

**Assemblée générale**

Distr. limitée
25 août 2020
Français
Original : anglais

**Commission des Nations Unies
pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Soixantième session
Vienne, 19-23 octobre 2020**

**Projet de dispositions relatives à l'utilisation et à
la reconnaissance internationale de la gestion de l'identité
et des services de confiance – synthèse des commentaires
présentés par les États et les organisations internationales**

Note du Secrétariat

Table des matières

	<i>Page</i>
I. Introduction.....	2
II. Principales questions soulevées.....	2
III. Synthèse des commentaires relatifs au chapitre I (Dispositions générales).....	9
IV. Synthèse des commentaires relatifs au chapitre II (Gestion de l'identité).....	17



I. Introduction

1. Avant le report de la soixantième session du Groupe de travail en raison de la pandémie de maladie à coronavirus (COVID-19), le Secrétariat a diffusé une note ([A/CN.9/WG.IV/WP.162](#)) contenant une version révisée du projet de dispositions relatives à l'utilisation et à la reconnaissance internationale de la gestion de l'identité et des services de confiance (le « projet de dispositions »).
2. Afin de faciliter la progression des travaux, le Secrétariat a prié les États, les organisations gouvernementales internationales et les organisations non gouvernementales internationales invitées aux sessions du Groupe de travail de présenter des commentaires sur le projet de dispositions, avant la tenue de la soixantième session du Groupe aux dates prévues pour son report. Il a élaboré un modèle de présentation des commentaires, qui comprenait un tableau contenant une liste non exhaustive de questions relatives aux différents projets de dispositions figurant dans le document [A/CN.9/WG.IV/WP.162](#), ainsi qu'un tableau pour la formulation de commentaires généraux sur le projet de dispositions.
3. À la date de la présente note, le Secrétariat a reçu des communications de la part de 24 États et de l'Union européenne, ainsi que de deux organisations internationales.
4. Le présent document (qui se compose des [A/CN.9/WG.IV/WP.164](#) et [A/CN.9/WG.IV/WP.164/Add.1](#)) ne reproduit pas les commentaires tels qu'ils ont été reçus. Il en fait la synthèse afin d'exposer les différents points de vue existants à l'égard du projet de dispositions, points de vue dont chacun est associé, par l'intermédiaire de notes de bas de page, aux États et aux organisations internationales qui le défendent. Chaque point de vue est présenté dans les termes du Secrétariat, qui ne reflètent pas nécessairement ceux employés dans leurs commentaires par les États et les organisations internationales concernés. Dans les notes de bas de page:
 - a) Le terme « UE » renvoie aux commentaires présentés conjointement par la Commission européenne et sept États membres de l'UE (Allemagne, Autriche, Belgique, France, Italie, Pologne et Tchéquie) ;
 - b) Le terme « UINL » renvoie à l'Union internationale du notariat ; et
 - c) Le terme « CIETAC » renvoie à la Commission chinoise d'arbitrage économique et commercial international.
5. En outre, la présente note ne fait pas la synthèse des commentaires présentés par la Banque mondiale au sujet du projet de dispositions ([A/CN.9/WG.IV/WP.163](#)), mais établit, au moyen des notes de bas de page, des liens entre ces commentaires et les différents points de vue exprimés.

II. Principales questions soulevées

6. Les commentaires présentés font ressortir un certain nombre de questions clefs, à savoir :
 - a) L'objet et la finalité du projet de dispositions ;
 - b) La nécessité de « cartographier » le paysage juridique existant applicable ;
 - c) Les concepts d'« identification électronique », de « contrôle d'identité » et de « service de confiance » ;
 - d) La prise en compte des systèmes de gestion de l'identité contractuels multipartites ;
 - e) L'interaction avec les systèmes de gestion de l'identité exploités par des gouvernements ; et
 - f) Le traitement à appliquer aux objets.

A. Objet et finalité du projet de dispositions

7. Comme le montrent les commentaires présentés, les avis divergent parmi les membres du Groupe de travail concernant ce à quoi doit servir le projet de dispositions. Selon un avis, il est destiné à assurer la reconnaissance juridique de l'utilisation de la gestion de l'identité et des services de confiance, tandis que, selon un autre avis, il vise à réglementer la fourniture des services de gestion de l'identité et des services de confiance. Cette divergence a été anticipée par la Banque mondiale qui, dans ses commentaires, indique que les projets de dispositions sur la gestion de l'identité traitent actuellement de l'utilisation et de la reconnaissance internationale des systèmes de gestion de l'identité, et invite le Groupe de travail à se demander s'ils devraient aborder les « opérations de gestion de l'identité » ainsi que le « fonctionnement d'un système de gestion de l'identité » et la « prestation de services de gestion de l'identité »¹.

8. Le Groupe de travail est convenu dès le départ que ses travaux sur la gestion de l'identité et les services de confiance devaient avoir pour objectifs « la reconnaissance juridique et la reconnaissance mutuelle »². Dans un premier temps, les débats ont porté sur les moyens d'atteindre ces objectifs dans un contexte international³. Toutefois, à sa cinquante-deuxième session, en 2019, la Commission a indiqué que le Groupe de travail devrait « s'attacher à élaborer un instrument qui pourrait s'appliquer à l'utilisation des systèmes de gestion de l'identité et des services de confiance à l'échelle tant interne qu'internationale »⁴. Elle a également indiqué que l'instrument devrait suivre les principes fondamentaux des travaux menés par la CNUDCI dans le domaine du commerce électronique, notamment la neutralité technologique, la non-discrimination à l'égard de l'utilisation de moyens électroniques, l'équivalence fonctionnelle et l'autonomie des parties⁵.

9. L'application du projet de dispositions peut se résumer comme suit :

a) Il confère une « reconnaissance juridique » à l'identification électronique et à la fourniture de services de confiance, en interdisant la discrimination à l'égard de l'utilisation de moyens électroniques pour vérifier l'identité d'une personne (identification électronique) ou les qualités particulières de données (fourniture d'un service de confiance) (art. 5 et 13) ;

b) Il donne un « effet juridique » à l'identification électronique et à la fourniture de services de confiance, en prévoyant qu'elles satisfont aux exigences juridiques à remplir pour i) l'identification en personne, ou ii) l'utilisation d'une procédure particulière pour l'exécution, l'envoi et la conservation de documents papier, si une méthode « fiable » est utilisée (art. 9 et 16 à 22) ;

c) Il prévoit – mais ne rend pas obligatoire – la désignation de systèmes de gestion de l'identité et de services de confiance qui soient « fiables » (détermination *ex ante* de la fiabilité) (art. 11 et 24) ;

d) Il impose certaines obligations indépendantes i) aux prestataires de services de gestion de l'identité ou de services de confiance concernant la fourniture des services et l'interaction avec les abonnés (art. 6, 7 et 14), et ii) aux abonnés en cas de violation des données (art. 8 et 15) ; et

e) Il confère une « reconnaissance internationale » aux systèmes de gestion de l'identité et aux services de confiance exploités et fournis, respectivement, en dehors de l'État (art. 26).

¹ A/CN.9/WG.IV/WP.163, p. 6.

² A/CN.9/902, par. 45.

³ A/CN.9/936, par. 61.

⁴ A/74/17, par. 172.

⁵ A/73/17, par. 159.

10. Comme le montre ce résumé, le projet de dispositions réglemente bien la fourniture des services de gestion de l'identité et des services de confiance, mais seulement dans une certaine mesure :

a) D'une part, il réglemente la fourniture de ces services de manière indirecte, en vertu de la condition de fiabilité prévue aux articles 9 et 16 à 22 (selon laquelle il est donné un effet juridique à l'identification électronique et aux services de confiance si une « méthode fiable » est utilisée). Plus précisément, en prévoyant que les règles régissant le système de gestion de l'identité ou le service de confiance concerné sont des facteurs pertinents pour déterminer la fiabilité, les articles 10 et 23 ont un effet indirect sur la conception des systèmes de gestion de l'identité et des services de confiance qu'un prestataire de services souhaitera utiliser afin de produire les effets juridiques prévus aux articles 9 et 16 à 22. La mesure dans laquelle le projet de dispositions octroie aux parties le droit de convenir de la fiabilité de la méthode reste une question ouverte (voir par. 23 et 24 ci-dessous).

b) D'autre part, il réglemente la fourniture de ces services de manière directe, en imposant certaines obligations aux prestataires de services et aux abonnés (comme indiqué au paragraphe 9 d) ci-dessus).

11. Toutefois, le projet de dispositions n'établit pas de régime complet pour ce qui est de réglementer la gestion de l'identité ou les services de confiance (tel que le régime relatif à la gestion de l'identité mis en place par la Suisse en application de la loi fédérale sur les services d'identification électronique, d'adoption récente, et le régime relatif aux services de confiance instauré dans l'UE conformément au règlement eIDAS)⁶. On pourrait dire, tout au plus, que le projet de dispositions vise à réglementer la fourniture des services de gestion de l'identité et des services de confiance dans la mesure nécessaire pour leur conférer une reconnaissance et des effets de droit.

B. Nécessité de « cartographier » le paysage juridique existant applicable

12. L'option A de l'article 9-1 suit une approche axée sur l'équivalence fonctionnelle pour donner un effet juridique à l'utilisation de la gestion de l'identité⁷. Elle consiste à identifier une personne, plutôt qu'à émettre des justificatifs aux fins de l'identification⁸. Toutefois, des questions ont été soulevées dans certains commentaires au sujet du rôle joué par l'équivalence fonctionnelle dans le projet de dispositions (voir la synthèse des commentaires sur la question 3 relative à l'article 9)⁹.

13. Les dispositions qui donnent des effets de droit à la gestion de l'identité et aux services de confiance selon une approche axée sur l'équivalence fonctionnelle supposent l'existence de lois applicables aux opérations menées à l'aide de documents papier ou en personne. Dans le contexte de la gestion de l'identité, il existe des lois qui exigent ou permettent l'identification d'une personne. Dans le contexte des services de confiance, il existe des lois qui exigent ou impliquent une procédure

⁶ 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 et abrogeant la directive 1999/93/CE.

⁷ Comme indiqué dans la note 32 du projet de dispositions, l'option B de l'article 9-1 ne suit pas une approche axée sur l'équivalence fonctionnelle.

⁸ Le Groupe de travail s'est demandé si la reconnaissance juridique devrait avoir pour objet les justificatifs d'identité électroniques qui sont fonctionnellement équivalents aux justificatifs d'identité sur support papier utilisés à des fins d'identification (par exemple, les passeports électroniques). Il a également envisagé de donner un effet juridique aux justificatifs d'identité électroniques qui n'ont pas d'équivalent papier. Voir, de manière générale, A/CN.9/965, par. 62 à 85.

⁹ Le Groupe de travail a également examiné le rôle de l'équivalence fonctionnelle lors de ses précédentes sessions ; voir *ibid.*

particulière pour l'exécution, l'envoi et la conservation des documents (voir, par exemple, articles 16 à 20). Le projet de dispositions suppose également l'existence de lois qui exigent l'identification d'une personne conformément à une procédure définie ou prescrite par la loi (par exemple, à l'aide de documents d'identité particuliers ou en présence physique de la personne à identifier) (art. 2-3).

14. Les questions connexes concernant la manière dont le projet de dispositions « se raccorde » aux systèmes de gestion de l'identité contractuels, ainsi qu'à ceux exploités par des gouvernements et établis par la législation, font l'objet d'un traitement distinct ci-dessous (voir par. 22 à 28).

C. Concepts d'« identification électronique », de « contrôle d'identité » et de « service de confiance »

15. Les définitions de chacun de ces termes figurant à l'article premier du projet de dispositions visent à tenir compte des décisions prises par le Groupe de travail, y compris celle de demander au Secrétariat de « veiller à ce que les notions d'authentification, d'identification et de vérification soient utilisées dans l'instrument de manière cohérente, et conformément à la terminologie adoptée par l'Union internationale des télécommunications (UIT) »¹⁰. Néanmoins, les membres du Groupe de travail ont fait part dans leurs commentaires d'une certaine inquiétude concernant ces termes, en estimant qu'ils risquaient d'être mal interprétés et que leurs définitions étaient peut-être mal formulées.

1. Identification électronique

16. Le concept d'« identification électronique » pose deux problèmes. Le premier est que le terme « identification électronique » pourrait être interprété à tort comme renvoyant à l'ensemble du processus de gestion de l'identité, plutôt qu'au processus distinct consistant à vérifier ou confirmer le lien existant entre une personne et une identité au vu des justificatifs d'identité présentés, conformément à la définition énoncée à l'article 1 d). Le second est que la définition de ce terme figurant à l'article 1 d) correspond au concept d'« authentification » tel qu'il s'entend dans certains systèmes de gestion de l'identité et certains systèmes juridiques. Par exemple, le règlement eIDAS de l'UE définit l'« authentification » dans le contexte de la gestion de l'identité comme « un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale »¹¹.

17. Si le terme « authentification » remplaçait « identification électronique », il serait utilisé à la fois pour la gestion de l'identité et les services de confiance, ce qui amène à considérer l'argument exprimé à la dernière session du Groupe de travail selon lequel « il [faut] veiller à ce que ce terme soit utilisé de manière cohérente dans l'ensemble du texte »¹². Il semblerait, au moins d'après la synthèse ci-dessous (voir l'alinéa c) de la question 1 relative à l'article premier), que l'utilisation du terme « authentification » dans les deux contextes ne pose pas de problème, compte tenu, en particulier, du fait que cette approche est adoptée dans le règlement eIDAS. De fait, il a été avancé que l'identification électronique était essentiellement un service

¹⁰ A/CN.9/1005, par. 86.

¹¹ 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 et abrogeant la directive 1999/93/CE. Il convient de noter que, contrairement à la version actuelle du projet de dispositions, le règlement eIDAS emploie le terme « identification électronique » pour désigner non pas le processus de confirmation, mais l'utilisation de « données d'identification personnelle » (c'est-à-dire d'une « identité », selon la terminologie du projet de dispositions) contenues dans un « moyen d'identification électronique » (c'est-à-dire dans un « justificatif d'identité », selon la terminologie du projet de dispositions) aux fins de cette confirmation.

¹² A/CN.9/1005, par. 85.

de confiance (dans la mesure où elle sert à vérifier ou confirmer le lien existant entre des données formant une « identité » et une personne particulière).

2. Contrôle d'identité

18. Le concept de « contrôle d'identité » pose problème, car il pourrait être interprété à tort comme renvoyant à la vérification ou la confirmation du lien existant entre la personne à identifier et une identité (c'est-à-dire à l'« identification électronique »), et non au processus qui intervient à l'étape d'inscription du processus de gestion de l'identité, située en amont, lors duquel le prestataire de services de gestion de l'identité (ou un autre participant au système de gestion de l'identité) collecte des attributs relatifs à l'abonné (par exemple, des données personnelles) et les vérifie en les comparant à des sources de confiance, comme les registres et statistiques de l'état civil, avant de délivrer à l'abonné des justificatifs d'identité aux fins de l'identification. Le terme « contrôle d'identité » est employé par l'UIT¹³.

19. Afin de lever le risque d'interprétation erronée, le Groupe de travail voudra peut-être se demander s'il faudrait réserver un traitement spécial au contrôle d'identité dans le projet de dispositions et, le cas échéant, s'il conviendrait d'utiliser un terme différent (par exemple, « inscription »)¹⁴.

3. Services de confiance

20. Le concept de « service de confiance » soulève la question de savoir si le projet de dispositions, au lieu de donner une reconnaissance et un effet juridiques aux « services de confiance » (art. 13 et 16 à 22), devrait plutôt traiter du produit de ces services. Pour l'essentiel, le produit d'un service de confiance est le message de données fourni par le prestataire de services de confiance qui sert à vérifier ou confirmer que d'autres données possèdent une qualité particulière, par exemple le fait que ces autres données i) identifient une personne particulière, ii) indiquent un moment précis, ou iii) font état d'une altération particulière.

21. Le Groupe de travail voudra peut-être se demander s'il conviendrait de reformuler la définition du terme « service de confiance » figurant à l'article 1 m), ainsi que le libellé de l'article 13, qui confère une reconnaissance juridique aux services de confiance, pour se concentrer sur le produit de ces services (c'est-à-dire sur le message de données généré lors de leur fourniture).

D. Prise en compte des systèmes de gestion de l'identité contractuels multipartites

22. Les commentaires présentés font apparaître une incertitude concernant la manière dont le projet de dispositions traite des systèmes de gestion de l'identité contractuels multipartites, comme les cadres de confiance. Ces systèmes font intervenir différents participants, notamment des agents d'inscription, des fournisseurs d'attributs et des fournisseurs d'authentification, qui remplissent des fonctions diverses au sein d'un réseau de contrats. La prise en compte des systèmes de gestion de l'identité contractuels multipartites soulève deux questions distinctes, mais liées entre elles. La première a trait au fondement contractuel de ces systèmes et au principe de l'autonomie des parties. La seconde concerne la participation de multiples parties à ces systèmes et la détermination du prestataire de services de gestion de l'identité approprié aux fins du projet de dispositions.

¹³ Voir Recommandation UIT-T X.1252.

¹⁴ Par exemple, i) les définitions renvoyant au « contrôle d'identité » pourraient plutôt renvoyer à l'« inscription », ii) à l'article 5 a), on pourrait éviter de faire référence au « contrôle d'identité » (qui n'est pas effectué par voie électronique), et iii) l'article 6 a) iii) pourrait expliquer en termes généraux ce qu'implique le « contrôle d'identité », plutôt que de faire référence à ce terme.

1. Autonomie des parties

23. Le projet de dispositions établit un ensemble de droits et d'obligations qui pourraient ne pas correspondre à ceux que prévoient les règles régissant un système de gestion de l'identité pour les différents participants à ce système, règles qui encadrent également les contrats conclus entre les participants. Il établit également un régime de responsabilité qui pourrait ne pas correspondre à celui que prévoient les règles régissant le système de gestion de l'identité (au moyen de clauses d'indemnisation, de non-responsabilité et de limitation de responsabilité). Le cas échéant, le projet de dispositions semble a priori prévaloir. Contrairement à la LTSE, il ne confère pas aux parties (par exemple, aux participants à un système de gestion de l'identité) le droit de modifier l'effet de ses dispositions par convention¹⁵, ce qui correspond à une approche réglementaire de la gestion de l'identité.

24. Le Groupe de travail voudra peut-être préciser si le projet de dispositions devrait obligatoirement s'appliquer, ou s'il devrait donner aux parties le droit de déroger par convention à ses dispositions au profit des règles du système de gestion de l'identité concerné, conformément au principe de l'autonomie des parties.

2. Détermination du prestataire de service de gestion de l'identité approprié

25. Le projet de dispositions renvoie au « prestataire de services de gestion de l'identité », au singulier. Si, dans certaines dispositions, ce terme pourrait s'interpréter comme ayant un sens collectif, d'autres dispositions, notamment l'article 6, envisagent un prestataire de services de gestion de l'identité unique remplissant diverses fonctions, y compris le contrôle d'identité, la gestion des justificatifs d'identité et l'identification électronique.

26. Le Groupe de travail voudra peut-être se demander s'il conviendrait de modifier le projet de dispositions pour tenir compte du fait que de multiples parties peuvent être chargées de remplir des fonctions au sein d'un système de gestion de l'identité. Une solution proposée dans les commentaires présentés¹⁶ consiste à désigner le prestataire de services de gestion de l'identité comme étant la personne qui procède à l'identification électronique (c'est-à-dire qui vérifie ou confirme le lien existant entre la personne à identifier et une identité) et à modifier l'article 6 afin d'obliger cette personne à « s'assurer » que les fonctions énumérées à cet article sont remplies (et ainsi de permettre que ces fonctions soient remplies par une personne autre que le prestataire de services de gestion de l'identité). Si le Groupe de travail souhaitait envisager cette solution, il pourrait également se demander comment, dans le cadre de l'option C de l'article 12, le prestataire de services de gestion de l'identité serait tenu responsable d'un manquement d'un autre participant à s'acquitter de ses fonctions, et s'il pourrait décharger sa responsabilité sur cet autre participant en vertu des règles régissant le système de gestion de l'identité.

E. Interaction avec les systèmes de gestion de l'identité exploités par des gouvernements

27. Les États du monde entier ont mis en place des systèmes de gestion de l'identité afin d'aider les particuliers (et les entreprises) à interagir avec les services publics (ainsi qu'avec le secteur privé). Ces systèmes exploités par des gouvernements sont parfois – mais pas toujours – établis par la législation¹⁷. Certains des commentaires

¹⁵ À comparer à l'article 5 de la LTSE, en vertu duquel « il est possible de déroger aux dispositions de [cette] Loi ou d'en modifier les effets par convention, à moins que cette convention soit invalide ou sans effets en vertu de la loi applicable ».

¹⁶ Voir l'alinéa b) de la question 1 relative à l'article 6.

¹⁷ Voir, par exemple, la loi indienne de 2016 intitulée *Aadhaar Act*, qui porte sur la fourniture ciblée de subventions, d'avantages et de services financiers et autres, la loi néo-zélandaise de 2012 intitulée *Electronic Identity Verification Act* (loi sur la vérification électronique de l'identité), la loi nigérienne de 2007 intitulée *National Identity Management Commission Act* (loi relative à la

présentés indiquent qu'il serait intéressant de se demander comment le projet de dispositions interagit avec les systèmes de gestion de l'identité exploités par des gouvernements, et le Groupe de travail voudra peut-être examiner cette question plus avant.

28. À cet égard, l'application du projet de dispositions peut se résumer comme suit :

a) Le projet de dispositions s'applique à l'utilisation des systèmes de gestion de l'identité et des services de confiance dans le cadre d'activités commerciales et de services touchant au commerce (art. 2-1), y compris lorsque des organismes publics sont concernés (soit en tant que parties commerciales, soit en tant que prestataires de services de gestion de l'identité) ;

b) Par ailleurs, le projet de dispositions n'oblige pas les organismes publics à utiliser un service de gestion de l'identité ou un service de confiance (art. 3-1), et les législations portant création de systèmes de gestion de l'identité exploités par des gouvernements auraient préséance en cas d'incohérence avec le projet de dispositions (art. 2-4) ;

c) Le projet de dispositions ne traite pas des questions de l'interopérabilité des systèmes de gestion de l'identité ou de la portabilité des justificatifs, notamment pour ce qui est des systèmes de gestion de l'identité exploités par des gouvernements. Plus précisément, il ne confère pas le droit aux participants à un autre système de gestion de l'identité d'utiliser des justificatifs d'identité délivrés par un système de gestion de l'identité exploité par un gouvernement (qui peuvent faire l'objet de restrictions en vertu du droit existant, y compris de lois relatives au respect de la vie privée et à la protection des données)¹⁸, ou d'accéder au système de gestion de l'identité exploité par un gouvernement pour procéder à une identification électronique au moyen de ces justificatifs ;

d) En outre, le projet de dispositions ne réserve pas de traitement juridique spécial aux « attributs » ou aux « identités » provenant d'une base de données exploitée par un gouvernement, par exemple des registres et statistiques de l'état civil (voir, ci-après, la synthèse des commentaires sur la question 6 relative à l'article premier), ou à l'identification électronique au moyen de justificatifs d'identité délivrés par un système de gestion de l'identité exploité par un gouvernement (sauf dans le cas où ce système de gestion de l'identité est désigné conformément à l'article 11).

Commission nationale de gestion de l'identité), et la loi philippine intitulée *Identification System Act* (loi sur les systèmes d'identification).

¹⁸ Voir, par exemple, les restrictions relatives à l'utilisation d'« identifiants publics » prévues aux clauses 9.1 et 9.2 de l'annexe 1 de la loi australienne de 1988 intitulée *Privacy Act* (loi sur la confidentialité).

III. Synthèse des commentaires relatifs au chapitre I (Dispositions générales)

A. Article premier – Définitions

1. Synthèse des commentaires répondant à des questions précises

<i>Question</i>	<i>Synthèse des commentaires</i>
<p>1. Selon la terminologie utilisée dans le document A/CN.9/WG.IV/WP.162, le processus de gestion de l'identité comprend deux étapes (ou phases), à savoir le « contrôle d'identité » et l'« identification électronique » (voir A/CN.9/WG.IV/WP.162, par. 2). Ces termes sont-ils adaptés pour décrire les étapes du processus de gestion de l'identité ? Les définitions de ces termes sont-elles précises ?</p>	<p>a) Les termes sont acceptables¹⁹.</p> <p>b) Il conviendrait d'utiliser le terme « authentification » à la place d'« identification électronique »²⁰, terme qui pourrait être interprété à tort comme désignant l'ensemble du processus de gestion de l'identité²¹.</p> <p>c) Il est approprié d'utiliser le terme « authentification » dans le contexte à la fois de la gestion de l'identité et des services de confiance²².</p> <p>d) Il conviendrait d'utiliser le terme « inscription » à la place d'« identification électronique »²³.</p> <p>e) L'établissement d'un lien entre le sujet et une identité (tel que décrit dans la définition de l'« identification électronique ») a lieu à l'étape du contrôle d'identité et non à celle de l'identification électronique²⁴.</p> <p>f) Le concept d'« identification électronique » devrait s'entendre comme renvoyant à la <i>confirmation</i> de l'identité²⁵.</p> <p>g) Le fait que le projet de dispositions parte du principe que le processus de gestion de l'identité ne comprend que deux phases – le contrôle d'identité et l'identification électronique (voir, par exemple, les définitions des termes « services de gestion de l'identité ») et « système de gestion de l'identité ») – constitue une erreur²⁶.</p> <p>h) Le projet de dispositions devrait expressément mentionner <i>l'authentification et l'échange d'informations relatives à l'identité ou la vérification et la validation</i> comme étape supplémentaire du processus de gestion de l'identité²⁷.</p>

¹⁹ Liban, Sénégal (concernant l'« identification électronique »), Singapour, Suisse, Ukraine, CIETAC, UINL.

²⁰ États-Unis, Royaume-Uni, UE.

²¹ États-Unis, Royaume-Uni.

²² États-Unis, UE.

²³ Danemark.

²⁴ Danemark, Royaume-Uni.

²⁵ Royaume-Uni.

²⁶ Danemark.

²⁷ Danemark, Suisse.

- | | |
|---|---|
| <p>2. La nouvelle définition du terme « authentification » dans le contexte des services de confiance (art. 21 et 22) est-elle acceptable (voir A/CN.9/WG.IV/WP.162, note de bas de page 3) ?</p> <p>3. Faut-il inclure une définition des « facteurs d'identification électronique » (tels qu'ils apparaissent à l'article 6) ? Le cas échéant, la définition figurant à la note de bas de page 6 du document A/CN.9/WG.IV/WP.162 est-elle acceptable ?</p> <p>4. Faut-il inclure une définition des « mécanismes d'identification électronique » (tels qu'ils apparaissent à l'article 6) ? Le cas échéant, la définition figurant à la note de bas de page 7 du document A/CN.9/WG.IV/WP.162 est-elle acceptable ?</p> | <p>a) La définition est acceptable²⁸.</p> <p>b) La définition n'est pas acceptable²⁹.</p> <p>c) Dans le chapitre sur les services de confiance, le terme « authentification » devrait être défini comme ayant trait à la <i>confirmation</i> (de l'identité, de l'intégrité, etc.)³⁰.</p> <p>a) Une définition de ce terme est nécessaire³¹. La définition figurant à la note de bas de page 6 est acceptable³².</p> <p>b) L'utilisation de ce terme souligne que la gouvernance de ces facteurs est distincte de celle des justificatifs d'identité³³.</p> <p>c) Une définition de ce terme n'est pas nécessaire³⁴.</p> <p>d) Le terme « facteurs d'identification électronique » ne devrait pas être utilisé³⁵. L'article 6 d) i) devrait être supprimé³⁶. Le terme « moyen d'identification électronique », tel qu'employé dans le règlement eIDAS, devrait remplacer « justificatifs d'identité »³⁷.</p> <p>a) Une définition de ce terme est nécessaire³⁸. La définition figurant à la note de bas de page 7 est acceptable³⁹.</p> <p>b) Il est nécessaire de définir ce terme, mais de sorte qu'il désigne les mécanismes au moyen desquels un sujet utilise des justificatifs d'identité pour « confirmer l'identité d'un tiers »⁴⁰.</p> <p>c) Le concept doit être examiné plus avant. La définition pose problème, car elle fait référence au comportement du sujet et non à celui du prestataire de services de gestion de l'identité⁴¹.</p> <p>d) Une définition de ce terme n'est pas nécessaire⁴².</p> <p>e) Le terme « facteurs d'identification électronique » ne devrait pas être utilisé. Il conviendrait de préciser le rapport entre ce concept et les « justificatifs d'identité »⁴³.</p> |
|---|---|

²⁸ Singapour, Suisse, UINL.

²⁹ Danemark, UE.

³⁰ République dominicaine, Royaume-Uni, UE, Ukraine, CIETAC.

³¹ Liban, Singapour, UE, CIETAC, UINL.

³² Liban, Singapour, UE, CIETAC, UINL.

³³ Singapour.

³⁴ États-Unis, Suisse, Ukraine.

³⁵ Danemark, Royaume-Uni.

³⁶ Royaume-Uni.

³⁷ Danemark.

³⁸ Liban, République dominicaine, UE, CIETAC.

³⁹ Liban, UE, CIETAC.

⁴⁰ Chine.

⁴¹ États-Unis.

⁴² Royaume-Uni, Suisse, Ukraine, UINL.

⁴³ Danemark.

Question

Synthèse des commentaires

5. La définition du terme « services de gestion de l'identité » devrait-elle faire état de « services consistant à gérer le contrôle d'identité ou l'identification électronique de [sujets][personnes] intégralement ou en partie sous forme électronique », de façon à inclure dans cette définition toute étape (par exemple, le contrôle d'identité) susceptible d'être effectuée hors ligne ?

Note du Secrétariat : Une précision analogue pourrait être apportée à la définition du terme « système de gestion de l'identité ».

6. Est-il nécessaire d'ajouter une précision (soit dans une définition, par exemple celle du terme « identité » ou celle du terme « contrôle d'identité », soit dans un document explicatif) pour indiquer que les registres et statistiques de l'état civil peuvent constituer une source fiable en ce qui concerne les attributs de personnes physiques et, de même, qu'un registre spécialisé peut constituer une source fiable en ce qui concerne les attributs de personnes morales ?

7. Faut-il inclure une définition du terme « niveau de garantie », tel qu'il apparaît aux articles 10-1 b), 11-3 et 27 c) ?

- a) Cette précision n'est pas nécessaire⁴⁴. Elle est implicite dans la définition⁴⁵.
- b) La définition des « services de gestion de l'identité » devrait préciser que ces services peuvent être fournis « intégralement ou en partie » sous forme électronique⁴⁶.
- c) La définition est trop imprécise et devrait comporter une liste indicative de services⁴⁷.

- a) Il n'est pas nécessaire de mentionner les registres et statistiques de l'état civil comme étant une source fiable pour les attributs⁴⁸.
- b) Le projet de dispositions ne devrait pas reconnaître les registres et statistiques de l'état civil comme étant une source fiable pour les attributs⁴⁹.
- c) Il pourrait être utile de mentionner les registres et statistiques de l'état civil comme étant une source fiable pour les attributs⁵⁰.
- d) Le projet de dispositions pourrait reconnaître les registres et statistiques de l'état civil comme étant une source fiable pour les attributs, à condition que définir le concept de « source fiable »⁵¹.
- e) Des exemples de sources fiables pour les attributs, notamment les registres et statistiques de l'état civil, pourraient être donnés dans un document explicatif⁵².

- a) Une définition de ce terme n'est pas nécessaire⁵³.
- b) Une définition de ce terme serait utile⁵⁴.
- c) Une définition de ce terme est nécessaire⁵⁵.

⁴⁴ Ukraine, UINL.

⁴⁵ UINL.

⁴⁶ Danemark, États-Unis, Liban, Royaume-Uni, Singapour, Suisse, UE, CIETAC.

⁴⁷ Argentine.

⁴⁸ CIETAC, UINL.

⁴⁹ États-Unis, Suisse, UE, Ukraine.

⁵⁰ Danemark, États-Unis.

⁵¹ Danemark.

⁵² Royaume-Uni.

⁵³ États-Unis, CIETAC, UINL.

⁵⁴ Liban, Royaume-Uni, Suisse, Ukraine.

⁵⁵ Argentine, Danemark.

2. Synthèse des autres commentaires relatifs à l'article premier

<i>Question</i>	<i>Synthèse des commentaires</i>
1. « Justificatifs d'identité »	a) La définition de ce terme devrait être modifiée pour faire référence à la vérification ou à l'authentification de l'identité (plutôt qu'à l'identification électronique) ⁵⁶ . b) Il faudrait plutôt utiliser le terme « authentificateur », et la définition devrait faire référence aux caractéristiques comportementales, afin de couvrir la biométrie ⁵⁷ .
2. « Contrôle d'identité »	<i>Voir l'alinéa d) de la question 1 relative à l'article premier</i>
3. « Abonné »	a) Tel qu'il est défini, le terme « abonné » pourrait s'interpréter comme désignant la partie qui se fie à un service plutôt que le sujet (c'est-à-dire la personne à identifier) ⁵⁸ . b) La définition du terme « abonné » pourrait s'interpréter comme incluant non seulement le sujet, mais aussi les fournisseurs d'attributs et d'autres personnes qui concluent un accord contractuel avec un prestataire de services de gestion de l'identité ⁵⁹ .
4. « Sujet »	<i>Voir l'alinéa a) de la question 1 relative à l'article 22.</i>
5. « Services de confiance »	a) La définition est imprécise et devrait comporter une liste indicative de services ⁶⁰ .
6. Termes non définis	a) Il conviendrait de définir le terme « identifiant » (utilisé dans la définition de l'« authentification ») ⁶¹ . b) Il conviendrait de définir le terme « gestion de l'identité » ⁶² . c) Il conviendrait de définir l'expression « règles qui régissent les systèmes de gestion de l'identité » (utilisées aux articles 6 c), 6 f) et 10-1 b)) ⁶³ . Voir également l'expression « règle [...] applicable au service de confiance » (utilisée à l'article 23-1 a)). d) Il conviendrait de définir le terme « vérification » (utilisé à l'article 6 a)) ⁶⁴ .

⁵⁶ Chine.

⁵⁷ Royaume-Uni.

⁵⁸ Danemark, Royaume-Uni.

⁵⁹ États-Unis. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 6 et 10).

⁶⁰ Danemark, Royaume-Uni.

⁶¹ République dominicaine. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 4).

⁶² États-Unis, République dominicaine. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 4).

⁶³ Argentine, République dominicaine. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 4 et 5).

⁶⁴ Argentine, République dominicaine. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 5).

<i>Question</i>	<i>Synthèse des commentaires</i>
7. Généralités concernant la terminologie	<p>a) Le projet de dispositions devrait faire référence aux concepts suivants : « commerce électronique », « document numérique », « échange de données électroniques » et « signature électronique »⁶⁵.</p> <p>b) Il conviendrait de modifier la définition des termes « services de gestion de l'identité » et « système de gestion de l'identité », de manière à éviter d'indiquer que l'« identification électronique » s'effectue « sous forme électronique », ce qui est redondant⁶⁶.</p> <p>c) La terminologie du projet de dispositions devrait suivre de plus près celle employée au niveau international en matière de respect de la vie privée et de protection des données⁶⁷.</p> <p>d) Une partie de la terminologie est obsolète et devrait être modifiée, afin de correspondre à l'usage actuel et de permettre la prise en compte d'évolutions ultérieures dans les domaines de la gestion de l'identité et des services de confiance⁶⁸.</p>

B. Article 2 – Champ d'application

1. Synthèse des commentaires répondant à des questions précises

Le modèle ne comportait pas de question précise concernant l'article 2.

2. Synthèse des autres commentaires relatifs à l'article 2

<i>Question</i>	<i>Synthèse des commentaires</i>
1. Éléments à inclure dans le champ d'application	<p>a) Le champ d'application actuel est suffisant⁶⁹.</p> <p>b) Le Groupe de travail devrait se demander si le projet de dispositions s'applique aux organismes publics qui se livrent à des activités commerciales⁷⁰.</p> <p>c) Le Groupe de travail devrait traiter séparément la gestion de l'identité et les services de confiance⁷¹. Au stade actuel, la tâche la plus importante à accomplir consiste à recenser et définir les questions pertinentes concernant i) les opérations liées à l'identité et les systèmes de gestion de l'identité, et ii) les lois existantes qui imposent aux acteurs privés des exigences en matière d'identification⁷².</p>

⁶⁵ République dominicaine.

⁶⁶ El Salvador.

⁶⁷ Argentine.

⁶⁸ Canada.

⁶⁹ Royaume-Uni. À comparer aux commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 6 et 7).

⁷⁰ Argentine.

⁷¹ Canada, États-Unis.

⁷² États-Unis.

*Question**Synthèse des commentaires*

2. Éléments à exclure du champ d'application

- a) Le projet de dispositions devrait comporter une disposition indiquant qu'il ne concerne ni la surveillance ou la localisation des personnes, ni le traitement des données personnelles à toutes autres fins⁷³.
- b) Le projet de dispositions ne devrait pas exiger l'utilisation d'un système de gestion de l'identité particulier⁷⁴.
- c) Le projet de dispositions devrait s'appliquer uniquement aux systèmes de gestion de l'identité multipartites. Les systèmes de gestion de l'identité bipartites devraient être exclus de son champ d'application⁷⁵.

3. Interaction avec les systèmes de gestion de l'identité exploités par des gouvernements

- a) La manière dont le projet de dispositions interagit avec les systèmes de gestion de l'identité exploités par des gouvernements est peu claire (s'agissant de savoir, par exemple, si une partie commerciale peut utiliser ces systèmes afin d'identifier une autre partie)⁷⁶.
- b) Le Groupe de travail pourrait envisager d'élaborer des dispositions supplémentaires concernant l'interaction, notamment sur les conditions d'accès aux systèmes de gestion de l'identité exploités par des gouvernements et d'autres conditions⁷⁷.

⁷³ Niger.

⁷⁴ États-Unis, Royaume-Uni. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 7).

⁷⁵ États-Unis.

⁷⁶ États-Unis. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 2, 3 et 6).

⁷⁷ Fédération de Russie. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 2 et 3).

C. Article 3 – Caractère volontaire de l'utilisation de services de gestion de l'identité et de services de confiance

1. Synthèse des commentaires répondant à des questions précises

<i>Question</i>	<i>Synthèse des commentaires</i>
1. Des questions ont été posées au sujet des liens entre les articles 2 et 3. Ces liens seraient-ils plus clairs si l'article 3 était reformulé comme suit : « Aucune disposition du présent [instrument] n'exige d'une [personne] [partie se fiant à un service] qu'elle accepte l'identification électronique d'un sujet ou qu'elle se fie à un service de confiance sans y avoir consenti. » ?	<p>a) Il n'est pas nécessaire de reformuler l'article 3 de cette façon⁷⁸.</p> <p>b) Il convient de reformuler l'article 3 de cette façon⁷⁹.</p> <p>c) L'article 3 devrait également comporter une disposition relative aux abonnés indiquant que l'instrument n'exige pas de ces derniers qu'ils présentent leur identité aux fins de l'identification électronique sans leur consentement⁸⁰.</p> <p>d) Il importe que le projet d'article confirme le caractère volontaire de l'utilisation pour toutes les parties⁸¹.</p> <p>e) Il existe un chevauchement partiel entre les articles 2-2 et 2-3, d'une part, et l'article 3-1, d'autre part⁸².</p> <p>f) Les articles 2 et 3 pourraient être fusionnés⁸³.</p>

2. Synthèse des autres commentaires relatifs à l'article 3

<i>Question</i>	<i>Synthèse des commentaires</i>
1. Consentement à l'utilisation d'un service de gestion de l'identité ou d'un service de confiance	<p>a) L'article 3 devrait préciser que le consentement doit être éclairé, donné librement, exprès et non ambigu, et qu'il peut être retiré⁸⁴.</p> <p>b) Il ne suffit pas que le consentement soit déduit du comportement de la personne (comme indiqué à l'article 3-2)⁸⁵.</p> <p>c) L'article 3 devrait préciser l'objet du consentement⁸⁶.</p>

⁷⁸ Suisse, UE, CIETAC.

⁷⁹ Liban, Royaume-Uni, Ukraine, UINL.

⁸⁰ Royaume-Uni.

⁸¹ Fédération de Russie, UE.

⁸² Fédération de Russie.

⁸³ Sénégal.

⁸⁴ Sénégal.

⁸⁵ République dominicaine, Sénégal. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 7).

⁸⁶ Royaume-Uni.

<i>Question</i>	<i>Synthèse des commentaires</i>
2. Autonomie des parties	<p>a) Le projet de dispositions devrait préciser comment l'instrument interagit avec les droits et obligations des parties qui découlent de contrats, notamment des contrats servant de base à des systèmes de gestion de l'identité multipartites (par exemple, des cadres de confiance)⁸⁷. Plus particulièrement, le Groupe de travail devrait envisager de déterminer les dispositions qui sont impératives et celles dont les parties peuvent modifier l'effet par convention⁸⁸.</p> <p>b) Le projet de dispositions devrait indiquer que les questions non régies par l'instrument sont réglées, le cas échéant, par le contrat conclu entre les parties, faute de quoi le droit du domicile de l'abonné devrait s'appliquer⁸⁹.</p> <p>c) Les règles impératives sont souvent redondantes et pourraient accroître les coûts des services de gestion de l'identité, ce qui serait particulièrement préjudiciable pour les petites et moyennes entreprises. En outre, il est difficile d'établir des consensus concernant des règles impératives, et l'examen de ce type de règles pourrait compromettre le principe de neutralité technologique⁹⁰.</p>

D. Article 4 – Interprétation

1. Synthèse des commentaires répondant à des questions précises

Le modèle ne comportait pas de question précise concernant l'article 4.

2. Synthèse des autres commentaires relatifs à l'article 4

<i>Question</i>	<i>Synthèse des commentaires</i>
1. Terminologie	<p>a) Le concept de « caractère international » de l'instrument n'est pas clair et pourrait être inapproprié pour une loi type⁹¹.</p> <p>b) Il est difficile de savoir en quoi consisterait l'« uniformité » d'application dans le cas d'une loi type⁹².</p> <p>c) Il n'est pas évident de savoir, dans le contexte d'une loi type, à qui s'applique le concept de « bonne foi »⁹³.</p> <p>d) Si l'instrument prenait la forme d'une loi type, il ne serait peut-être pas nécessaire qu'il renvoie aux règles de droit international privé aux fins de son interprétation⁹⁴.</p>

⁸⁷ États-Unis, Royaume-Uni. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 3 et 8).

⁸⁸ Canada. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 3 et 8).

⁸⁹ Argentine.

⁹⁰ Fédération de Russie.

⁹¹ États-Unis.

⁹² États-Unis.

⁹³ États-Unis.

⁹⁴ États-Unis.

IV. Synthèse des commentaires relatifs au chapitre II (Gestion de l'identité)

A. Article 5 – Reconnaissance juridique de la gestion de l'identité

1. Synthèse des commentaires répondant à des questions précises

Le modèle ne comportait pas de question précise concernant l'article 5.

2. Synthèse des autres commentaires relatifs à l'article 5

<i>Question</i>	<i>Synthèse des commentaires</i>
1. Application de l'article 5	a) Le champ d'application et l'objet de cette disposition ne sont pas clairs ⁹⁵ . b) Il est difficile de savoir comment l'article 5 interagit avec les exigences prévues par le droit existant concernant l'identification au moyen de documents papier, notamment au vu de l'article 2-3 ⁹⁶ .

B. Article 6 – Obligations incombant aux prestataires de services de gestion de l'identité

1. Synthèse des commentaires répondant à des questions précises

<i>Question</i>	<i>Synthèse des commentaires</i>
1. Est-il souhaitable de conserver dans le chapeau les mots « au minimum » ?	a) Ces mots devraient être conservés ⁹⁷ . Ils indiquent clairement que la liste des fonctions remplies par les prestataires de services de gestion de l'identité n'est pas exhaustive ⁹⁸ . b) Ces mots sont difficilement interprétables si l'on ne sait pas quelles fonctions des prestataires de services de gestion de l'identité sont couvertes ⁹⁹ .

⁹⁵ Danemark.

⁹⁶ États-Unis.

⁹⁷ Liban, Sénégal, Suisse, UE (si l'instrument prend la forme d'une loi type), Ukraine, CIETAC, UINL.

⁹⁸ Ukraine.

⁹⁹ Danemark.

2. Synthèse des autres commentaires relatifs à l'article 6

<i>Question</i>	<i>Synthèse des commentaires</i>
1. Prise en compte des systèmes de gestion de l'identité multipartites	<p>a) Le projet de dispositions doit tenir compte des systèmes de gestion de l'identité multipartites, dans lesquels les fonctions énumérées à l'article 6 peuvent être remplies par différents participants au système, chacun pouvant assurer diverses fonctions¹⁰⁰.</p> <p>b) Dans un système de gestion de l'identité multipartite, la partie qui assure l'identification électronique devrait être responsable des autres fonctions énumérées à l'article 6 (relatives au contrôle d'identité et à la gestion des justificatifs d'identité), même si, en pratique, elle ne les remplit pas elle-même. En conséquence, même si la liste des fonctions figurant à l'article 6 est appropriée, il convient de modifier le libellé de cet article afin d'indiquer que, dans la pratique, certaines des fonctions énumérées peuvent être remplies par des personnes autres que le « prestataire de services de gestion de l'identité »¹⁰¹.</p>
2. Fonctions énumérées	<p>a) Il conviendrait de préciser les modalités d'inscription des sujets¹⁰².</p> <p>b) En général, ce n'est pas le prestataire de services de gestion de l'identité qui actualise les attributs (comme indiqué à l'article 6 b))¹⁰³.</p> <p>c) L'article 6 devrait également prévoir des obligations de confidentialité, de sécurité, de conservation et de continuité de service¹⁰⁴.</p>

C. Article 7 – Obligations incombant aux prestataires de services de gestion de l'identité en cas de violation des données

1. Synthèse des commentaires répondant à des questions précises

<i>Question</i>	<i>Synthèse des commentaires</i>
1. Le fait de « contenir » une atteinte à la sécurité constitue-t-il l'objectif visé par les mesures prises par le prestataire de services de gestion de l'identité pour y répondre, comme l'exige l'article 7-1 a) ?	<p>a) L'objectif visé est de « contenir » l'atteinte à la sécurité¹⁰⁵.</p> <p>b) L'objectif visé est de mettre fin à l'atteinte à la sécurité¹⁰⁶.</p> <p>c) Le fait de contenir l'atteinte à la sécurité n'est pas le seul objectif visé.</p> <p>d) Le fait de contenir l'atteinte à la sécurité n'est pas suffisant. L'objectif visé est de remédier à l'atteinte à la sécurité ou de l'atténuer¹⁰⁷.</p>

¹⁰⁰ États-Unis, Royaume-Uni. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 7 et 8).

¹⁰¹ Royaume-Uni.

¹⁰² El Salvador.

¹⁰³ Danemark.

¹⁰⁴ Sénégal.

¹⁰⁵ Liban, Royaume-Uni, Suisse, UE, Ukraine, CIETAC, UINL.

¹⁰⁶ Sénégal.

¹⁰⁷ Danemark.

2. Synthèse des autres commentaires relatifs à l'article 7

<i>Question</i>	<i>Synthèse des commentaires</i>
1. Terminologie	<p>a) Il est nécessaire de préciser le concept d'« incidence importante »¹⁰⁸.</p> <p>b) Il convient de préciser l'obligation de « remédier à l'atteinte ou à la perte » prévue à l'article 7-1 b)¹⁰⁹.</p> <p>c) Il n'est pas évident de savoir à quoi renvoie le terme « loi applicable »¹¹⁰.</p> <p><i>Note du Secrétariat : Le Groupe de travail a décidé d'insérer cette référence à la « loi applicable » à sa cinquante-neuvième session (voir A/CN.9/1005, par. 34 à 36).</i></p>
2. Conditions préalables	<p>a) Les obligations prévues à l'article 7 devraient s'appliquer pour toute atteinte à la sécurité (qu'elle ait ou non une « incidence importante »)¹¹¹.</p> <p>b) Les obligations prévues à l'article 7 ne devraient s'appliquer que si le prestataire de services de gestion de l'identité a connaissance de l'atteinte à la sécurité¹¹².</p>
3. Prise en compte des systèmes de gestion de l'identité multipartites	<p>a) Dans un système de gestion de l'identité multipartite, les obligations prévues à l'article 7 devraient être réparties entre les différents participants et imposées au participant responsable de la composante du système qui est atteinte ou compromise¹¹³.</p>

¹⁰⁸ États-Unis.

¹⁰⁹ États-Unis. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 9).

¹¹⁰ États-Unis.

¹¹¹ États-Unis.

¹¹² Singapour.

¹¹³ États-Unis, République dominicaine. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 8 et 9).

D. Article 8 – Obligations incombant aux abonnés

1. Synthèse des commentaires répondant à des questions précises

<i>Question</i>	<i>Synthèse des commentaires</i>
1. Existe-t-il des circonstances dans lesquelles les droits et obligations des tiers qui se fient à un service devraient être abordés dans le projet de dispositions (par exemple, pour notifier des atteintes dont ils ont connaissance) ?	<p>a) Le projet de dispositions ne devrait pas aborder les droits et obligations des tiers qui se fient à un service¹¹⁴. En général, les obligations des parties qui se fient à un service sont traitées dans les règles régissant le système de gestion de l'identité¹¹⁵.</p> <p>b) Le projet de dispositions ne devrait pas aborder les droits et obligations des parties qui se fient à un service dans le cas où il n'existe pas de relation contractuelle entre la partie qui se fie à un service et le prestataire de services de gestion de l'identité¹¹⁶. Si la partie qui se fie à un service est un participant au système de gestion de l'identité, elle devrait être soumise aux obligations prévues aux articles 6 et 7¹¹⁷.</p> <p>c) Le projet de dispositions devrait imposer l'obligation i) de n'utiliser le mécanisme d'identification électronique que conformément aux conditions du prestataire de services de gestion de l'identité, et ii) de ne pas utiliser le mécanisme d'identification à des fins ou pour des activités interdites par la loi, ou de manière discriminatoire¹¹⁸.</p>

2. Synthèse des autres commentaires relatifs à l'article 8

<i>Question</i>	<i>Synthèse des commentaires</i>
1. « Abonné »	<i>Voir la question 3 relative à l'article premier</i>
2. Portée des obligations	<p>a) Il ne serait peut-être pas raisonnable d'imposer aux abonnés les obligations prévues à l'article 8. Par exemple, un abonné peut avoir connaissance de circonstances qui indiquent que les justificatifs d'identité ou les mécanismes d'identification électronique ont été compromis, mais ne pas en mesurer l'importance. En outre, l'abonné ne serait peut-être pas en mesure de déterminer l'existence d'un « risque important »¹¹⁹.</p> <p>b) Le projet de dispositions devrait imposer à l'abonné l'obligation de notifier au prestataire de services de gestion de l'identité toute fraude ou usurpation de son identité¹²⁰.</p>

¹¹⁴ Danemark (également pour l'article 16), États-Unis, Liban (également pour l'article 16), Singapour, Suisse (également pour l'article 16), UE (également pour l'article 16), Ukraine (également pour l'article 16).

¹¹⁵ Danemark, UE.

¹¹⁶ États-Unis, Suisse.

¹¹⁷ République dominicaine.

¹¹⁸ Royaume-Uni. Le Groupe de travail voudra peut-être se demander si ces obligations supplémentaires devraient être imposées à l'abonné ou à une partie qui se fie à un service.

¹¹⁹ États-Unis. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 9 et 10).

¹²⁰ Niger.

E. Article 9 – Identification au moyen de la gestion de l'identité

1. Synthèse des commentaires répondant à des questions précises

<i>Question</i>	<i>Synthèse des commentaires</i>
1. Quelle est l'option la plus appropriée pour l'article 9-1 ?	a) L'option A ¹²¹ . b) L'option B ¹²² .
2. Quels sont les liens entre les articles 2-3 et 9 ?	a) Les articles 2-3 et 9 se contredisent ¹²³ . b) Il ressort clairement de l'article 2-3 que l'article 9 n'a pas d'incidence sur une éventuelle procédure particulière prescrite par la loi ¹²⁴ . L'article 9 s'applique si le droit interne exige une identification, mais pas dans le cas où cette identification doit se faire selon une procédure particulière ¹²⁵ . c) L'article 2-3 énonce le principe, tandis que l'article 9 traite de la méthode à suivre ¹²⁶ .
3. Faut-il conserver une disposition sur l'équivalence fonctionnelle pour l'identification, ou bien les éléments d'identification des signatures et des cachets électroniques sont-ils suffisants pour atteindre l'objectif souhaité, à savoir établir des normes d'équivalence fonctionnelle pour l'identification ?	a) Il convient de conserver une disposition sur l'équivalence fonctionnelle pour l'identification ¹²⁷ . b) Il serait préférable de ne pas conserver de disposition sur l'équivalence fonctionnelle pour l'identification ¹²⁸ . c) L'équivalence fonctionnelle n'est peut-être pas la question appropriée ¹²⁹ .
4. Si l'article 9 est maintenu, la norme de fiabilité de la méthode qui y est visée doit-elle être qualifiée de « suffisamment fiable » pour mieux refléter les différentes normes d'identification hors ligne ?	a) La norme de la méthode utilisée devrait être « suffisamment fiable » ¹³⁰ . b) Il faudrait définir ce qui s'entend par norme « suffisamment fiable » ¹³¹ . c) La norme ne devrait pas être qualifiée de « suffisamment fiable » ¹³² . d) Il n'est pas nécessaire de qualifier la norme de fiabilité, car la question de savoir si elle est appropriée est traitée à l'article 11 ¹³³ .

¹²¹ Fédération de Russie, Singapour, Suisse, UE, UINL.

¹²² Chine, Ukraine, CIETAC.

¹²³ États-Unis.

¹²⁴ Royaume-Uni.

¹²⁵ Singapour.

¹²⁶ Liban.

¹²⁷ Liban, Royaume-Uni, Sénégal, Singapour, Suisse.

¹²⁸ Chine, UINL.

¹²⁹ États-Unis.

¹³⁰ États-Unis, Liban, Royaume-Uni, Singapour, Suisse. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 12).

¹³¹ Sénégal, UINL.

¹³² Danemark.

¹³³ UE.

<i>Question</i>	<i>Synthèse des commentaires</i>
5. Est-il souhaitable d'insérer une disposition reconnaissant que le prestataire de services de gestion de l'identité pourrait être la personne qui cherche à se fier à l'identification électronique ?	<p>a) Une telle disposition est souhaitable¹³⁴. Seulement dans le cas d'un système de gestion de l'identité multipartite dont la partie qui se fie à l'identification électronique est un participant¹³⁵.</p> <p><i>Voir l'alinéa c) de la question 2 relative à l'article 2.</i></p> <p>b) Une telle disposition n'est pas nécessaire¹³⁶. Il ressort clairement du projet de dispositions que l'article 9 s'applique dans le cas où le prestataire de services de gestion de l'identité est la partie qui se fie à l'identification électronique¹³⁷. Cette précision pourrait figurer dans un document explicatif¹³⁸.</p>

2. Synthèse des autres commentaires relatifs à l'article 9

<i>Question</i>	<i>Synthèse des commentaires</i>
1. Étude des lois internes exigeant une identification	a) Le Groupe de travail devrait recenser les lois existantes qui imposent aux acteurs privés des exigences en matière d'identification ¹³⁹ .
2. Objet de l'évaluation de fiabilité (« méthode » de l'identification électronique ou « système de gestion de l'identité »/« services de confiance »)	<p>a) L'exigence de fiabilité devrait concerner non seulement la « méthode » de l'identification électronique, mais aussi le système de gestion de l'identité dans son ensemble¹⁴⁰.</p> <p><i>Voir également la question 2 relative à l'article 26</i></p>
3. Utilisation de la Loi type de la CNUDCI sur les signatures électroniques (LTSE) comme modèle	a) Il n'est pas certain qu'il faille utiliser la LTSE comme modèle pour les projets de dispositions sur la gestion de l'identité, étant donné que cette loi est plus complexe et concerne un plus grand nombre de parties ¹⁴¹ .

¹³⁴ Liban. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 4).

¹³⁵ États-Unis.

¹³⁶ Royaume-Uni, Suisse, UE.

¹³⁷ UE.

¹³⁸ Suisse.

¹³⁹ États-Unis. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 6 et 7).

¹⁴⁰ République dominicaine. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 12 et 13).

¹⁴¹ États-Unis, Royaume-Uni. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 10 et 11).

F. Article 10 – Facteurs pertinents pour déterminer la fiabilité

1. Synthèse des commentaires répondant à des questions précises

<i>Question</i>	<i>Synthèse des commentaires</i>
<p>1. L'article 10-1 d) vise à prendre en compte les systèmes de gestion de l'identité régis par des règles contractuelles comme les cadres de confiance. Il ne s'applique qu'aux parties à ces accords contractuels. La disposition remplit-elle adéquatement l'objectif visé ? Ou faut-il apporter des précisions supplémentaires (soit dans la disposition même, soit dans un document explicatif) ?</p>	<p>a) L'article 10-1 d) est suffisant dans son libellé actuel¹⁴².</p> <p>b) Il n'est pas évident de savoir i) comment les normes mentionnées aux articles 10 et 23 interagissent avec les accords contractuels, et ii) comment déterminer l'importance relative des accords contractuels et des autres facteurs énumérés aux articles 10 et 23 (notamment lorsque cette détermination est effectuée par la personne, l'organe ou l'autorité chargé de la désignation conformément aux articles 11-2 a) et 24-2 a))¹⁴³.</p> <p>c) L'article 10-1 d) devrait préciser à quels types d'accords il s'applique¹⁴⁴.</p> <p>d) L'article 10-1 devrait indiquer comment prendre en compte un accord conclu entre les parties lorsque le système de gestion de l'identité ne fournit pas d'authentification « forte »¹⁴⁵.</p> <p>e) Il conviendrait d'apporter des précisions concernant l'objet de l'article 10-1 d) dans un document explicatif¹⁴⁶.</p> <p>f) Un accord conclu entre les parties ne devrait pas être un facteur à prendre en compte pour déterminer la fiabilité. Il convient de déterminer la fiabilité des systèmes de gestion de l'identité et des services de confiance selon des normes communes¹⁴⁷.</p>
<p>2. Le titre de l'article 10 en reflète-t-il correctement le contenu ? Si ce n'est pas le cas, faudrait-il le remplacer par « Exigences pour déterminer la fiabilité » ? Les titres des articles 10 et 23 devraient-ils être harmonisés ?</p>	<p>a) Le titre de l'article 10 est approprié¹⁴⁸. Le titre de l'article 23 devrait être modifié en conséquence¹⁴⁹.</p> <p>b) Il convient de remplacer le titre de l'article 10 par « Exigences pour déterminer la fiabilité »¹⁵⁰. Le titre de l'article 23 devrait être modifié en conséquence¹⁵¹.</p>

¹⁴² Liban, Royaume-Uni.

¹⁴³ États-Unis (également pour l'article 23-1 h)).

¹⁴⁴ Suisse (également pour l'article 23-1 h)).

¹⁴⁵ UINL.

¹⁴⁶ Singapour.

¹⁴⁷ UE (également pour l'article 23-1 h)).

¹⁴⁸ Liban, Singapour, UINL.

¹⁴⁹ Singapour.

¹⁵⁰ Danemark, Royaume-Uni, Suisse, UE.

¹⁵¹ Danemark, Royaume-Uni, UE.

2. Synthèse des autres commentaires relatifs à l'article 10

<i>Question</i>	<i>Synthèse des commentaires</i>
1. Contenu de l'article 10	<p>a) Il conviendrait de remanier la liste des facteurs énumérés à l'article 10 de manière à en faire des exigences, un système de gestion de l'identité devant satisfaire chacune d'elles pour être considéré comme fiable¹⁵².</p> <p>b) L'article 10 devrait préciser comment évaluer chaque facteur et comment apporter la preuve de la conformité¹⁵³.</p> <p>c) La fiabilité dépend de nombreux facteurs, et il convient de ne pas chercher à les énumérer dans le projet de dispositions¹⁵⁴.</p>
2. « Normes et procédures internationales reconnues » pour la détermination de la fiabilité (art. 10-1 b))	<p>a) Il n'existe pas de telles normes et procédures¹⁵⁵ ou des éclaircissements sont nécessaires à cet égard¹⁵⁶.</p> <p>b) Aucun organisme n'établit de telles normes et procédures¹⁵⁷.</p>
3. Règles régissant la gouvernance (art. 10-1 b) i))	<p>a) Le libellé devrait indiquer que ces règles comprennent i) la vérification du moyen d'identification de la personne à identifier, ii) la présence physique de la personne à identifier, et iii) la vérification en face à face¹⁵⁸.</p> <p>b) Il convient de préciser le concept de « gouvernance »¹⁵⁹.</p>

G. Article 11 – Désignation des systèmes de gestion de l'identité fiables

1. Synthèse des commentaires répondant à des questions précises

Le modèle ne comportait pas de question précise concernant l'article 11.

2. Synthèse des autres commentaires relatifs à l'article 11

<i>Question</i>	<i>Synthèse des commentaires</i>
1. Processus de désignation des systèmes de gestion de l'identité fiables	a) Il est nécessaire de fournir des orientations et des précisions supplémentaires au sujet du processus de désignation ¹⁶⁰ .
2. « Normes et procédures internationales reconnues » pour la détermination de la fiabilité (art. 11-3)	<i>Voir la question 2 relative à l'article 10.</i>

¹⁵² UE.

¹⁵³ Danemark.

¹⁵⁴ États-Unis.

¹⁵⁵ États-Unis (également pour l'article 23-1 b)).

¹⁵⁶ Danemark.

¹⁵⁷ Danemark, États-Unis (également pour l'article 23-1 b)).

¹⁵⁸ Chine.

¹⁵⁹ CIETAC.

¹⁶⁰ Danemark.

H. Article 12 – Responsabilité des prestataires de services de gestion de l’identité

1. Synthèse des commentaires répondant à des questions précises

<i>Question</i>	<i>Synthèse des commentaires</i>
1. Quelle est l’option la plus appropriée pour l’article 12 ?	<ul style="list-style-type: none"> a) L’option A¹⁶¹. b) L’option B¹⁶². c) L’option C¹⁶³. d) Aucune n’est préférable¹⁶⁴.
2. Si l’option A est préférée, est-il même nécessaire d’inclure une telle disposition sur la responsabilité ?	<ul style="list-style-type: none"> a) Une disposition sur la responsabilité serait tout de même nécessaire ou souhaitable¹⁶⁵. b) Une disposition sur la responsabilité ne serait pas nécessaire¹⁶⁶.
3. Si l’option B ou l’option C est préférée, est-il nécessaire d’inclure une clause d’exonération de responsabilité couvrant les prestataires publics de services de gestion de l’identité ?	<ul style="list-style-type: none"> a) Une exonération de responsabilité pour les prestataires publics de services de gestion de l’identité et de services de confiance ne serait pas nécessaire¹⁶⁷. D’après les articles 12-2 et 25-2 (option C), cette question est laissée au droit applicable¹⁶⁸. Quoi qu’il en soit, il ne devrait pas être possible de limiter la responsabilité en cas de décès ou de blessure d’une personne¹⁶⁹. b) Une exonération de responsabilité pour les prestataires publics de services de gestion de l’identité et de services de confiance serait nécessaire¹⁷⁰. c) Une telle exonération serait probablement trop large, et il ne devrait être décidé de l’instaurer qu’une fois connu le régime de responsabilité prévu par le droit existant¹⁷¹.

¹⁶¹ Liban (également pour l’article 25), Suisse (également pour l’article 25).

¹⁶² UINL (mais option A pour l’article 25).

¹⁶³ Argentine (uniquement pour l’article 25), Danemark (également pour l’article 25), Fédération de Russie (également pour l’article 25), Royaume-Uni (également pour l’article 25), Sénégal (également pour l’article 25), Singapour (également pour l’article 25), UE (également pour l’article 25), Ukraine (également pour l’article 25).

¹⁶⁴ États-Unis.

¹⁶⁵ Liban (également pour l’article 25, option A préférée), Suisse (également pour l’article 25, option A préférée).

¹⁶⁶ Argentine (uniquement pour l’article 25), États-Unis (aucune option préférée), Ukraine (également pour l’article 25, option C préférée), UINL (option B préférée, mais option A pour l’article 25).

¹⁶⁷ Danemark (également pour l’article 25), Royaume-Uni (également pour l’article 25), Sénégal (également pour l’article 25), Ukraine (également pour l’article 25), UE (également pour l’article 25), UINL.

¹⁶⁸ Royaume-Uni (également pour l’article 25), UE (également pour l’article 25).

¹⁶⁹ Royaume-Uni (également pour l’article 25).

¹⁷⁰ CIETAC (également pour l’article 25).

¹⁷¹ États-Unis.

*Question**Synthèse des commentaires*

4. Si l'option B ou l'option C est préférée, est-il souhaitable de traiter différemment la responsabilité d'un prestataire de services de gestion de l'identité découlant de l'utilisation d'un système de gestion de l'identité désigné conformément à l'article 11 ? Le cas échéant, selon quelles modalités ?

- a) Le projet de dispositions pourrait limiter la responsabilité des prestataires de services de gestion de l'identité et de services de confiance exploitant un système de gestion de l'identité désigné¹⁷².
- b) Le projet de dispositions pourrait établir une présomption de faute de la part des prestataires de services de gestion de l'identité et de services de confiance exploitant un système de gestion de l'identité désigné ou proposant un service de confiance désigné¹⁷³.
- c) Le projet de dispositions pourrait établir une présomption d'absence de faute de la part des prestataires de services de gestion de l'identité exploitant un système de gestion de l'identité désigné¹⁷⁴.
- d) L'article 12 ne devrait s'appliquer qu'aux prestataires de services de gestion de l'identité et de services de confiance exploitant un système de gestion de l'identité désigné ou proposant un service de confiance désigné¹⁷⁵.
- e) Le texte relatif à cette question devrait être placé entre crochets¹⁷⁶.

2. Synthèse des autres commentaires relatifs à l'article 12

*Question**Synthèse des commentaires*

1. Prise en compte des systèmes de gestion de l'identité multipartites

- a) Le projet de dispositions devrait également traiter de la responsabilité des autres participants à un système de gestion de l'identité multipartite (par exemple, agents d'inscription, fournisseurs d'attributs, fournisseurs d'authentification)¹⁷⁷.

2. Options pour ce qui est de limiter la responsabilité des prestataires de services de gestion de l'identité

- a) Un prestataire de services de gestion de l'identité ne devrait pas être tenu responsable vis-à-vis d'une partie qui se fie à un service si elle a subi des dommages pour s'être fiée à un justificatif compromis alors qu'elle aurait dû savoir que ce justificatif était compromis¹⁷⁸.
- b) Un prestataire de services de gestion de l'identité ou de services de confiance ne devrait pas être tenu responsable vis-à-vis d'un abonné pour des dommages dus à un niveau de garantie insuffisant i) si l'abonné savait que le niveau de garantie était insuffisant, ou ii) si l'abonné n'a pas procédé à une évaluation des risques suffisante pour déterminer le niveau de garantie requis¹⁷⁹.

¹⁷² Singapour (également pour l'article 25).

¹⁷³ UE (également pour l'article 25).

¹⁷⁴ Royaume-Uni.

¹⁷⁵ Danemark (également pour l'article 25).

¹⁷⁶ États-Unis.

¹⁷⁷ Argentine, États-Unis. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 15).

¹⁷⁸ États-Unis.

¹⁷⁹ Royaume-Uni (également pour l'article 25).

Question

Synthèse des commentaires

3. Opportunité de traiter la question de la responsabilité

- a) En général, la responsabilité est traitée dans les règles régissant le système de gestion de l'identité et varie donc selon le type de système¹⁸⁰.
- b) Il est nécessaire d'examiner plus avant le régime de responsabilité prévu par le droit existant (notamment la mesure dans laquelle les parties peuvent répartir la responsabilité entre elles par convention)¹⁸¹.

Voir également la question 2 relative à l'article 3.

4. Terminologie

- c) Les questions relatives à la responsabilité sont très complexes et il sera peut-être difficile de parvenir à un consensus¹⁸².
- a) L'option C des articles 12 et 25 devrait prévoir non seulement que les prestataires de services de gestion de l'identité ou de services de confiance sont « tenus responsables des dommages », mais aussi qu'ils assument les « conséquences juridiques » du manquement à leurs obligations¹⁸³.
- b) Il convient de préciser le concept de « conséquences juridiques », qui est utilisé dans l'option B des articles 12 et 25¹⁸⁴.
- c) Le terme « dommages », qui apparaît dans l'option C (art. 12-1), s'entend comme signifiant « préjudice »¹⁸⁵.

5. Nature de la responsabilité

- a) Le projet de dispositions devrait préciser que la responsabilité des prestataires de services de gestion de l'identité et de services de confiance peut être de nature civile ou pénale. Toute négligence volontaire de la part du prestataire de services de gestion de l'identité ou de services de confiance concernant le respect de ses obligations peut engager sa responsabilité pénale¹⁸⁶.

¹⁸⁰ États-Unis. Voir également les commentaires présentés par la Banque mondiale (A/CN.9/WG.IV/WP.163, p. 14 et 16).

¹⁸¹ États-Unis (également pour l'article 25).

¹⁸² CIETAC.

¹⁸³ Fédération de Russie (également pour l'article 25).

¹⁸⁴ États-Unis (également pour l'article 25).

¹⁸⁵ États-Unis.

¹⁸⁶ Madagascar (également pour l'article 25).