientations au niveau national, par exemple sous la forme d'une loi type, il pourrait être nécessaire d'examiner la question du partage des responsabilités, en gardant à l'esprit que les parties elles-mêmes pourraient décider de cette question. Dans ce dernier cas, a-t-on ajouté, une discussion sur la limitation de la responsabilité pourrait également être nécessaire.

117. Il a été indiqué qu'en règle générale les prestataires de services devraient être tenus responsables des services qu'ils fournissaient. Il a été ajouté que ce principe devrait s'appliquer à la fois aux prestataires de services de gestion de l'identité et aux prestataires de services de confiance. Il a été expliqué que des services de meilleure qualité étaient fournis à un coût plus élevé et que, pour cette raison, il était possible de présumer l'intention ou la négligence des prestataires de ces services en cas de dommage découlant de l'utilisation de ces derniers.

118. Rappelant que les travaux du Groupe de travail étaient axés sur l'identité de transaction, une question a été soulevée au sujet de la responsabilité éventuelle des entités publiques. Il a été expliqué que celles-ci pourraient être tenues responsables en tant qu'autorités de surveillance et prestataires de services. Il a été ajouté que la question de leur responsabilité pourrait également se poser lorsque les justificatifs de l'identité de transaction délivrés par des prestataires de services privés s'appuyaient sur des justificatifs de l'identité fondamentale fournis par les pouvoirs publics.

K. Mécanismes de coopération institutionnelle

119. Le rôle des mécanismes de coopération institutionnelle pour ce qui était d'assurer la reconnaissance juridique mutuelle et l'interopérabilité des systèmes de gestion de l'identité et des services de confiance a été mentionné. Il a également été dit que ces mécanismes pourraient prendre différentes formes et revêtir une nature publique ou privée. L'avis a été exprimé que cette coopération institutionnelle, quelles qu'en soient les modalités, nécessiterait le cas échéant l'adoption de critères objectifs et d'un mécanisme de vérification de la conformité avec ces critères. Il a été ajouté que toute décision relative aux mécanismes de coopération institutionnelle devait tenir compte du point de vue du secteur privé.

120. S'agissant du paragraphe 39 du document A/CN.9/WG.IV/WP.154, il a été proposé de remplacer la référence au cadre technique commun par une référence à l'interopérabilité, afin de ne pas remettre en cause le principe de neutralité technologique. L'avis a été exprimé que l'harmonisation des règles juridiques et des cadres contractuel et législatif contribuait à la mise en place d'un cadre juridique commun.

L. Transparence

121. Il a été dit que par le terme de transparence, il fallait entendre la clarté et la divulgation des conditions de service, du code de conduite suivi par les prestataires de services (c'est-à-dire de leurs politiques opérationnelles) et des rapports d'évaluation. Il a été expliqué que cette divulgation pourrait être destinée aux abonnés, au public en général ou aux autorités de surveillance, selon qu'il convenait, sous réserve de la protection de toute information confidentielle.

122. Il a été dit que la transparence des conditions de service était importante pour permettre aux abonnés de faire un choix informé entre les offres concurrentes disponibles sur le marché. Il a été ajouté que cet aspect était également jugé important pour les concurrents, par exemple pour l'évaluation de leurs offres comparativement à celle des autres acteurs du marché, ainsi que pour les autres parties prenantes, par exemple pour la surveillance de la concurrence sur le marché.

123. Il a été indiqué qu'un autre aspect de la transparence concernait la notification des atteintes à la sécurité, qui pouvaient avoir une incidence non seulement sur les systèmes mais aussi sur les opérations. Il a été expliqué qu'un mécanisme approprié de notification de ces atteintes était jugé important pour l'amélioration de la performance et l'accroissement du niveau de confiance.

124. Il a été dit qu'un certain nombre de règlements, ayant trait notamment à la protection des données, seraient applicables dans le contexte de la transparence.

M. Conservation des données

125. L'avis a été réitéré que la protection de la vie privée et la conservation des données étaient des sujets importants, mais qui sortaient du cadre du mandat confié au Groupe de travail. Il a été indiqué que les résultats de ses travaux ne devaient pas viser à modifier la législation existante dans ces domaines ou dans d'autres.

126. L'importance des services d'archivage électroniques pour les entreprises a été mentionnée. Il a été expliqué que l'archivage électronique avait pour fonction précise d'assurer la sécurité juridique concernant la validité des documents électroniques archivés, en cas de litige et pour d'autres besoins. Il a été proposé que le mécanisme de reconnaissance juridique pour l'archivage électronique se limite à assurer la conformité avec les exigences juridiques du pays dans lequel les documents archivés devaient être utilisés.

N. Surveillance des prestataires de services

127. Il a été convenu que l'examen des aspects liés à la surveillance devait être mené conjointement avec celui de la certification (voir sect. I ci-dessus). Il a été déclaré que, s'ils avaient de nombreux aspects en commun, ces deux sujets présentaient néanmoins des différences qui devaient être prises en compte dans la terminologie et les dispositions dont ils feraient l'objet. Il a été jugé qu'une caractéristique distinctive de la surveillance était la nécessité de prendre des mesures correctives et coercitives en cas de non-respect des exigences impératives.

128. L'avis a été réitéré qu'il ne fallait pas sous-estimer le rôle des autorités de surveillance nationales comme seuls organismes capables d'assurer la stabilité et une surveillance appropriée. On a souligné la différence entre surveillance et contrôle, notamment l'autocontrôle et le contrôle par d'autres acteurs du marché et par les

abonnés aux services. Il a également été question du rôle croissant des autorités nationales non seulement dans la surveillance, mais aussi dans la mise au point et le déploiement de systèmes de gestion de l'identité et dans la prestation de services de gestion de l'identité et de services de confiance, ce qui nécessiterait de traiter séparément ces fonctions des pouvoirs publics. Concernant la question de savoir si un modèle particulier de surveillance, public ou privé (contractuel), serait nécessaire, il a été jugé prématuré de tirer une conclusion.

129. On a mentionné la difficulté à surveiller la technologie du registre distribué, étant donné, par exemple, qu'il pouvait ne pas y avoir de prestataire central à surveiller. Il a également été dit qu'en pareille situation, il serait difficile de prendre des mesures correctives et coercitives, notamment en modifiant un système de chaînes de blocs publiques à l'aide d'une « fourchette dure » ou par un autre moyen.

O. Décisions du Groupe de travail au titre du point 4 de l'ordre du jour

130. L'avis a été exprimé que les futurs documents établis par le Secrétariat devraient comporter des projets de dispositions supplémentaires sur les sujets fondamentaux de manière à faciliter l'avancée des travaux. Il a été ajouté que ces projets de dispositions devraient mentionner les diverses options envisageables, se baser sur les textes législatifs existants et les propositions soumises au Groupe de travail par les États et les organisations internationales, et être élaborés avec l'aide d'experts.

131. L'avis a également été exprimé que les futurs documents devraient s'attacher à recenser les questions essentielles permettant de saisir pleinement la portée du projet et présenter les données d'analyse et de recherche nécessaires pour effectuer des choix informés.

132. Il a été déclaré que les deux approches proposées étaient compatibles et toutes deux utiles. Il a été rappelé que la présentation des documents faisait l'objet de délais stricts, de sorte qu'il ne serait peut-être pas possible de mener de vastes consultations d'experts entre les sessions.

133. Le Groupe de travail a prié le Secrétariat d'établir les documents destinés à sa cinquante-huitième session sur la base des documents existants, en élaborant de nouvelles dispositions sur les sujets fondamentaux et en recensant et illustrant les questions clefs pour ses travaux, sans perdre de vue les délais applicables.

V. Assistance technique et coordination

134. Le Groupe de travail a entendu un rapport oral du Secrétariat sur les activités d'assistance technique et de coopération entreprises depuis le rapport oral que le Secrétariat lui avait présenté à ce sujet à sa session précédente. Il a été question, en particulier, des formalités conventionnelles en rapport avec la Convention des Nations Unies sur l'utilisation des communications électroniques dans les contrats internationaux (New York, 23 novembre 2005)[2] et des activités que le Secrétariat menait afin de promouvoir les textes de la CNUDCI sur le commerce électronique, notamment en coopération avec d'autres organismes, tels que la Commission économique et sociale pour l'Asie et le Pacifique (CESAP) et la Conférence des Nations Unies sur le commerce et le développement (CNUCED). Les travaux du Secrétariat visant à illustrer l'interaction entre les textes de la CNUDCI et les dispositions pertinentes des accords de libre-échange ont également été mentionnés.

135. Le Groupe de travail a également été informé des manifestations passées et à venir sur le commerce électronique organisées ou suivies par le Secrétariat en application du mandat consistant à compiler des informations sur les questions juridiques liées à l'économie numérique que lui avait confié la Commission[3]. Les

[2] Nations Unies, *Recueil des Traités*, vol. 2898, nº 50525.

[3] *Documents officiels de l'Assemblée générale, soixante-treizième session, Supplément nº 17* (A/73/17), par. 253 b).

États et les organisations ont été invités à participer ou à contribuer de toute autre façon à ces activités.

136. On a remercié le Secrétariat pour les informations qu'il avait fournies et les activités d'assistance technique et de coopération qu'il avait menées dans le domaine du droit du commerce électronique. Il a été dit qu'outre l'élaboration de textes juridiques, les activités visant à promouvoir l'adoption, la compréhension et l'application plus larges de ces textes ainsi que la coordination étaient essentielles à la réalisation du mandat de la CNUDCI.