



Assemblée générale

Distr. limitée
10 septembre 2021
Français
Original : anglais

**Commission des Nations Unies
pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Soixante-deuxième session
Vienne, 22-26 novembre 2021**

Note explicative sur le projet de dispositions relatives à l'utilisation et à la reconnaissance internationale de la gestion de l'identité et des services de confiance

Note du Secrétariat

Table des matières

	<i>Page</i>
I. Introduction	2
Annexe	
Note explicative sur le projet de dispositions relatives à l'utilisation et à la reconnaissance internationale de la gestion de l'identité et des services de confiance	3
I. Introduction	3
A. Objet de la présente note explicative	3
B. Objectifs	3
C. Champ d'application	4
D. Structure	4
E. Généralités	5
F. Concepts et principes fondamentaux	6
II. Commentaire par article	9
A. Chapitre I. Dispositions générales (art. 1 à 4)	9
B. Chapitre II. Gestion de l'identité (art. 5 à 12)	14
C. Chapitre III. Services de confiance (art. 13 à 24)	23
D. Chapitre IV. Aspects internationaux (art. 25 et 26)	29



I. Introduction

1. À sa soixante et unième session, le Groupe de travail a demandé au secrétariat de lui présenter des projets de documents explicatifs avec la version révisée du projet de dispositions afin qu'il l'examine à sa soixante-deuxième session. Ces documents figurent dans la note explicative annexée au présent document.
2. La note explicative a été établie par le secrétariat afin que le Groupe de travail l'examine et l'adopte éventuellement. Elle rend compte des délibérations du Groupe de travail, telles qu'elles ont été communiquées à la Commission, ainsi que d'autres informations contextuelles sur le mandat du Groupe de travail. Elle renvoie au projet de dispositions figurant dans le document [A/CN.9/WG.IV/WP.170](#) et sera modifiée en fonction des éventuelles modifications qui seront apportées à ces dispositions – et des éventuelles observations – telles qu'approuvées par le Groupe de travail à sa soixante-deuxième session. La note explicative peut également aider le Groupe de travail à finaliser le projet de dispositions.

Annexe

Note explicative sur le projet de dispositions relatives à l'utilisation et à la reconnaissance internationale de la gestion de l'identité et des services de confiance

I. Introduction

A. Objet de la présente note explicative

1. [à compléter]

B. Objectifs

2. Au cours des 20 dernières années, les activités commerciales en ligne ont connu une croissance exponentielle (c'est-à-dire des opérations électroniques entre entreprises, entre entreprises et consommateurs, et entre entreprises et États). De 64 milliards de dollars en 1999, le commerce électronique mondial est passé à 29 000 milliards de dollars en 2017¹, croissance qui coïncide avec celle de l'accès à Internet pour les particuliers et les entreprises. Par exemple, la part des ménages ayant accès à Internet est passée de 35 % en 2002 à 83,6 % en 2017². La disponibilité de services publics (y compris des services à caractère commercial), bancaires et de paiement en ligne a augmenté dans les mêmes proportions.

3. Cette croissance est alimentée par la confiance accordée à l'environnement en ligne et doit pouvoir s'appuyer sur un sentiment de confiance dans cet environnement. La capacité à identifier chaque partie de manière fiable, surtout en l'absence de toute interaction personnelle préalable, constitue l'un des aspects importants de la confiance en ligne. Au fil des années, diverses solutions ont été proposées pour répondre au besoin d'identification en ligne, ce qui a conduit à la multiplication des systèmes, des méthodes, des technologies et des dispositifs destinés à créer et gérer des identités numériques de personnes physiques et morales. Le traitement au niveau mondial des aspects juridiques de la gestion de l'identité peut permettre non seulement de relier ces différentes solutions, mais aussi de favoriser l'interopérabilité des systèmes de gestion de l'identité, qu'ils soient exploités par des opérateurs privés ou publics.

4. Le développement du recours à la gestion de l'identité et aux services de confiance se heurte à des obstacles. Parmi les obstacles de nature juridique figurent notamment : 1) l'absence de législation donnant des effets juridiques à la gestion de l'identité et aux services de confiance ; 2) l'existence d'approches juridiques divergentes en matière de gestion de l'identité, notamment de lois fondées sur des exigences spécifiques à une technologie ; 3) l'application de lois exigeant des documents d'identité papier pour la conclusion d'opérations commerciales en ligne ; et 4) l'absence de mécanismes pour la reconnaissance juridique internationale de la gestion de l'identité et des services de confiance³.

5. Le principal objectif du [projet d'instrument] est de surmonter ces obstacles en élaborant des règles juridiques uniformes. Ces règles ont plusieurs objectifs : accroître l'efficacité ; abaisser les coûts des opérations ; augmenter la sécurité des opérations électroniques, notamment la sécurité juridique, de manière à instaurer la

¹ CNUCED, Rapport sur le commerce électronique et le développement 2001, document des Nations Unies, UNCTAD/SDTE/ECB/1, p. 44 (disponible en anglais seulement) ; CNUCED, Rapport sur l'économie numérique 2019 – Création et captation de valeur : incidences pour les pays en développement, document des Nations Unies, UNCTAD/DER/2019, p. 15.

² UIT, Statistiques sur les TIC, Évolution des TIC à l'échelle mondiale, 2001-2018, disponible (en anglais seulement) à l'adresse www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

³ A/CN.9/965, par. 52.

confiance ; et contribuer à réduire la fracture numérique grâce à des solutions harmonisées.

6. Ce faisant, le [projet d'instrument] contribue à la réalisation des objectifs de développement durable. Plus précisément, l'importance de l'identité est soulignée dans l'objectif de développement durable n° 16, dont la cible 9 consiste à garantir à tous une identité juridique, ce qui, dans le contexte de l'économie numérique, correspond au droit à une identité numérique. L'établissement d'un cadre juridique pour la gestion de l'identité et les services de confiance aidera à rendre l'identité numérique opérationnelle en toute sécurité. En favorisant la confiance dans l'environnement en ligne, ce cadre contribuera également au développement durable et à l'inclusion sociale, conformément à l'objectif de développement durable n° 9, qui vise, entre autres, à encourager l'innovation.

C. Champ d'application

7. [à compléter]

D. Structure

8. Le [projet d'instrument] comprend quatre chapitres, traitant respectivement des dispositions générales, de la gestion de l'identité, des services de confiance et des aspects internationaux. Les chapitres I et IV s'appliquent à la fois à la gestion de l'identité et aux services de confiance. En outre, la structure et le contenu des chapitres II et III présentent d'importantes analogies. Les remarques sur une disposition du chapitre II peuvent également s'appliquer à la disposition correspondante du chapitre III, dans la mesure où les dispositions coïncident. C'est le cas, en particulier, des articles 13, 14, 15, 22, 23 et 24, par rapport aux articles 5, 6 et 7, 8, 10, 11 et 12, respectivement.

9. Le chapitre I contient les définitions de certains termes utilisés dans le [projet d'instrument] ; délimite le champ d'application ; contient des dispositions relatives à l'utilisation volontaire de systèmes de gestion de l'identité et de services de confiance, y compris de services particuliers ; définit la relation entre le [projet d'instrument] et d'autres lois, notamment les exigences relatives à l'identification ou à l'utilisation de services de confiance spécifiques ; et contient des dispositions relatives à l'interprétation autonome, notamment pour combler des lacunes, du [projet d'instrument] compte tenu de son caractère uniforme et de son origine internationale.

10. Le chapitre II définit les principaux éléments du régime juridique applicable à la gestion de l'identité, énonce un certain nombre d'obligations fondamentales qui incombent aux prestataires de services de gestion de l'identité et aux abonnés, et fixe des règles en ce qui concerne la responsabilité des prestataires de services de gestion de l'identité. L'article 5 établit le principe de la reconnaissance juridique de l'identification électronique et de la non-discrimination à l'égard de l'utilisation de services de gestion de l'identité. L'article 6 énonce les principales obligations qui incombent aux prestataires de services de gestion de l'identité ; ce faisant, il recense les principales étapes du cycle de vie de la gestion de l'identité. L'article 7 traite des obligations qui incombent aux prestataires de services de gestion de l'identité en cas de violation des données et est complété par l'article 8, relatif aux obligations des abonnés lorsque les justificatifs d'identité ont été compromis. L'article 9 contient une règle d'équivalence fonctionnelle entre l'identification hors ligne et l'identification électronique qui exige l'utilisation d'une méthode fiable. La fiabilité de la méthode est évaluée au moyen d'une détermination *ex post* sur la base des circonstances visées à l'article 10 ou au moyen d'une désignation *ex ante* conformément à l'article 11. En outre, lorsqu'une méthode a effectivement rempli sa fonction, il n'est pas nécessaire de déterminer sa fiabilité. Enfin, l'article 12 traite de la responsabilité des prestataires de services de gestion de l'identité.

11. Le chapitre III définit les principaux éléments constitutifs du régime juridique applicable à l'utilisation des services de confiance. L'article 13 contient une règle générale sur la non-discrimination à l'égard des effets juridiques des services de confiance. L'article 14 énonce les obligations qui incombent aux prestataires de services de confiance et l'article 15 traite des obligations qui incombent aux abonnés des services de confiance lorsque ces derniers ont été compromis. Les articles 16 à 21 décrivent les fonctions que remplissent certains services de confiance mentionnés (signatures électroniques ; cachets électroniques ; horodatages électroniques ; archivage électronique ; services d'envoi recommandé électroniques ; authentification de site Web) et les exigences associées, notamment l'utilisation d'une méthode fiable. Les dispositions relatives aux services de confiance mentionnés ont pour la plupart été rédigées sous forme de règles d'équivalence fonctionnelle. Cependant, étant donné qu'un service de confiance risque de ne pas avoir d'équivalent papier, une règle d'équivalence fonctionnelle n'est pas indispensable. L'article 22 donne des indications sur la détermination *ex post* de la fiabilité de la méthode utilisée par le service de confiance et l'article 23 sur sa désignation *ex ante*. Enfin, l'article 24 énonce des règles sur la responsabilité des prestataires de services de confiance.

12. Le chapitre IV traite de la reconnaissance internationale de la gestion de l'identité et des services de confiance, qui est l'un des principaux objectifs du [projet d'instrument]. Le [projet d'instrument] n'envisage pas la création d'un organisme spécialisé dans la reconnaissance juridique de la gestion de l'identité et des services de confiance, mais prévoit plusieurs mécanismes se fondant sur une approche décentralisée. Outre les articles 25 et 26, les dispositions spécifiques des articles 10-3, 11-4, 22-3 et 23-4, relatives à la non-discrimination géographique lors de la détermination de la fiabilité des services de gestion de l'identité et des services de confiance et lors de la désignation de services de gestion de l'identité et de services de confiance fiables, sont directement pertinentes. Les accords contractuels peuvent également être pertinents pour l'utilisation des systèmes de gestion de l'identité et des services de confiance à l'échelle internationale.

E. Généralités

1. Historique

13. [voir par. 4 à 20 du document [A/CN.9/WG.IV/WP.169](#)]

14. [à compléter]

2. Relation avec les textes existants de la CNUDCI

15. Les textes existants de la CNUDCI ne contiennent pas de dispositions sur les services de confiance. Cependant, ils contiennent des règles d'équivalence fonctionnelle qui peuvent être pertinentes pour certains services de confiance. En particulier, l'article 7 de la Loi type de la CNUDCI sur le commerce électronique (LTCE), l'article 6 de la Loi type de la CNUDCI sur les signatures électroniques (LTSE), l'article 9-3 de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (CCE) et l'article 9 de la Loi type de la CNUDCI sur les documents transférables électroniques énoncent les exigences auxquelles les signatures électroniques doivent satisfaire pour être fonctionnellement équivalentes aux signatures papier. L'article 16 du [projet d'instrument] se fonde sur l'article 9 de la Loi type de la CNUDCI sur les documents transférables électroniques. De même, l'article 10 de la LTCE énonce les règles d'équivalence fonctionnelle applicables à la conservation des données. L'article 19 du [projet d'instrument] se fonde sur l'article 10-1 de la LTCE.

16. Les articles 16 à 21 du [projet d'instrument] traitent des services de confiance qui ont pour objet de garantir certaines qualités d'un message de données. Cependant, les services de confiance visés par ces dispositions n'ont pas tous d'équivalent papier. En outre, il ne sera peut-être pas nécessaire d'utiliser un service de confiance

mentionné dans le [projet d'instrument] pour satisfaire aux règles d'équivalence fonctionnelle énoncées dans ces textes de la CNUDCI.

F. Concepts et principes fondamentaux

17. Cette section explique plusieurs concepts et principes fondamentaux qui sous-tendent le [projet d'instrument]. Les termes définis dans le [projet d'instrument] sont expliqués plus avant dans le commentaire sur l'article premier ci-dessous, tandis qu'une liste plus exhaustive des termes et concepts relatifs à la gestion de l'identité et aux services de confiance, établie sur la base des définitions contenues dans des textes juridiques et techniques internationalement reconnus, figure dans le document [A/CN.9/WG.IV/WP.150](#). Comme indiqué dans ce document, ces textes emploient parfois des termes différents pour le même concept ou définissent le même terme différemment.

1. Principes fondamentaux

18. Tout comme les textes existants de la CNUDCI, le [projet d'instrument] se fonde sur les principes d'autonomie des parties, de neutralité technologique, d'équivalence fonctionnelle et de non-discrimination à l'égard de l'utilisation des moyens électroniques, sous réserve de toute modification⁴. Bien que le [projet d'instrument] ne les énonce pas expressément, ces principes généraux encadrent les principales dispositions du texte. Par exemple, le principe de non-discrimination, tel qu'il s'applique à la gestion de l'identité et aux services de confiance, est énoncé aux articles 5 et 13, respectivement, tandis que le principe d'équivalence fonctionnelle sous-tend les articles 9 et 16 à 21.

19. L'approche d'équivalence fonctionnelle présuppose l'existence d'exigences légales qui prévoient directement ou indirectement l'exécution d'une opération physique ou sur papier, telle que l'utilisation d'un justificatif papier pour identifier une personne ou une communication papier pour authentifier un fait ou une chose. Elle analyse ensuite les objectifs et les fonctions de ces exigences en vue de déterminer comment atteindre ces objectifs ou remplir ces fonctions par des moyens électroniques. Toutefois, tout comme la technologie numérique a rendu possible des activités qui n'ont pas d'équivalent papier, certains services de gestion de l'identité et certains services de confiance visés par le [projet d'instrument] n'ont peut-être pas d'équivalent papier.

2. Gestion de l'identité

20. L'identification est le processus qui consiste à distinguer une personne sur la base d'informations la concernant (à savoir des attributs). Ces informations peuvent être recueillies ou observées. L'identification est particulièrement importante pour instaurer la confiance dans les opérations en ligne. Elle consiste essentiellement à vérifier que les attributs recueillis ou observés correspondent à une « identité » préalablement établie pour la personne identifiée. Ainsi, l'identification a souvent lieu lorsqu'une identité particulière est invoquée et que des attributs sont présentés en vue de leur vérification.

21. En conséquence, en vertu du [projet d'instrument], la gestion de l'identité comporte deux étapes (ou phases) distinctes : tout d'abord, la délivrance de justificatifs d'identité, c'est-à-dire de données qui peuvent être présentées pour une identification électronique ; ensuite, la présentation et la vérification de ces justificatifs par des moyens électroniques :

a) La première étape de la gestion de l'identité consiste à recueillir les attributs qui peuvent constituer l'« identité fondamentale » de la personne (c'est-à-dire les attributs enregistrés par les organismes publics dans les registres et

⁴ [A/CN.9/902](#), par. 52 et 63.

statistiques de l'état civil lorsqu'il s'agit de personnes physiques et dans les registres des sociétés et des entreprises lorsqu'il s'agit de personnes morales). Ces attributs peuvent être présentés sous la forme de justificatifs délivrés par les administrations publiques (par exemple, un certificat d'enregistrement) et vérifiés auprès de l'organisme émetteur. Ce processus, qui peut être exécuté « hors ligne » à l'aide de justificatifs matériels présentés en personne, aboutit à la délivrance de justificatifs à la personne ;

b) La seconde étape de la gestion de l'identité implique la présentation de ces justificatifs par des moyens électroniques et la vérification par des moyens électroniques que la personne présentant les justificatifs est bien celle à qui les justificatifs ont été délivrés lors de la première étape.

22. Les systèmes de gestion de l'identité sont utilisés pour gérer les processus d'identification associés à chacune de ces étapes, ainsi que pour gérer les attributs recueillis, les justificatifs d'identité délivrés et les moyens utilisés pour la vérification. Ils peuvent faire intervenir une seule entité qui exécute tous les processus requis à chaque étape de la gestion de l'identité, ou différentes entités. En outre, certains systèmes de gestion de l'identité peuvent offrir différents « services » de gestion de l'identité en fonction des besoins des parties (à savoir la partie qui cherche à identifier et la partie qui cherche à être identifiée).

23. Les systèmes de gestion de l'identité sont utilisés pour fournir des services de gestion de l'identité. Ils peuvent être exploités par des entités publiques ou privées et offrir différents services de gestion de l'identité. Dans la pratique, les systèmes publics de gestion de l'identité correspondent généralement à un service unique de gestion de l'identité, tandis que les systèmes privés peuvent correspondre à plusieurs services ayant différents niveaux de fiabilité. Les systèmes de gestion de l'identité peuvent aussi être classés en fonction de leur caractère centralisé ou décentralisé. Le [projet d'instrument] est neutre quant à la technologie et au modèle utilisés et peut donc s'appliquer à tous types de systèmes et de services de gestion de l'identité.

24. Les prestataires de services de gestion de l'identité, les abonnés, les parties utilisatrices et les autres entités concernées peuvent accepter d'opérer dans le cadre de politiques, de normes et de technologies compatibles spécifiées dans les règles du système, afin que les justificatifs fournis par chaque prestataire de services de gestion de l'identité participant puissent être compris et reconnus par toutes les parties utilisatrices participantes. Cet arrangement peut être appelé « fédération d'identité » et les règles du système, qui sont de nature contractuelle, « cadre de confiance ». La fédération d'identité peut permettre d'augmenter le nombre d'utilisateurs et d'applications utilisant les mêmes services de gestion de l'identité, ce qui, à son tour, peut aider à maîtriser les coûts et à assurer la viabilité à long terme.

3. Services de confiance

25. Les services de confiance jouent également un rôle important pour instaurer la confiance dans l'utilisation des opérations électroniques. Ils visent essentiellement à fournir une assurance quant à certaines qualités des messages de données, telles que la source, l'intégrité et le moment où certains actes concernant les données ont été exécutés. Si le [projet d'instrument] recense un certain nombre de services de confiance couramment utilisés, il reconnaît que d'autres services de confiance peuvent exister ou être mis au point à l'avenir.

26. La notion de service de confiance telle qu'employée dans le [projet d'instrument] concerne la prestation d'un service mais pas seulement ce service. Par exemple, elle concerne les services qui prennent en charge les méthodes de création et de gestion d'une signature électronique, mais pas seulement la signature électronique.

4. Détermination de la fiabilité

27. Conformément aux textes existants de la CNUDCI, plusieurs dispositions du [projet d'instrument] font référence à l'utilisation d'une méthode fiable. Le [projet d'instrument] prévoit deux mécanismes pour déterminer la fiabilité de la méthode : les articles 10 et 22 fournissent une liste indicative des facteurs pertinents pour déterminer la fiabilité ; et les articles 11 et 23 prévoient un mécanisme pour désigner des méthodes fiables. Cette approche s'appuie sur les articles 6 et 7 de la LTSE.

28. En associant ces deux aspects (détermination de la fiabilité et désignation d'une méthode fiable), le [projet d'instrument] ne favorise pas un mécanisme par rapport à l'autre, mais vise à combiner les avantages des deux mécanismes tout en minimisant leurs inconvénients et à permettre en fin de compte aux parties de choisir la solution préférée.

29. Les textes de la CNUDCI traitant des services de confiance ne contiennent pas tous des dispositions prévoyant à la fois l'approche *ex ante* et l'approche *ex post*. Toutefois, ces deux approches sont généralement considérées comme compatibles et complémentaires.

a) Détermination *ex post* de la fiabilité

30. La détermination de la fiabilité n'intervient qu'en cas de litige, donc après l'utilisation de la méthode (*ex post*). D'une manière générale, le [projet d'instrument] permet donc de réaliser des opérations de gestion de l'identité, et prévoit qu'il faut déterminer la fiabilité de la méthode utilisée qu'en cas de contestation de la validité d'une opération du fait qu'une ou plusieurs parties n'ont pas été identifiées ou pas de manière suffisante.

31. L'approche *ex post* a le mérite d'offrir aux parties un maximum de souplesse dans le choix des technologies et des méthodes. En outre, elle permet une gestion décentralisée et ne requiert pas la mise en place d'un mécanisme institutionnel, évitant ainsi les coûts susceptibles d'en découler.

32. En revanche, l'approche *ex post* présente l'inconvénient de ne pas favoriser la sécurité juridique à l'avance et n'offre aucune prévisibilité aux parties quant à la validité de la méthode utilisée, les exposant ainsi potentiellement à des risques supplémentaires dans le cas où la méthode utilisée ne serait pas considérée comme fiable. En outre, la fiabilité de la méthode est déterminée au moyen d'un processus d'arbitrage par un tiers, ce qui peut prendre du temps et conduire à des décisions incohérentes.

b) Désignation *ex ante* de services fiables

33. La désignation de services fiables a lieu avant qu'une méthode ne soit utilisée (*ex ante*), sur la base d'une liste de circonstances prédéterminées, et ce de manière générale et non par référence à une opération particulière. La définition ultérieure des circonstances énoncées dans le [projet d'instrument] ne devrait pas conduire à l'imposition d'exigences spécifiques à une technologie.

34. La désignation ne s'applique pas à des types génériques de services de gestion de l'identité et de services de confiance ou à l'ensemble des services de gestion de l'identité et des services de confiance offerts par un prestataire, mais plutôt à un service particulier fourni par un prestataire de services donné.

35. Par rapport à l'approche *ex post*, l'approche *ex ante* peut fournir plus de clarté et de prévisibilité en ce qui concerne l'effet juridique des services de gestion de l'identité et des services de confiance, y compris lorsqu'ils sont utilisés à l'échelle internationale. Toutefois, sa gouvernance doit lui permettre de s'adapter rapidement à toute évolution technologique afin de ne pas entraver l'innovation. Autrement, elle risque de discriminer les services de gestion de l'identité et les services de confiance qui, bien que disponibles et basés sur des méthodes fiables, n'ont pas été pas désignés.

36. L'État adoptant doit nommer l'entité chargée de la désignation, qui peut être un organisme privé ou public. Ces entités peuvent être accréditées conformément aux normes techniques applicables aux organismes de certification des produits, des processus et des services. La certification (y compris l'autocertification) est également utile pour évaluer les services sur la base de normes axées sur les résultats et peut donc être pertinente pour leur désignation.

37. Le mécanisme institutionnel nécessaire à la mise en œuvre de l'approche *ex ante* requiert un mécanisme spécifique de désignation qui est souvent géré de manière centralisée. Ce mécanisme comprend divers éléments tels que les critères d'évaluation des services, les détails du processus d'évaluation des décisions et les sources de financement. En fonction de plusieurs facteurs, notamment des dispositifs institutionnels, la gouvernance du système d'octroi de licences risque d'être complexe et coûteuse. Pour cette raison, la désignation peut s'appliquer de préférence aux services qui offrent un niveau de garantie et de fiabilité plus élevé et qui sont donc utilisés pour des opérations de valeur supérieure. Pour les États adoptants désireux d'utiliser l'approche *ex ante*, le [projet d'instrument] présuppose l'existence du mécanisme institutionnel nécessaire et ne prévoit pas sa mise en place ou son administration.

5. Aspects internationaux

38. Le [projet d'instrument] vise principalement à autoriser, sur le plan juridique, l'utilisation internationale des systèmes de gestion de l'identité et des services de confiance. Pour ce faire, il applique les principes de la neutralité technologique et de la non-discrimination à l'égard de l'origine géographique. Ces principes sous-tendent les articles 10-3, 11-4, 22-3 et 23-4 du [projet d'instrument]. En outre, le chapitre IV (art. 25 et 26) traite spécifiquement de la reconnaissance internationale.

39. Le [projet d'instrument] n'exige pas la mise en place d'un dispositif institutionnel formel pour la reconnaissance juridique internationale. Toutefois, il existe de tels dispositifs aux niveaux régional et bilatéral. Les États adoptants voudront peut-être utiliser le [projet d'instrument] comme modèle pour établir un dispositif institutionnel avec des partenaires internationaux, notamment dans le cadre d'un accord spécifique.

40. Le [projet d'instrument] peut également contribuer à la mise en œuvre des dispositions relatives à la reconnaissance juridique mutuelle figurant dans les accords de libre-échange ou dans les accords sur l'économie numérique.

II. Commentaire par article

A. Chapitre I. Dispositions générales (art. 1 à 4)

1. Article premier. Définitions

41. L'article premier contient les définitions des termes utilisés dans le [projet d'instrument]⁵.

« *Attribut* »

42. Par « attribut », on entend un élément d'information ou de donnée associé à une personne. Les attributs d'une personne physique peuvent être notamment le nom, l'adresse, l'âge et l'adresse électronique, ainsi que des données telles que la présence du sujet sur les réseaux et l'appareil utilisé. Les attributs d'une personne morale sont notamment la raison sociale, le siège social, le nom d'enregistrement, le pays

⁵ Une liste de termes et de concepts relatifs à la gestion de l'identité et aux services de confiance, compilée sur la base des définitions figurant dans des textes juridiques et techniques internationalement reconnus, a été établie à l'appui de l'élaboration du [projet d'instrument] et est disponible dans le document [A/CN.9/WG.IV/WP.150](#).

d'enregistrement. La notion d'attribut est utilisée dans la définition du terme « identité ».

43. Les attributs peuvent contenir des données personnelles dont le traitement est soumis à la loi sur la confidentialité et la protection des données. Le [projet d'instrument] ne traite pas de la confidentialité et de la protection des données et préserve expressément l'application de cette loi.

Références

[A/CN.9/WG.IV/WP.150](#), par. 13.

« Message de données »

44. La définition du terme « message de données » figure dans tous les textes existants de la CNUDCI sur le commerce électronique. Ce terme est le principal point de référence pour définir les exigences des services de confiance puisque le résultat de l'utilisation d'un service de confiance est l'assurance des qualités d'un message de données.

Références

[A/CN.9/1045](#), par. 40.

« Identification électronique » [« Authentification »]

45. Par « identification électronique », on désigne la vérification du lien entre l'identité prétendue et les justificatifs présentés, ce qui constitue la seconde étape de la gestion de l'identité. Ce terme est utilisé à la place du terme « authentification » pour répondre aux préoccupations concernant les multiples significations du terme « authentification ». Du point de vue technique, le terme « authentification » désigne la présentation d'une preuve de l'identité.

46. Le terme « identification » sans qualificatif est utilisé dans un sens non technique à l'article 9.

Références

[A/CN.9/1005](#), par. 13, 84 à 86 et 92 ; [A/CN.9/1045](#), par. 134 à 136 ; [A/CN.9/1051](#), par. 67.

« Identité »

47. La définition de l'« identité » est au cœur de la notion de gestion de l'identité et renvoie à la capacité d'identifier de manière unique une personne physique ou morale dans un contexte particulier. Il s'agit donc d'une notion relative au contexte. Cette définition s'inspire de celle figurant dans la recommandation UIT-T X.1252, clause 6.40.

Références

[A/CN.9/WG.IV/WP.150](#), par. 31 ; [A/CN.9/1005](#), par. 108.

« Justificatifs d'identité »

48. Par « justificatifs d'identité », on entend les données ou l'objet matériel contenant ces données présentés aux fins du contrôle d'identité. Les justificatifs numériques peuvent être des noms d'utilisateur, des cartes à puce, des identifiants de téléphonie mobile et des certificats numériques, des passeports biométriques et des cartes d'identité électroniques. Les justificatifs d'identité sous forme électronique peuvent être utilisés en ligne ou hors ligne, en fonction des caractéristiques du système de gestion de l'identité. Le terme « justificatifs d'identité » est pratiquement synonyme du terme « moyen d'identification électronique » utilisé dans la législation régionale et nationale (par exemple, à l'article 3-2 du Règlement eIDAS).

Références

[A/CN.9/1005](#), par. 110 ; [A/CN.9/1045](#), par. 137.

« Services de gestion de l'identité »

49. La définition du terme « services de gestion de l'identité » traduit l'idée selon laquelle la gestion de l'identité comprend deux étapes (ou phases) : le « contrôle d'identité » et l'« identification électronique ». Elle fait référence aux services de gestion de l'identité qui interviennent dans l'une ou l'autre des étapes ou dans les deux, car le terme « ou » est utilisé de manière inclusive. L'article 6 a) relatif aux obligations fondamentales du prestataire de services de gestion de l'identité, décrit les différentes phases et étapes que comporte la fourniture de services de gestion de l'identité.

Références

[A/CN.9/1005](#), par. 84 et 109.

« Prestataire de services de gestion de l'identité »

50. Le prestataire de services de gestion de l'identité est la personne physique ou morale qui fournit des services de gestion de l'identité en exécutant, directement ou par l'intermédiaire de sous-traitants, les fonctions énumérées à l'article 6. Toutefois, ces fonctions ne sont peut-être pas toutes pertinentes pour l'ensemble des systèmes de gestion de l'identité et, par conséquent, un prestataire de services de gestion de l'identité n'exécute pas nécessairement chacune des fonctions énumérées.

Références

[A/CN.9/971](#), par. 97 ; [A/CN.9/1005](#), par. 111 ; [A/CN.9/1045](#), par. 88.

« Système de gestion de l'identité »

51. La définition du terme « système de gestion de l'identité » fait référence au système utilisé pour la gestion de l'identité en procédant au contrôle de l'identité et à l'identification électronique. Elle fait référence aux « fonctions et fonctionnalités », conformément à la terminologie de l'Union internationale des télécommunications (UIT), à savoir la recommandation UIT-T X.1252, clause 6.43. Contrairement à la définition du terme « services de gestion de l'identité », la définition du terme « système de gestion de l'identité » englobe nécessairement les deux étapes, même si différents prestataires de services interviennent dans chacune d'entre elles.

Références

[A/CN.9/1005](#), par. 112.

« Contrôle d'identité »

52. Le terme « contrôle d'identité » fait référence à la première étape de la gestion de l'identité et comprend l'inscription, qui est le processus utilisé par les prestataires de services de gestion de l'identité pour vérifier les déclarations d'identité d'un sujet avant de lui délivrer un justificatif. Il est utilisé à la place du terme « identification » pour répondre aux préoccupations concernant les multiples significations de ce dernier terme.

Références

[A/CN.9/1005](#), par. 84.

« Abonné »

53. Le terme « abonné » désigne la personne à laquelle les services sont fournis et n'inclut pas les parties utilisatrices. Il présuppose l'existence d'un contrat entre le prestataire de services et l'abonné. Par exemple, le signataire d'une signature électronique entre dans la définition du terme « abonné ».

Références

[A/CN.9/1005](#), par. 43 et 96 ; [A/CN.9/1045](#), par. 18 et 22.

« Service de confiance »

54. La définition du terme « service de confiance » comprend une description abstraite de l'objet des services de confiance, qui consiste essentiellement à garantir la qualité des données notamment leur véracité et authenticité, et une liste non exhaustive des services de confiance qui sont énumérés dans le [projet d'instrument]. La fourniture d'une liste non exhaustive permet d'appliquer les règles générales régissant les services de confiance aux futurs types de services de confiance.

55. La référence aux « méthodes de création et de gestion » permet de préciser que la notion de « service de confiance » renvoie aux services fournis et non au résultat découlant de leur utilisation. Le service de confiance n'est pas, par exemple, la signature électronique elle-même (à savoir les données identifiant le signataire et indiquant sa volonté concernant l'information contenue dans le message de données sous-jacent), mais plutôt le service qui prend en charge la signature électronique (à savoir le service offrant des méthodes permettant au signataire de créer la signature électronique et de garantir que celle-ci remplit les fonctions requises).

Références

[A/CN.9/965](#), par. 101 à 106 ; [A/CN.9/971](#), par. 110 et 111 ; [A/CN.9/1005](#), par. 14 à 18 ; [A/CN.9/1051](#), par. 35 à 40.

« Prestataire de services de confiance »

56. Le prestataire de services de confiance est une personne physique ou morale qui fournit des services de confiance. Un prestataire de services de certification au sens de la LTSE est par exemple un prestataire de services de confiance en matière de signatures électroniques. Contrairement aux prestataires de services de gestion de l'identité (art. 6), le [projet d'instrument] ne détermine pas les fonctions dont doivent s'acquitter les prestataires de services de confiance.

57. Le [projet d'instrument] n'exige pas le recours à un tiers prestataire de services de confiance comme condition de la reconnaissance juridique. Si l'on ne fait pas appel à un tiers prestataire de services de confiance, la même entité peut avoir les rôles de prestataire de services de confiance et d'abonné.

Références

[à compléter]

2. Article 2. Champ d'application

58. L'article 2 définit le champ d'application du [projet d'instrument] par référence à l'utilisation et à la reconnaissance internationale des systèmes de gestion de l'identité et des services de confiance dans le cadre d'activités commerciales et de services touchant au commerce. L'expression « services touchant au commerce » vise à englober les opérations qui sont étroitement liées au commerce mais qui ne sont pas de nature commerciale. Ces opérations peuvent faire intervenir des entités publiques comme les autorités douanières qui gèrent un guichet unique pour les formalités d'importation et d'exportation.

59. Étant donné que l'utilisation de la gestion de l'identité et de services de confiance a des incidences au-delà des opérations commerciales, les États adoptants peuvent étendre le champ d'application du [projet d'instrument] à tous les types d'opérations.

60. Conformément au principe général qui sous-tend les textes de la CNUDCI sur le commerce électronique et qui consiste à éviter toute modification du droit matériel existant ou à réduire au minimum les modifications devant y être apportées, le paragraphe 2 a) précise que le [projet d'instrument] n'introduit aucune nouvelle obligation en matière d'identification.

61. Le paragraphe 2 b) et c), qui indique que le [projet d'instrument] n'exige pas l'utilisation d'un service particulier de gestion de l'identité ou d'un service de confiance particulier, met en œuvre les principes de neutralité technologique, notamment en ce qui concerne la neutralité des modèles et des systèmes.

62. Le paragraphe 3 préserve les exigences légales qui imposent l'utilisation d'une certaine procédure d'identification ou l'utilisation d'un service de confiance particulier. Ces exigences généralement d'ordre réglementaire comprennent, par exemple, la demande de délivrance d'un document d'identité particulier (par exemple, un passeport) ou d'un document d'identité avec certaines caractéristiques correspondant à des attributs pertinents (par exemple, une carte d'identité avec photo et date de naissance du titulaire). Les exigences en matière d'identification peuvent également prévoir que l'identification soit effectuée par une certaine personne ayant des fonctions spécifiques. Lorsqu'une identification électronique est possible, les organismes de réglementation compétents exigent souvent l'utilisation d'une procédure de gestion de l'identité spécifique ou d'un service de confiance particulier, notamment l'utilisation de justificatifs d'identité délivrés par une autorité publique.

63. Compte tenu de sa nature habilitante, le [projet d'instrument], à l'instar des lois types existantes de la CNUDCI, est sans incidence sur l'application aux services de gestion de l'identité et aux services de confiance de toute autre loi susceptible de régir ces activités ou certains aspects essentiels des opérations effectuées à l'aide de ces services. Le paragraphe 4 précise ce principe en rapport avec la loi sur la confidentialité et la protection des données, qui est expressément mentionnée en raison de sa pertinence. La disposition ne fait pas référence à la confidentialité dans d'autres contextes.

Références

[A/74/17](#), par. 172 ; [A/CN.9/936](#), par. 52 ; [A/CN.9/965](#), par. 125 ; [A/CN.9/971](#), par. 23 ; [A/CN.9/1005](#), par. 115 ; [A/CN.9/1045](#), par. 76 à 78.

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

64. L'article 3 indique que le [projet d'instrument] n'impose pas l'utilisation de la gestion de l'identité ou de services de confiance à une personne qui n'a pas accepté d'utiliser la gestion de l'identité ou des services de confiance. Toutefois, le consentement peut être déduit du comportement d'une partie, par exemple lorsqu'elle opte pour l'utilisation d'un logiciel de commerce électronique particulier ou d'un système de communication électronique pris en charge par des services de gestion de l'identité et des services de confiance.

65. Le principe de l'utilisation volontaire de la gestion de l'identité et des services de confiance est lié au principe de l'autonomie des parties, car les deux principes se fondent sur la volonté. Le consentement à l'utilisation de services de gestion de l'identité et de services de confiance ne coïncide pas nécessairement avec le consentement donné au traitement des informations personnelles en vertu de la loi sur la confidentialité et la protection des données.

66. L'article 3, qui se fonde sur l'article 8-2 de la CCE, empêche l'imposition de toute nouvelle obligation d'utiliser des services de gestion de l'identité et des services

de confiance à l'abonné, au prestataire de services et à la partie utilisatrice, dans le respect de la règle générale tendant à éviter toute modification du droit matériel.

67. Une obligation d'utiliser les services de gestion de l'identité et les services de confiance peut exister dans une autre loi. Elle peut être imposée dans les opérations avec des entités publiques ou dans les opérations impliquant le respect d'obligations réglementaires.

Références

[A/CN.9/965](#), par. 22 et 110 ; [A/CN.9/1005](#), par. 116 ; [A/CN.9/1045](#), par. 79.

4. Article 4. Interprétation

68. L'article 4 s'inspire de dispositions figurant dans plusieurs traités et lois types existants de la CNUDCI, notamment ceux relatifs au commerce électronique (art. 3 de la LTCE ; art. 4 de la LTSE ; art. 5 de la CCE ; art. 3 de la Loi type sur les documents transférables électroniques).

69. Le paragraphe 1 vise à promouvoir une interprétation uniforme dans les États adoptants. Pour ce faire, il attire l'attention des juges et des autres organes juridictionnels sur le fait que les textes qui incorporent le [projet d'instrument] dans le droit interne doivent être interprétés en fonction de leur origine internationale et de la nécessité d'une application uniforme. Les juges sont donc encouragés à tenir compte des décisions rendues par des juridictions étrangères lorsqu'ils statuent sur des affaires, afin de contribuer à promouvoir une interprétation uniforme à l'échelle internationale.

70. Le paragraphe 2 vise à préserver l'interprétation et l'application uniformes des dispositions du [projet d'instrument] en prévoyant que les questions qui ne sont pas expressément tranchées par le [projet d'instrument] seront réglées selon les principes généraux dont il s'inspire, plutôt que par des principes établis par le droit interne.

71. Comme d'autres textes législatifs de la CNUDCI sur le commerce électronique, le [projet d'instrument] n'énonce pas explicitement les principes généraux sur lesquels il se fonde. Les principes de non-discrimination à l'égard de l'utilisation des moyens électroniques, de neutralité technologique, d'équivalence fonctionnelle et d'autonomie des parties sous-tendent généralement les textes législatifs de la CNUDCI sur le commerce électronique et ont été jugés pertinents également pour le [projet d'instrument], sous réserve d'ajustements. Par exemple, bien que l'autonomie des parties soit un principe fondamental du droit commercial, son application est soumise aux limites fixées par le droit impératif, y compris les dispositions du [projet d'instrument] auxquelles les parties ne peuvent déroger. En outre, comme indiqué ci-dessus (par. 20), le principe d'équivalence fonctionnelle ne s'applique peut-être pas lorsqu'un équivalent hors ligne n'existe pas.

Références

[A/CN.9/936](#), par. 67 et 72 ; [A/CN.9/1005](#), par. 117 et 118 ; [A/CN.9/1051](#), par. 53 à 56.

B. Chapitre II. Gestion de l'identité (art. 5 à 12)

1. Article 5. Reconnaissance juridique de la gestion de l'identité

72. L'article 5 accorde une reconnaissance juridique à la gestion de l'identité, en prévoyant que la forme électronique du contrôle d'identité et de l'identification électronique ne les prive pas, en soi, de leurs effets juridiques, de leur validité, de leur force exécutoire ou de caractère probant. Le paragraphe 1 applique donc le principe général de non-discrimination à l'égard de l'utilisation de moyens électroniques dans le domaine de la gestion de l'identité. Ce principe s'applique indépendamment de l'existence d'un équivalent hors ligne.

73. L'article 5 interdit toute discrimination à l'égard de l'identification électronique en tant que résultat du processus de gestion de l'identité. Son titre fait référence à la « reconnaissance juridique » et non à la « non-discrimination », afin de maintenir l'uniformité avec le titre des dispositions correspondantes dans les textes existants de la CNUDCI.

74. L'alinéa b) précise que le fait que le service de gestion de l'identité ne soit pas un service désigné n'empêche pas sa reconnaissance juridique. En d'autres termes, il accorde une reconnaissance juridique égale aux services de gestion de l'identité qui sont désignés et à ceux qui ne le sont pas, ce qui garantit la neutralité quant à l'approche choisie pour évaluer la fiabilité. Toutefois, il n'implique pas qu'un service de gestion de l'identité utilise des méthodes fiables et offre donc un niveau de garantie suffisant pour l'identification électronique : pour parvenir à ce résultat, la fiabilité de la méthode utilisée doit être évaluée conformément aux articles 10 et 11, selon le cas.

75. La référence à l'article 2-3 figurant dans le chapeau de l'article 5 souligne que l'article 5 ne porte pas atteinte à toute exigence légale selon laquelle une personne doit être identifiée conformément à une procédure définie ou prescrite par la loi. L'article 2-3 qualifie non seulement l'article 5 mais aussi toutes les autres dispositions du [projet d'instrument].

Références

[A/CN.9/965](#), par. 107 et 108 ; [A/CN.9/1005](#), par. 79 à 86 ; [A/CN.9/1045](#), par. 17 et 82 à 84.

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

76. L'article 6 énonce les obligations qui incombent aux prestataires de services de gestion de l'identité. Celles énumérées sont les principales obligations du prestataire de services de gestion de l'identité et peuvent être complétées par des obligations légales ou contractuelles supplémentaires. Le non-respect de ces obligations peut engager la responsabilité en vertu de l'article 12 et avoir un effet négatif sur la fiabilité du service de gestion de l'identité, notamment d'un service désigné.

77. En outre, l'article 6 vise à garantir que le prestataire de services de gestion de l'identité reste responsable pour l'intégralité des services de gestion de l'identité fournis à l'abonné, même si certaines fonctions sont exécutées par d'autres entités telles que des entrepreneurs ou des prestataires de services de gestion de l'identité autonomes dans le cadre de systèmes multipartites de gestion de l'identité du secteur privé. Cet article n'empêche pas le prestataire de services de gestion de l'identité d'externaliser des fonctions, ni de répartir les risques entre ses sous-traitants ou d'autres partenaires commerciaux.

78. Les systèmes de gestion de l'identité peuvent varier de manière non négligeable quant à leur objet et leur conception, ainsi qu'à leurs services fournis. La conception du système de gestion de l'identité peut également être fonction du modèle choisi. Toutes les obligations énumérées à l'article 6 n'incombent pas nécessairement à tous les prestataires de services de gestion de l'identité : c'est plutôt la conception du système de gestion de l'identité et le type de services fournis qui détermineront quelles obligations incombent à un prestataire de services de gestion de l'identité donné. Cette souplesse dans la conception de l'approche des systèmes de gestion de l'identité se reflète dans les mots « adaptées à l'objet et à la conception ».

79. Les obligations sont décrites de manière technologiquement neutre, car l'application du principe de neutralité technologique dans le contexte de la gestion de l'identité exige que la configuration minimale requise fasse référence aux propriétés du système, et non à des technologies spécifiques.

80. Dans la pratique, les fonctions énumérées à l'article 6 sont habituellement régies par des règles de fonctionnement contractuelles, en particulier lorsque des prestataires de services de gestion de l'identité du secteur privé interviennent. Ces règles, qui

fournissent des orientations sur la manière dont les opérations doivent être menées, se fondent sur des politiques, sont mises en œuvre par des pratiques et se traduisent dans des accords contractuels. L'obligation de « avoir en place des règles, politiques et pratiques de fonctionnement » traduit cette pratique commerciale. En raison de leur importance juridique et pratique, l'alinéa d) exige que les règles, politiques et pratiques de fonctionnement soient facilement accessibles aux abonnés et aux tiers.

81. Le principe selon lequel le prestataire de services de certification doit être lié par ses déclarations et ses engagements est énoncé à l'article 9 a) de la LTSE, qui prévoit que ledit prestataire est tenu d'agir en conformité avec les déclarations qu'il fait concernant ses politiques et pratiques.

Références

[A/CN.9/936](#), par. 69 ; [A/CN.9/1045](#), par. 85 à 95.

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

82. L'article 7 définit les principales obligations qui incombent aux prestataires de services de gestion de l'identité en cas de violation des données ayant une incidence importante sur un système de gestion de l'identité. Les obligations prévues à l'article 7 s'appliquent indépendamment de l'objet et de la conception du système de gestion de l'identité et ne peuvent être modifiées par contrat, y compris dans les règles de fonctionnement. Les atteintes à la sécurité peuvent toucher à la fois les systèmes et les services de gestion de l'identité et également avoir des incidences sur les attributs gérés dans le système de gestion de l'identité.

83. La notion de « violation des données » correspond à une atteinte à la sécurité entraînant la destruction, la perte, la modification ou la divulgation non autorisée, que ce soit de manière accidentelle ou illégale, de données transmises, stockées ou traitées d'une autre manière, ou encore l'accès non autorisé à ces données. Elle peut être définie dans la loi sur la confidentialité et la protection des données.

84. La notion d'« incidence importante » est utilisée dans les lois régionales⁶ et nationales. Plusieurs facteurs peuvent contribuer à l'évaluation de cette incidence. Des formulaires de notification aident à évaluer l'incidence en précisant la durée de l'atteinte, le type de données et le pourcentage d'abonnés concernés, ainsi que d'autres informations pertinentes. Des orientations techniques pour le signalement des incidents, ainsi que des rapports annuels sur les incidents de sécurité, sont également disponibles.

85. Estimant que des mesures autres que la suspension totale pourraient être appropriées, l'article 7 exige que le prestataire de services de gestion de l'identité prenne « toutes les mesures raisonnables » pour répondre à une atteinte à la sécurité et limiter ses effets.

86. Le paragraphe 1 c) établit l'obligation de notifier les atteintes à la sécurité, qui constitue un aspect du principe de transparence. Un mécanisme approprié de notification de ces atteintes est important pour améliorer la qualité de fonctionnement des systèmes et augmenter le niveau de confiance dans les services de gestion de l'identité et les services de confiance.

87. Certains aspects des obligations énoncées à l'article 7, tels que l'identification des parties qui doivent être avisées en cas d'atteinte, le moment et le contenu de la notification, et la divulgation d'une atteinte et de ses détails techniques, peuvent être spécifiés dans la législation nationale, dans les accords contractuels et dans les règles,

⁶ Art. 19-2 du 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 (« Règlement eIDAS »).

politiques et pratiques de fonctionnement du prestataire de services de gestion de l'identité.

88. Les obligations visées à l'article 7 peuvent coïncider avec les obligations prévues par la loi sur la confidentialité et la protection des données. Le cas échéant, toutes les actions énoncées, et pas seulement la notification, doivent être exécutées conformément à la loi applicable en matière de confidentialité et de protection des données.

89. L'article 7 s'applique conjointement avec la loi sur la confidentialité et la protection des données ainsi qu'avec toute autre loi applicable à l'activité concernée. Il existe notamment des éléments communs, mais également de grandes différences, entre les notifications relatives aux violations des données et celles relatives aux atteintes à la sécurité.

Références

[A/CN.9/971](#), par. 84 à 87 ; [A/CN.9/1005](#), par. 32 à 36 et 94 ; [A/CN.9/1045](#), par. 96 à 101.

4. Article 8. Obligations incombant aux abonnés

90. L'article 8 énonce les obligations qui incombent aux abonnés en matière de notification des atteintes, ou de tout risque connexe, visant les justificatifs d'identité. Ces obligations complètent celles qui incombent au prestataire de services de gestion de l'identité selon lesquelles ce dernier doit fournir un moyen permettant de notifier les atteintes à la sécurité [art. 6 e)] et de réagir en cas d'atteinte à la sécurité ou de perte d'intégrité (art. 7).

91. L'obligation qui incombe à l'abonné en cas de violation des données s'applique lorsque les justificatifs d'identité ont été compromis ou qu'il est fortement possible qu'ils aient été compromis. Celle-ci est différente des obligations qui incombent au prestataire de services de la gestion de l'identité en cas de violation des données, à savoir une atteinte à la sécurité ou la perte d'intégrité ayant une incidence importante sur un système de gestion de l'identité.

92. La référence à la possibilité que les justificatifs d'identité aient pu être compromis vise à garantir qu'aucune attente déraisonnable en ce qui concerne les connaissances techniques ne soit imposée aux abonnés. L'obligation de notification s'impose uniquement dans des circonstances connues de l'utilisateur qui font naître un doute justifié quant au bon fonctionnement des justificatifs d'identité.

93. Le contrat entre l'abonné et le prestataire de services de gestion de l'identité peut énoncer des obligations supplémentaires pour l'abonné. Ce contrat peut également contenir des informations supplémentaires sur la manière dont l'obligation de notification prévue à l'article 8 peut être respectée.

94. L'expression « en utilisant d'une autre manière des moyens raisonnables » indique que l'abonné n'est pas tenu d'utiliser les voies de communication fournies par le prestataire de services de gestion de l'identité.

95. La notion de « justificatifs d'identité compromis » se réfère aux cas d'accès non autorisé aux justificatifs d'identité.

96. Le paragraphe b) vise à traiter les cas où l'abonné n'a pas effectivement connaissance que ses données ont été compromises mais qu'il a des raisons de croire que cela a pu se produire. Il s'inspire de l'article 8-1 b) ii) de la LTSE, qui contient des obligations similaires pour le signataire.

Références

[A/CN.9/936](#), par. 68 ; [A/CN.9/971](#), par. 88 à 96 ; [A/CN.9/1005](#), par. 37 à 43, 95 et 96 ; [A/CN.9/1045](#), par. 102 à 105.

5. Article 9. Identification d'une personne au moyen de la gestion de l'identité

97. Dans les textes de la CNUDCI sur le commerce électronique, les règles d'équivalence fonctionnelle définissent les conditions que doit remplir un document, une méthode ou un processus électronique pour satisfaire à une exigence légale dans l'environnement papier. L'article 9 prévoit une règle d'équivalence fonctionnelle pour les cas où la loi exige l'identification, ou lorsque les parties conviennent de s'identifier mutuellement. L'objectif de cette disposition étant d'établir les conditions d'équivalence entre l'identification hors ligne et l'identification en ligne, l'article 9 ne s'applique que si un équivalent de l'identification hors ligne existe. Il constitue néanmoins une disposition essentielle pour mettre en place un régime juridique régissant la gestion de l'identité.

98. Conformément aux principes établis dans les textes de la CNUDCI, cette règle d'équivalence fonctionnelle complète la règle de reconnaissance juridique énoncée à l'article 5. Toutefois, si l'article 5 s'applique à toutes les formes d'identification électronique, indépendamment de l'existence d'un équivalent de l'identification hors ligne, l'article 9 vise à établir l'identification électronique en tant qu'équivalent fonctionnel de l'identification hors ligne et ne peut donc fonctionner que par référence à un équivalent papier.

99. L'article fait référence à l'utilisation de services de gestion de l'identité pour indiquer que les exigences en matière d'équivalence sont satisfaites lorsque des justificatifs d'identité sont utilisés, et non des systèmes de gestion de l'identité ou l'identité elle-même.

100. L'article 9 n'a pas d'incidence sur les exigences d'identification selon une procédure ou méthode particulière, comme le prévoit l'article 2-3. Ces exigences peuvent être liées au respect des règles en vigueur, notamment celles applicables dans les domaines bancaire et de la lutte contre le blanchiment d'argent (voir par. 62 ci-dessus).

101. L'identification électronique peut être utilisée pour satisfaire à l'obligation de vérifier certains attributs de l'identité d'une personne, par exemple l'âge ou le lieu de résidence, comme l'exige l'identification fondée sur des documents physiques. À cet égard, étant donné que la notion d'« identité » est définie par rapport au « contexte », qui détermine à son tour les attributs requis pour l'identification, l'identification effective d'une personne sur la base de l'article 9 comprend la vérification des attributs requis. Les mots « à cette fin » traduisent également la nécessité de vérifier les attributs pertinents. Les dispositions énoncées à l'article 10 relatives à la fiabilité n'exigent pas la vérification d'attributs particuliers, car elles portent sur les processus de gestion des justificatifs d'identité plutôt que les attributs contenus dans ces justificatifs.

102. Les articles 9 et 16 à 21 du [projet d'instrument] font référence aux cas de figure dans lesquels la loi exige ou prévoit des conséquences lorsqu'une action n'a pas été exécutée. Cette formulation, qui est reprise de l'article 9 de la CCE, a été utilisée afin de tenir compte des règles d'équivalence fonctionnelle lorsque la loi n'exige pas, mais prévoit des conséquences juridiques pour certaines actions, et couvre également les cas où la loi autorise certaines actions (voir art. 9 de la Loi type de la CNUDCI sur les documents transférables électroniques).

Références

[A/CN.9/965](#), par. 62 à 85 ; [A/CN.9/971](#), par. 24 à 49 ; [A/CN.9/1005](#), par. 97 à 100 ; [A/CN.9/1045](#), par. 106 à 117 ; [A/CN.9/1051](#), par. 42 à 44.

6. Article 10. Critères de fiabilité pour les services de gestion de l'identité

103. L'article 10 donne des orientations sur la manière de déterminer la fiabilité de la méthode utilisée pour l'identification à l'article 9 après que la méthode a été utilisée (approche *ex post*).

104. Le paragraphe 1 a) met en œuvre l'approche *ex post* en indiquant que la méthode doit être « [s]uffisamment fiable au regard de l'objet pour lequel le service de gestion de l'identité est utilisé ». Cette disposition traduit l'idée que la fiabilité est une notion relative. Toutefois, contrairement à certains services de confiance qui peuvent remplir plusieurs fonctions, l'identification électronique ne remplit qu'une seule fonction, à savoir l'identification fiable par des moyens électroniques. Cette fonction peut être utilisée à différentes fins, chacune étant associée à un niveau de fiabilité différent.

105. Le paragraphe 1 b) contient une clause visant à empêcher la répudiation du service de gestion de l'identité lorsque celui-ci a effectivement rempli sa fonction. La répudiation se produit lorsqu'un sujet déclare ne pas avoir effectué une action. Pour que le mécanisme prévu au paragraphe 1 b) fonctionne, il faut que la méthode, qu'elle soit fiable ou non, ait effectivement rempli la fonction d'identification, c'est-à-dire qu'elle ait associé la personne qui cherche à s'identifier aux justificatifs d'identité. Cette disposition s'inspire de l'article 9-3 b) ii) de la CCE.

106. Le paragraphe 2 contient une liste de circonstances, décrites en termes technologiquement neutres, susceptibles d'être pertinentes pour aider le juge à déterminer la fiabilité. Cette liste étant indicative et non exhaustive, d'autres circonstances peuvent également être pertinentes. En outre, toutes les circonstances énumérées ne sont pas nécessairement pertinentes dans tous les cas où la fiabilité doit être déterminée. En particulier, la pertinence de l'accord entre les parties peut fortement varier en fonction de la question de savoir si la juridiction concernée reconnaît ou pas l'autonomie des parties dans le domaine de l'identification. De plus, les accords contractuels étant parfois sans incidence sur les tiers, cette circonstance ne serait donc pas pertinente dans les cas faisant intervenir des tiers.

107. Le paragraphe 3 précise que le lieu où le service de gestion de l'identité est fourni et le lieu où se trouve l'établissement du prestataire de services de gestion de l'identité ne sont pas pertinents en soi pour la détermination de la fiabilité. Cette disposition vise à faciliter la reconnaissance internationale des services de gestion de l'identité et s'inspire de l'article 12-1 de la LTSE, qui établit une règle générale de non-discrimination pour la détermination de l'efficacité juridique d'un certificat ou d'une signature électronique. Pour en savoir plus sur l'interaction entre les articles 12-1 et 12-2 de la LTSE, voir [A/CN.9/483](#), par. 28 à 36.

108. Selon le paragraphe 4, la désignation d'un service de gestion de l'identité fiable conformément à l'article 11 offre une présomption de fiabilité aux méthodes utilisées par le service désigné. C'est la seule distinction entre les services de gestion de l'identité désignés et ceux non désignés. En outre, selon le paragraphe 5 b), la présomption de fiabilité liée à la désignation peut être réfutée.

109. Le paragraphe 5 clarifie la relation entre les articles 10 et 11 en précisant que l'existence d'un mécanisme de désignation n'exclut pas la détermination *ex post* de la fiabilité de la méthode. Cette disposition s'inspire de l'article 6-4 de la LTSE.

a) Cadre relatif aux niveaux de garantie

110. Les articles 10 et 11 font référence à la notion de « niveau de garantie » ou à des cadres similaires désignés par d'autres termes. Le niveau de garantie donne des indications aux parties utilisatrices sur le degré de confiance qu'elles peuvent accorder aux processus de contrôle de l'identité et d'identification électronique et les aide à déterminer s'ils sont adéquats à des fins spécifiques. Le [projet d'instrument] ne définit pas de niveaux de garantie ni n'exige la définition ou l'utilisation de tels niveaux.

111. Les cadres relatifs aux niveaux de garantie prévoient différents niveaux de garantie qui sont associés à un certain nombre d'exigences. En d'autres termes, ils décrivent les exigences auxquelles les systèmes et services de gestion de l'identité doivent répondre pour offrir un certain niveau de garantie en ce qui concerne leur fiabilité. Les niveaux de garantie doivent être décrits en termes génériques afin de préserver la neutralité technologique.

112. L'exigence d'assurer un certain niveau de garantie quant à la fiabilité des identités utilisées peut être définie par référence aux niveaux décrits dans un cadre relatif aux niveaux de garantie. Certains systèmes et services de gestion de l'identité peuvent ainsi être classés au regard des exigences concernant le niveau de garantie requis. Le respect, par un service de gestion de l'identité, des exigences associées au niveau de garantie requis permet d'utiliser ce service pour une opération particulière.

b) Certification et supervision

113. L'article 10 mentionne, parmi les circonstances possiblement pertinentes, « [t]oute supervision ou toute certification fournie concernant le système de gestion de l'identité ». La certification et la supervision peuvent jouer un rôle important pour instaurer la confiance dans les prestataires de services de gestion de l'identité et leurs services, notamment en déterminant la fiabilité de la méthode utilisée, car ils sont associés à un certain niveau d'objectivité dans l'évaluation de la fiabilité de la méthode utilisée. Cette exigence figure déjà à l'article 12 a) vi) de la Loi type de la CNUDCI sur les documents transférables électroniques et à l'article 10 f) de la LTSE.

114. Les options de certification sont notamment les suivantes : l'autocertification, la certification par un tiers indépendant ; la certification par un tiers indépendant accrédité ; et la certification par un organisme public. Le type de service en jeu, le coût et le niveau de garantie requis ont des incidences sur le choix de la forme de certification la plus appropriée. Dans le contexte interentreprises, 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 différents.

115. L'existence d'un mécanisme de supervision des systèmes et services de gestion de l'identité est parfois considérée comme utile, voire nécessaire, pour instaurer la confiance dans la gestion de l'identité. Toutefois, la mise en place d'un organe de supervision a des répercussions administratives et financières susceptibles d'être coûteuses. Le [projet d'instrument] n'impose ni ne facilite la mise en place d'un régime de supervision.

116. Différentes approches existent en ce qui concerne la participation des pouvoirs publics à la certification et à la supervision, qui est une décision politique appartenant à l'État adoptant. L'approche adoptée dans le [projet d'instrument] est fondée sur la neutralité du modèle et les références à la certification et à la supervision n'excluent pas les régimes d'autocertification. Lorsque les entités publiques sont à la fois organismes de certification et de supervision et prestataires de services de gestion de l'identité, les fonctions de certification et de supervision peuvent être séparées de la fourniture de services de gestion de l'identité.

117. Dans certains cas, par exemple lorsque certaines technologies de registres distribués sont utilisées, une solution présupposant l'intervention d'un organisme central de certification, d'accréditation ou de supervision pourrait ne pas convenir en raison des difficultés à identifier l'organisme qualifié pour demander la certification, l'organisme devant être évalué et celui chargé de prendre des mesures correctives et coercitives, entre autres.

Références

[A/CN.9/965](#), par. 40 à 55 et 112 à 115 ; [A/CN.9/971](#), par. 50 à 61 ; [A/CN.9/1005](#), par. 101 ; [A/CN.9/1045](#), par. 118 à 124 ; [A/CN.9/1051](#), par. 47 à 49 ; [A/CN.9/WG.IV/WP.153](#), par. 74 et 75.

7. Article 11. Désignation des systèmes [et services] de gestion de l'identité fiables

118. L'article 11 complète l'article 10 en offrant la possibilité de désigner des systèmes [et services] de gestion de l'identité. Plus précisément, il énumère les conditions qu'un système [ou service] de gestion de l'identité doit remplir pour figurer sur la liste de systèmes [et services] de gestion de l'identité désignés.

119. La désignation des systèmes [et services] de gestion de l'identité utilisant des méthodes fiables tient compte de toutes les circonstances pertinentes, y compris celles énumérées à l'article 10 utilisées pour déterminer la fiabilité de la méthode. La référence aux circonstances énumérées à l'article 10 assure un certain degré de cohérence entre les méthodes considérées comme fiables *ex ante* et celles jugées fiables *ex post*. En outre, la désignation doit « être conforme aux normes et procédures internationalement reconnues qui sont pertinentes pour l'exécution du processus de désignation » afin de promouvoir la reconnaissance juridique et l'interopérabilité internationales.

120. La diffusion d'informations sur les systèmes [et services] de gestion de l'identité désignés est essentielle pour les faire connaître aux abonnés potentiels. L'entité de désignation est tenue de publier une liste des systèmes [et services] de gestion de l'identité désignés, notamment les coordonnées des prestataires de services de gestion de l'identité, par exemple sur son site Web, ou d'informer autrement le public de la désignation. Les listes jouent un rôle important pour assurer la transparence du processus de désignation des services de gestion de l'identité, y compris dans le contexte international, et leur pertinence est également reconnue dans les normes techniques fréquemment utilisées.

121. Le paragraphe 2 a) fait référence aux normes et procédures pertinentes pour déterminer la fiabilité et vise à assurer une certaine uniformité en ce qui concerne les résultats des évaluations *ex ante* et *ex post* de la fiabilité. Le paragraphe 3 quant à lui fait explicitement référence aux normes et procédures pertinentes pour la désignation, telles que les évaluations de conformité et les audits, qui sont spécifiques à l'approche *ex ante*.

122. Comme l'article 10-3, le paragraphe 4 précise que le lieu où le système [ou service] de gestion de l'identité est fourni et le lieu où se trouve l'établissement du prestataire de services de gestion de l'identité ne sont pas pertinents en soi pour la désignation d'un service fiable. Il s'inspire donc de l'article 12-1 de la LTSE, qui établit une règle générale de non-discrimination pour la détermination de l'efficacité juridique d'un certificat ou d'une signature électronique. En pratique, cette disposition permet à un prestataire de services de gestion de l'identité étranger de demander à l'autorité compétente de l'État adoptant de désigner le système [ou service] de gestion de l'identité, comme l'indique également l'article 25-3.

Références

[A/CN.9/965](#), par. 40 à 55 ; [A/CN.9/971](#), par. 68 à 76 ; [A/CN.9/1005](#), par. 102 et 105 ; [A/CN.9/1045](#), par. 125 à 129.

8. Article 12. Responsabilité des prestataires de services de gestion de l'identité

123. Le régime de responsabilité peut avoir une incidence importante sur la promotion de l'utilisation de systèmes de gestion de l'identité et de services de confiance et est un élément central du [projet d'instrument]. L'article 12 établit un régime de responsabilité unique des prestataires de services de gestion de l'identité à l'égard des abonnés, selon lequel un prestataire de services de gestion de l'identité doit être tenu responsable des conséquences de tout manquement à l'obligation de fournir les services requis par la loi et convenus par contrat.

124. L'article 12 repose sur trois éléments : a) il est sans incidence sur le droit impératif, notamment les obligations impératives qui incombent au prestataire de services de gestion de l'identité en vertu du [projet d'instrument] ; b) il établit la responsabilité du prestataire de services de gestion de l'identité en cas de manquement à ses obligations impératives, que ces obligations soient ou non de nature contractuelle ; et c) il reconnaît qu'il est possible de limiter la responsabilité dans certaines conditions.

125. La nature de la responsabilité qui découle de l'article 12 est statutaire et, en tant que telle, distincte de la responsabilité qui découle du droit des contrats. L'objectif

visé est de reconnaître que le prestataire de services peut être responsable en cas de manquement aux obligations lui incombant en vertu du [projet d'instrument], indépendamment du fait que ces obligations aient également ou non une base contractuelle. Cette disposition s'applique indépendamment de la nature publique ou privée du prestataire de services de gestion de l'identité.

126. La responsabilité des prestataires de services de gestion de l'identité peut découler de l'utilisation de services de gestion de l'identité désignés et non désignés. Toutefois, elle n'est pas absolue. Par exemple, un prestataire de services de gestion de l'identité peut ne pas être responsable vis-à-vis d'un abonné si la perte a été causée par l'utilisation d'un justificatif compromis alors que ce dernier le savait, ou aurait dû le savoir.

127. Les questions relatives à la responsabilité qui ne sont pas traitées à l'article 12 relèvent de la loi applicable en dehors du projet de dispositions. Ces questions comprennent le degré de vigilance et de faute, la charge de la preuve, la détermination du montant des dommages et de l'indemnisation, etc.

128. L'article 12 permet de limiter la responsabilité dans certaines conditions, à savoir lorsqu'une limite est imposée à l'objet ou à la valeur des opérations pour lesquelles le service de gestion de l'identité pouvait être utilisé, et que l'abonné a été informé de cette limite.

129. Il peut être nécessaire de limiter la responsabilité pour contenir le coût de l'assurance, entre autres. Ces limites sont fixées dans le contrat entre le prestataire de services et l'abonné. Dans la pratique, elles figurent généralement dans les règles, politiques et pratiques de fonctionnement du prestataire de services.

130. La mesure dans laquelle un prestataire de services de gestion de l'identité peut limiter sa responsabilité est déterminée par la loi applicable. Le [projet d'instrument] est sans incidence sur l'application de toute loi qui restreint le droit d'un prestataire de services de limiter sa responsabilité ou de fixer les conditions de cette limite.

131. Le paragraphe 3 b) ne vise pas à introduire une nouvelle obligation d'information, mais indique que la disposition ne l'emporte pas sur des exigences plus strictes en matière d'information prévues par la loi applicable. Cette dernière établira toute obligation d'information applicable, telle que la notification ou l'approbation expresse.

132. L'article 12 ne traite que de la responsabilité des prestataires de services de gestion de l'identité vis-à-vis des abonnés. Un tiers subissant une perte résultant de l'utilisation de services de gestion de l'identité peut demander réparation au prestataire de services ou à l'abonné en vertu des règles existantes en matière de responsabilité. Dans ce dernier cas, l'abonné pourrait alors se retourner contre le prestataire de services de gestion de l'identité.

133. L'article 12 n'empêche pas le prestataire de services de limiter sa responsabilité vis-à-vis des tiers en vertu d'une autre loi. L'article 6 d) exige que les règles, politiques et pratiques de fonctionnement du prestataire de services soient facilement accessibles également aux tiers. Toutefois, le [projet d'instrument] n'exige pas spécifiquement que le prestataire de services informe les tiers qui se fient à lui d'éventuelles limites de responsabilité, car l'identification préalable de ces tiers peut être difficile.

134. L'article 12 s'applique aux prestataires de services de gestion de l'identité, indépendamment de leur nature publique ou privée. Un État adoptant devra peut-être adapter cette disposition à toute règle spéciale sur la responsabilité des entités publiques. L'article 12 ne s'applique pas aux entités publiques exerçant des fonctions de supervision et gérant les registres et statistiques de l'état civil qui peuvent fournir des justificatifs d'identité fondamentale.

Références

[A/CN.9/936](#), par. 83 à 86 ; [A/CN.9/965](#), par. 116 à 118 ; [A/CN.9/971](#), par. 98 à 107 ; [A/CN.9/1005](#), par. 76 ; [A/CN.9/1045](#), par. 130 à 131 ; [A/CN.9/1051](#), par. 13 à 29.

C. Chapitre III. Services de confiance (art. 13 à 24)**1. Article 13. Reconnaissance juridique des services de confiance**

135. L'article 13 établit une règle générale de non-discrimination à l'égard du résultat découlant de l'utilisation d'un service de confiance, en énumérant certaines qualités d'un message de données. La référence au résultat découlant de l'utilisation d'un service de confiance est conforme à l'approche adoptée à l'article 5, qui accorde une reconnaissance juridique à l'identification électronique en tant que résultat de l'utilisation de la gestion de l'identité.

136. L'article 13 s'applique aux services de confiance, qu'ils aient été mentionnés ou non dans le [projet d'instrument], et fonctionne indépendamment de l'existence d'une règle d'équivalence fonctionnelle.

Références

[A/CN.9/971](#), par. 112 à 115 ; [A/CN.9/1005](#), par. 19 à 26 ; [A/CN.9/1045](#), par. 16 et 17.

2. Article 14. Obligations incombant aux prestataires de services de confiance

137. L'article 14 établit les principales obligations qui incombent aux prestataires de services de confiance, que le service de confiance ait été mentionné ou non. Des accords contractuels peuvent préciser et compléter ces obligations, mais pas s'en écarter. Cette approche est similaire à celle adoptée aux articles 6 et 7 sur les obligations des prestataires de services de gestion de l'identité.

138. La référence aux règles, politiques et pratiques de fonctionnement « au regard de l'objet et à la conception du service de confiance » vise à reconnaître que les obligations incombant aux prestataires de services de confiance varient en fonction de la conception et de la fonction de chaque service de confiance.

139. L'obligation de mettre à la disposition des tiers les politiques et les pratiques est conforme à la pratique existante, qui reconnaît que ces informations sont importantes pour les parties utilisatrices lorsqu'elles décident d'accepter ou non le résultat de l'utilisation dudit service, conformément au principe de l'utilisation volontaire des services de confiance (art. 2-2 c) et art. 3-1).

140. Les limites fixées en ce qui concerne l'objet ou la valeur de l'opération pour laquelle le service de confiance peut être utilisé sont généralement énoncées dans les règles de fonctionnement régissant le service de confiance, qui comprennent également les politiques et les pratiques du prestataire de services de confiance. Le paragraphe 1 c) vise donc également à satisfaire à l'obligation de transparence vis-à-vis des tiers en ce qui concerne les limitations contractuelles applicables. Une disposition analogue figure à l'article 9-1 d) ii) de la LTSE.

Références

[A/CN.9/971](#), par. 152 et 153 ; [A/CN.9/1005](#), par. 28 à 36 et 73 ; [A/CN.9/1045](#), par. 18 à 21 et 57.

3. Article 15. Obligations incombant aux abonnés

141. L'article 15 énonce les obligations qui incombent aux abonnés lorsque le service de confiance est compromis. Le [projet d'instrument] ne prévoit pas d'obligations supplémentaires pour les abonnés en ce qui concerne l'utilisation du service de confiance. Des exemples de ces obligations figurent à l'article 8-1 a) et c) de la LTSE.

142. L'article 15 énonce les obligations qui incombent aux abonnés lorsque des services de confiance sont compromis, tandis que l'article 14-2 énonce les obligations qui incombent aux prestataires de services de confiance en cas de violation des données. La notion de « service de confiance compromis » fait référence à des cas d'accès non autorisé à des services de confiance. Ainsi, l'article 15 présuppose qu'un événement qui affecte la fiabilité du service de confiance est survenu tandis que l'article 14 présuppose qu'une atteinte à la sécurité ou une perte d'intégrité a une incidence importante sur le service de confiance.

143. Le contrat conclu entre le prestataire de services de confiance et l'abonné fournit généralement des informations détaillées sur les mesures à prendre pour respecter les obligations énoncées à l'article 15. Ces accords contractuels font généralement référence aux politiques et pratiques du prestataire de services de confiance.

144. Le [projet d'instrument] ne contient pas de règles de responsabilité pour les abonnés. Par conséquent, les dispositions contractuelles, qui peuvent prévoir des obligations supplémentaires pour les abonnés, et les règles de responsabilité générales détermineront la responsabilité de l'abonné.

145. Contrairement à certaines dispositions des textes existants de la CNUDCI (voir art. 11 de la LTSE), l'article 15 n'établit pas d'obligations pour les tiers, dont la responsabilité peut être engagée en vertu d'une autre loi.

Références

[A/CN.9/1005](#), par. 37 à 43 ; [A/CN.9/1045](#), par. 22 à 26.

4. Article 16. Signatures électroniques

146. L'article 16 porte sur les signatures électroniques. Tous les textes législatifs de la CNUDCI sur le commerce électronique contiennent des dispositions sur l'utilisation des signatures électroniques, qui peuvent être apposées tant par des personnes physiques que par des personnes morales. Le texte de l'article 16 s'inspire de celui de l'article 9 de la Loi type de la CNUDCI sur les documents transférables électroniques, qui, à son tour, se fonde sur l'article 9-3 de la CCE.

147. L'exigence d'une signature papier est satisfaite si une méthode est utilisée pour identifier le signataire du message de données et indiquer son intention concernant le message de données signé. La référence à l'utilisation de la méthode « concernant l'information contenue dans le message de données » s'applique tant à l'identification de la personne qu'à l'indication de son intention.

148. Les signatures électroniques peuvent être utilisées à diverses fins, notamment pour identifier l'auteur d'un message et l'associer à son contenu. Il existe plusieurs technologies et méthodes susceptibles de satisfaire aux exigences d'une signature électronique. Dans un contexte commercial, les parties peuvent identifier la technologie et la méthode de signature électronique les plus appropriées en tenant compte des coûts, du niveau de sécurité recherché, de la répartition des risques et d'autres considérations. Les textes existants de la CNUDCI ont examiné en détail les objectifs et les méthodes des signatures électroniques (Guide pour l'incorporation de la LTSE, par. 29 à 62 ; promouvoir la confiance, par. 24 à 66).

Références

[A/CN.9/971](#), par. 116 à 119 ; [A/CN.9/1005](#), par. 44 à 51 ; [A/CN.9/1045](#), par. 34 ; [A/CN.9/1051](#), par. 50.

5. Article 17. Cachets électroniques

149. Les cachets électroniques permettent de garantir l'origine et l'intégrité d'un message de données provenant d'une personne morale. En pratique, ils associent la fonction de signature électronique générique en ce qui concerne l'origine, et celle de certains types de signature, typiquement basés sur l'utilisation de clés

cryptographiques, en ce qui concerne l'intégrité. Ces signatures électroniques sont prévues à l'article 6-3 d) de la LTSE. Par conséquent, la description de l'exigence d'intégrité énoncée à l'article 17 se fonde sur l'article 6-3 d) de la LTSE.

150. L'article 17 s'inspire de la législation régionale, selon laquelle « [o]utre le document délivré par une personne morale, les cachets électroniques peuvent servir à authentifier tout bien numérique de ladite personne, tel un code logiciel ou des serveurs » (Règlement eIDAS, considérant 65).

151. La garantie quant à l'origine du message de données peut être obtenue en établissant sa provenance, ce qui, à son tour, exige d'identifier la personne morale à l'origine du message de données. La méthode utilisée pour identifier la personne morale qui appose le cachet est la même que celle utilisée pour identifier un signataire, et les dispositions de la CNUDCI sur les signatures électroniques ont été généralement adoptées et s'appliquent aux personnes physiques et morales.

152. En outre, selon les dispositions figurant dans les textes de la CNUDCI, l'intégrité est nécessaire à l'établissement de l'équivalence fonctionnelle avec la notion d'« original » dans l'environnement papier. En particulier, l'article 6-3 d) de la LTSE fait référence à la notion d'« intégrité » dans le cas où l'exigence légale de signature a pour but de garantir l'intégrité de l'information à laquelle elle se rapporte.

153. Au vu de ce qui précède, les pays ayant déjà adopté des dispositions de la CNUDCI sur les signatures électroniques garantissant l'intégrité ne font pas nécessairement de distinction entre les fonctions pour lesquelles une signature électronique est utilisée et celles pour lesquelles un cachet électronique est utilisé. Cela est également lié à une pratique commerciale consistant à utiliser des méthodes hybrides combinant signatures et cachets électroniques.

Intégrité

154. L'intégrité est un élément essentiel des cachets électroniques et de l'archivage électronique, et peut être un élément facultatif pour d'autres services de confiance. Dans les textes existants de la CNUDCI, l'intégrité est exigée pour assurer l'équivalence fonctionnelle avec la notion d'« original » dans l'environnement papier (art. 8 de la LTCE). Les articles 17 et 19 s'inspirent de l'article 8-3 de la LTCE en ce qui concerne les exigences visant à garantir l'intégrité.

Références

[A/CN.9/971](#), par. 124 à 128 ; [A/CN.9/1005](#), par. 52 à 54 et 58 ; [A/CN.9/1045](#), par. 35, 36 et 56 à 58.

6. Article 18. Horodatages électroniques

155. Les horodatages électroniques fournissent la preuve de la date et de l'heure auxquelles le cachet a été apposé aux données. En général, la loi prévoit des conséquences dans le cas où la date et l'heure d'un événement particulier ne peuvent être prouvées avec un niveau de confiance suffisant. Par exemple, il est parfois nécessaire de prouver la date de conclusion d'un contrat à des fins d'opposabilité.

156. Les horodatages sont généralement apposés lorsque certaines actions sont exécutées, par exemple la génération d'un document électronique dans sa forme définitive, la signature, l'envoi et la réception d'une communication électronique, etc. L'exigence de préciser un fuseau horaire peut, mais ne doit pas nécessairement, être satisfaite par référence au temps universel coordonné (UTC).

157. L'article 18 mentionne non seulement les « documents, documents d'activité, informations », mais aussi les « données », afin de couvrir les cas où les horodatages sont associés à des données qui ne figurent pas dans un document et qui ne sont pas présentées de manière organisée comme des informations.

Références

[A/CN.9/971](#), par. 129 à 134 ; [A/CN.9/1005](#), par. 55.

7. Article 19. Archivage électronique

158. L'article 19 traite des services d'archivage électronique, qui assurent la sécurité juridique quant à la validité des documents électroniques conservés. La méthode utilisée pour l'archivage électronique apporte une garantie pour ce qui est de l'intégrité des documents électroniques archivés et de la date et de l'heure de l'archivage. En outre, les informations archivées doivent être accessibles conformément à l'exigence d'équivalence fonctionnelle avec la notion d'« forme écrite » dans l'environnement papier (art. 6-1 de la LTCE).

159. L'article 19 s'inspire, entre autres, de l'article 10 de la LTCE, qui traite de la conservation des messages de données. Toutefois, l'article 10 de la LTCE parle de « conservation » des messages de données parce qu'il s'agit de satisfaire à l'obligation légale de conservation des documents papier, tandis que l'article 19 parle d'« archivage » parce qu'il traite du service de confiance fourni pour satisfaire à cette obligation (c'est-à-dire l'archivage électronique).

160. Les messages de données archivés ne doivent pas nécessairement avoir été envoyés ou reçus et peuvent être conservés par leur auteur.

161. Pour transmettre et conserver des messages de données, il peut être nécessaire, pour des raisons techniques, d'ajouter des informations au message de données et de les modifier mais sans altérer leur intégrité. Ces ajouts et modifications sont autorisés tant que le contenu du message de données reste complet et inchangé. En particulier, le paragraphe a) ii) autorise les déplacements de fichiers et les changements de format, qui sont des pratiques ordinaires en matière de conservation des données. Son libellé se fonde sur l'article 8-3 a) de la LTCE.

162. L'article 19 ne traite pas de la question de savoir si les documents électroniques archivés doivent faire l'objet d'une migration de manière à ce qu'il soit possible d'y accéder indépendamment de l'obsolescence technologique. Cette condition est satisfaite par l'application du principe de neutralité technologique et des exigences d'équivalence fonctionnelle avec la notion d'« intégrité », c'est-à-dire que, lorsqu'il est exigé qu'une information soit présentée, cette information peut être montrée à la personne à laquelle elle doit être présentée (art. 8-1 b) de la LTCE).

Références

[A/CN.9/971](#), par. 135 à 138 ; [A/CN.9/1005](#), par. 56 à 61 ; [A/CN.9/1045](#), par. 37 à 41.

8. Article 20. Services d'envoi recommandé électroniques

163. L'article 20 garantit l'envoi d'une communication électronique par l'expéditeur et sa réception par le destinataire, l'heure à laquelle l'envoi et la réception ont eu lieu, l'intégrité des données échangées et l'identité de l'expéditeur et du destinataire.

164. Les services d'envoi recommandé électroniques sont l'équivalent des services d'envoi recommandé, car les deux types de services sont utilisés pour prouver la transmission des communications. Pour garantir la sécurité et la confidentialité des échanges électroniques, le destinataire doit être identifié avant de pouvoir accéder à la communication électronique.

165. L'article 20 ne fait pas référence à des notions qui sont utilisées dans les textes existants de la CNUDCI, telles que l'« expédition » et la « réception » (voir art. 10 de la CCE), car il a été élaboré en mettant l'accent sur l'équivalence fonctionnelle entre les services d'envoi recommandé et les services d'envoi recommandé électroniques plutôt que sur les notions sous-jacentes.

Références

[A/CN.9/971](#), par. 139 à 141 ; [A/CN.9/1005](#), par. 62 à 64 ; [A/CN.9/1045](#), par. 42 à 44.

9. Article 21. Authentification de site Web

166. L'article 21 traite de l'authentification des sites Web, dont la fonction essentielle est de relier ledit site à la personne à laquelle le nom de domaine a été attribué ou concédé sous licence afin de confirmer la fiabilité du site. L'authentification d'un site Web comprend donc deux éléments : l'identification du détenteur du nom de domaine et la mise en relation de cette personne avec le site en question. Elle ne vise pas à identifier le site Web.

167. L'article 21 n'est pas une règle d'équivalence fonctionnelle puisqu'un site Web n'existe que sous forme électronique et que son authentification n'a donc pas d'équivalent hors ligne.

168. L'expression « personne qui détient le nom de domaine » désigne la personne à laquelle le droit d'utiliser le nom de domaine a été attribué ou concédé sous licence par un bureau d'enregistrement de noms de domaine. Cette personne n'est pas nécessairement « propriétaire » du site, ni la personne qui fournit ou exploite le contenu.

169. Des mesures de protection supplémentaires peuvent être nécessaires dans les cas où un nom de domaine est utilisé pour une plateforme qui héberge des pages Web créées et gérées par différentes personnes. Par exemple, la personne exploitant la plateforme peut avoir besoin d'identifier ces personnes selon une certaine procédure pour maintenir l'authentification du site Web.

Références

[A/CN.9/971](#), par. 142 à 144 ; [A/CN.9/1005](#), par. 65 et 66 ; [A/CN.9/1045](#), par. 47 et 48.

10. Article 22. Critères de fiabilité pour les services de confiance

170. L'article 22 dresse une liste non exhaustive des circonstances qui peuvent être pertinentes pour déterminer la fiabilité de la méthode utilisée selon l'approche *ex post*. La liste s'inspire des listes figurant à l'article 10 de la LTSE et à l'article 12 de la Loi type de la CNUDCI sur les documents transférables électroniques.

171. Tout comme la notion de méthode fiable utilisée par les services de gestion de l'identité (voir par. 104 ci-dessus), la notion de méthode fiable utilisée par les services de confiance est relative et varie en fonction de l'objectif poursuivi. La nature relative de la fiabilité est mentionnée au paragraphe 1 a), notamment par l'expression « suffisamment fiable », qui, selon la pratique établie à la CNUDCI, vise à mieux rendre compte des diverses utilisations des services de confiance, ainsi que par le membre de phrase « au regard de l'objet pour lequel le service de confiance est utilisé ».

Niveaux de fiabilité

172. La LTSE et plusieurs lois internes sur les signatures électroniques établissent une distinction entre les services de confiance selon leur niveau de fiabilité. Plus précisément, selon ces lois, les signatures électroniques qui satisfont à certaines exigences ont des effets juridiques plus importants et sont donc réputées offrir un niveau de fiabilité plus élevé. En outre, certaines lois exigent parfois que seules les signatures électroniques offrant un niveau de fiabilité plus élevé peuvent être désignées. Cette approche n'a pas été suivie dans le [projet d'instrument] et les services de confiance peuvent être désignés indépendamment du niveau de fiabilité qu'ils offrent.

173. Étant donné que les justificatifs d'identité offrant un niveau de garantie élevé peuvent être utilisés pour des services de confiance présentant des niveaux de fiabilité

différents, il n'existe pas de corrélation directe entre le niveau de garantie d'un service de gestion de l'identité et le niveau de fiabilité du service de confiance.

Références

[A/CN.9/965](#), par. 106 ; [A/CN.9/971](#), par. 120 et 121 ; [A/CN.9/1005](#), par. 67, 68 et 73 ; [A/CN.9/1045](#), par. 18 à 21, 27 à 29, 52 à 57 et 61 ; [A/CN.9/1051](#), par. 45 et 46.

11. Article 23. Désignation de services de confiance fiables

174. L'article 23 complète l'article 22 en permettant la désignation de services de confiance selon l'approche *ex ante*. Plus précisément, il énumère les conditions qu'un service de gestion de l'identité doit remplir pour figurer sur la liste de services de gestion de l'identité désignés présumés fiables aux fins des articles 16 à 21.

175. L'article 23 porte sur la désignation de services de confiance, étant entendu que le processus de désignation des services de confiance suppose nécessairement une évaluation de ces méthodes. Comme pour la désignation de services de gestion de l'identité, la désignation de services de confiance dont on présume qu'ils utilisent des méthodes fiables ne s'applique pas à des types génériques de services de confiance ni à l'ensemble des services de confiance offerts par un prestataire de services de confiance particulier, mais à un service de confiance déterminé fourni par un prestataire de services donné.

176. Le seul effet juridique de la désignation étant la présomption de fiabilité de la méthode utilisée, l'utilisation de services de confiance qui ont été désignés, mais qui ont perdu cette désignation, ne permet pas à la partie concernée de se prévaloir de cette présomption, mais n'a pas de conséquences sur la détermination de la fiabilité de la méthode.

177. L'article 23 exige que l'autorité de désignation publie une liste des services de confiance désignés, notamment les coordonnées des prestataires de services de confiance. Cette exigence vise à promouvoir la transparence et à informer les abonnés potentiels du service de confiance concerné. Les États adoptants pourraient envisager de regrouper ces listes de manière à ce que les informations puissent être consignées dans un répertoire supranational centralisé, à l'instar des répertoires régionaux existants.

Références

[A/CN.9/971](#), par. 150 à 152 ; [A/CN.9/1005](#), par. 69 à 73 ; [A/CN.9/1045](#), par. 30 à 33 et 58 à 61.

12. Article 24. Responsabilité des prestataires de services de confiance

178. À titre de principe général, les prestataires de services de confiance devraient être tenus responsables des conséquences de tout manquement à l'obligation de fournir les services conformément aux conditions convenues ou à d'autres exigences prévues par la loi. Plusieurs facteurs, notamment le type de service de confiance fourni, permettent de déterminer l'étendue de cette responsabilité. Comme pour les autres dispositions du [projet d'instrument], l'article 24 est sans incidence sur la responsabilité en cas de non-respect des obligations qui ne relèvent pas du [projet d'instrument].

179. Dans certains cas, l'identification du prestataire de services de confiance peut s'avérer difficile voire impossible (par exemple, les services d'horodatage utilisés en conjonction avec la technologie des registres distribués) et, par conséquent, la responsabilité ne peut être attribuée. Dans ces cas, le système peut prévoir d'autres moyens d'instaurer la confiance dans l'utilisation du service de confiance.

180. S'agissant des textes existants de la CNUDCI, la LTSE comporte des dispositions traitant des effets juridiques liés au comportement du signataire (art. 8), du prestataire de services de certification (art. 9) et de la partie se fiant à la signature

ou au certificat (art. 11). Ces dispositions précisent les obligations de chaque entité intervenant dans le cycle de vie de la signature électronique. La LTSE prévoit en outre la possibilité que les prestataires de services de certification limitent la portée ou l'étendue de leur responsabilité.

Références

[A/CN.9/1005](#), par. 74 à 76 ; [A/CN.9/1045](#), par. 62 à 66.

D. Chapitre IV. Aspects internationaux (art. 25 et 26)

1. Article 25. Reconnaissance internationale

181. L'article 25 établit un système de reconnaissance juridique internationale de la gestion de l'identité et des services de confiance qui prévoit que les systèmes de gestion de l'identité, les justificatifs d'identité, les services de gestion de l'identité et les services de confiance nationaux et étrangers bénéficient du même traitement juridique. Il se fonde sur le principe de non-discrimination à l'égard de l'origine géographique.

182. L'un des objectifs de l'article 25 est d'éviter que les prestataires de services aient à demander à être désignés dans plusieurs pays en vertu de l'article 23. Cela peut être particulièrement utile dans les pays où sont utilisées des normes techniques nationales qui, en tant que telles, risquent de ne pas être les mêmes que celles applicables ailleurs. La reconnaissance mutuelle de la certification, lorsqu'elle existe, peut jouer un rôle important dans la mise en œuvre de cette disposition.

183. La référence au « niveau de fiabilité » énoncé à l'article 25 englobe à la fois la notion de niveau de garantie, terme technique utilisé pour évaluer les services de gestion de l'identité, et celle de niveau de fiabilité, terme technique utilisé pour évaluer les services de confiance. À leur tour, ces notions peuvent être pertinentes pour déterminer la fiabilité d'un service ou pour désigner un service fiable conformément aux chapitres II et III.

184. Le [projet d'instrument] n'établit pas un ensemble commun de niveaux de garantie pour les systèmes de gestion de l'identité et de niveaux de fiabilité pour les services de confiance étant donné qu'il est difficile de se mettre d'accord sur des définitions mondialement reconnues. En outre, les lois et les pratiques commerciales pour élaborer ces définitions varient d'un pays à l'autre, notamment en ce qui concerne le rôle des autorités centrales par rapport à celui des accords contractuels.

185. Par ailleurs, la détermination du niveau de garantie d'un service de gestion de l'identité et du niveau de fiabilité d'un service de confiance est un exercice qui demande beaucoup de temps et de ressources, et tous les pays ne disposent pas forcément des ressources adéquates. Ces pays peuvent grandement bénéficier de la possibilité de reconnaître les services de gestion de l'identité et les services de confiance étrangers en s'appuyant sur des déterminations et désignations faites à l'étranger.

186. Les mots « un système de gestion de l'identité, un service de gestion de l'identité ou un justificatif d'identité, selon qu'il convient » visent à englober tous les aspects possiblement pertinents pour la reconnaissance internationale. Dans la pratique, il peut être préférable de se concentrer sur un service de gestion de l'identité en particulier et de ne pas reconnaître tous les services de gestion de l'identité proposés par un système de gestion de l'identité comme étant également fiables alors qu'un ou plusieurs d'entre eux ont peut-être un niveau de fiabilité inférieur. En outre, la reconnaissance des justificatifs d'identité ne devrait pas utiliser des justificatifs de gestion de l'identité qui sont restés inchangés alors que le service de gestion de l'identité utilisé pour les délivrer a été compromis.

187. La reconnaissance des services de gestion de l'identité et de confiance étrangers peut obliger le prestataire de services à adapter ses conditions de service. Par exemple,

le droit impératif du pays où est accordée la reconnaissance peut avoir des incidences sur la capacité du prestataire de services à limiter sa responsabilité.

188. Le paragraphe 1 propose deux libellés possibles sur l'équivalence du niveau de fiabilité requis. Le premier libellé requiert au moins le même niveau de fiabilité ; le second, un niveau de fiabilité substantiellement équivalent. La référence à un « niveau de fiabilité au moins équivalent » renvoie à des niveaux de fiabilité supérieurs à celui requis.

189. L'expression « niveau de fiabilité substantiellement équivalent » vise à englober les cas où le niveau de fiabilité défini dans différents pays ne correspond pas exactement, ce qui risque d'arriver en raison de l'absence de définition universellement reconnue de niveaux de fiabilité spécifiques. Une autre préoccupation à laquelle cette expression peut répondre concerne les éventuels obstacles au commerce liés à la nécessité de se conformer à des exigences techniques strictes.

190. Si des systèmes, services ou justificatifs offrent un niveau de fiabilité substantiellement équivalent, leur fiabilité, déterminée conformément aux articles 10 et 22, sera également équivalente. La référence à un « niveau de fiabilité substantiellement équivalent » renvoie à des niveaux de fiabilité supérieurs à celui requis. Elle est reprise de l'article 12 de la LTSE.

191. Le paragraphe 3 précise la manière dont les autorités chargées de la désignation peuvent désigner des services de gestion de l'identité et des services de confiance étrangers. Il développe les mécanismes visés aux articles 11-4 et 23-4, qui prévoient la non-discrimination géographique dans le processus de désignation, en permettant à l'autorité de désignation de l'État adoptant de se fier aux services de gestion de l'identité et aux services de confiance désignés par une autorité de désignation étrangère.

192. Lors de l'adoption des règlements d'application, l'État adoptant peut décider si le paragraphe 3 devrait fonctionner sur la base d'une reconnaissance automatique (par exemple, les systèmes de gestion de l'identité et les services de confiance désignés par l'autorité étrangère seraient automatiquement dotés du statut juridique de système ou service désigné dans l'État adoptant) ou sous la forme d'une présomption (par exemple, les services de gestion de l'identité et les services de confiance désignés par l'autorité étrangère seraient présumés fiables dans l'État adoptant, mais nécessiteraient, pour avoir le statut juridique de système ou service désigné dans cet État, une intervention de l'autorité de désignation).

193. Les mécanismes qui se fondent sur l'article 25-3 peuvent remplacer les dispositifs issus de la conclusion d'accords de reconnaissance mutuelle ad hoc entre organismes de contrôle.

Références

[A/CN.9/936](#), par. 75 à 77 ; [A/CN.9/1005](#), par. 120 ; [A/CN.9/1045](#), par. 67 à 74 ; [A/CN.9/1051](#), par. 57 à 66.

2. Article 26. Coopération

194. Des mécanismes de coopération institutionnelle pourraient grandement contribuer à assurer la reconnaissance juridique mutuelle et l'interopérabilité technique des systèmes de gestion de l'identité et des services de confiance. De tels mécanismes existent sous différentes formes et peuvent être de nature privée ou publique. La coopération peut consister en des échanges d'informations, de données d'expérience et de bonnes pratiques, notamment en ce qui concerne les exigences techniques, par exemple, sur les niveaux de garantie et les niveaux de fiabilité.

195. En outre, l'article 26 peut contribuer à la définition commune des normes techniques qui permettent de déterminer l'équivalence, y compris en ce qui concerne les niveaux de garantie et les niveaux de fiabilité.

Références

[A/CN.9/965](#), par. 119 et 120 ; [A/CN.9/1005](#), par. 122 ; [A/CN.9/1045](#), par. 75 ;
[A/CN.9/WG.IV/WP.153](#), par. 95 à 98.
