CNUDCI | COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL

Loi type de la CNUDCI sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance

NATIONS UNIES

Pour obtenir des informations complémentaires, s'adresser à :

Secrétariat de la CNUDCI, Centre international de Vienne,
B.P. 500, 1400 Vienne (Autriche)

Téléphone : (+43-1) 26060-4060
Fax : (+43-1) 26060-5813
Site Web : https://uncitral.un.org
Courrier électronique : uncitral@un.org

COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL

Loi type de la CNUDCI sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance

NATIONS UNIES
Vienne, 2023

NOTE

Les cotes des documents de l'Organisation des Nations Unies se composent de lettres majuscules et de chiffres. La simple mention d'une cote dans un texte signifie qu'il s'agit d'un document de l'Organisation.

PUBLICATION DES NATIONS UNIES

eISBN 978-92-1-002854-7

Les appellations employées dans cette publication et la présentation des données qui y figurent n'impliquent de la part du Secrétariat de l'Organisation des Nations Unies aucune prise de position quant au statut juridique des pays, territoires, villes ou zones, ou de leurs autorités, ni quant au tracé de leurs frontières ou limites.

Les liens vers des sites Internet mentionnés dans la présente publication visent à faciliter la lecture et sont exacts à la date de publication. L'Organisation des Nations Unies ne peut garantir qu'ils resteront valables dans l'avenir et décline toute responsabilité pour le contenu de sites Web externes.

Production éditoriale : Section des publications, de la bibliothèque et des services en anglais, Office des Nations Unies à Vienne.

Table des matières

Loi type de la CNUDCI sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance

Résolution adoptée par l'Assemblée générale le 7 décembre 2022

77/101. Loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance

L'Assemblée générale,

Rappelant sa résolution 2205 (XXI) du 17 décembre 1966, portant création de la Commission des Nations Unies pour le droit commercial international et donnant à celle-ci pour mandat d'encourager l'harmonisation et l'unification progressives du droit commercial international et, ce faisant, de prendre en considération les intérêts de tous les peuples, en particulier ceux des pays en développement, en favorisant un large développement du commerce international,

Rappelant également sa résolution 60/21 du 23 novembre 2005, par laquelle elle a adopté la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux et invité tous les États à envisager de devenir parties à la Convention, et ses résolutions 51/162 du 16 décembre 1996, 56/80 du 12 décembre 2001 et 72/114 du 17 décembre 2017, dans lesquelles elle a recommandé que tous les États prennent dûment en considération la Loi type sur le commerce électronique, la Loi type sur les signatures électroniques et la Loi type sur les documents transférables électroniques de la Commission,

Consciente du fait que la Convention, la Loi type sur le commerce électronique, la Loi type sur les signatures électroniques et la Loi type sur les documents transférables électroniques sont d'une utilité certaine pour les États en ce qu'elles permettent et facilitent le recours au commerce électronique dans les échanges internationaux,

Convaincue que la confiance, la sécurité juridique et la prévisibilité du commerce électronique, y compris au niveau international, se trouveront renforcées par l'harmonisation de certaines règles applicables à la reconnaissance légale de la gestion de l'identité et des services de confiance sur une base technologiquement neutre et, selon qu'il convient, conformément à l'approche fondée sur l'équivalence fonctionnelle,

Rappelant qu'à sa quarante-neuvième session, en 2016, la Commission avait chargé le Groupe de travail IV (Commerce électronique) d'entreprendre des travaux dans le domaine de l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance[1],

Notant que le Groupe de travail a consacré 10 sessions, de 2017 à 2022, à ces travaux et que la Commission a examiné à sa cinquante-cinquième session, en 2022, un projet de loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance élaboré par le Groupe de travail, ainsi que des observations sur ce projet reçues de gouvernements et d'organisations internationales invitées aux sessions du Groupe de travail[2],

Convaincue qu'une loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance complétera utilement les textes existants de la Commission dans le domaine du commerce électronique en aidant les États à renforcer la législation régissant l'utilisation de la gestion de l'identité et des services de confiance, ou à légiférer lorsqu'une telle législation n'existe pas, en particulier en ce qui concerne les aspects internationaux,

1. *Remercie* la Commission des Nations Unies pour le droit commercial international d'avoir achevé et adopté la Loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance [3];

2. *Prie* le Secrétaire général de publier la Loi type et une note explicative, y compris sous forme électronique, dans les six langues officielles de l'Organisation des Nations Unies, et de les diffuser largement auprès des gouvernements et des organismes intéressés ;

3. *Recommande* à tous les États de tenir compte de la Loi type lorsqu'ils modifieront leur législation régissant la gestion de l'identité et les services de confiance ou en adopteront une, et invite les États qui auront utilisé la Loi type à en informer la Commission ;

4. *Recommande* également aux États de continuer à envisager de devenir parties à la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux[4] et de tenir compte de la Loi type sur le commerce électronique[5], de la Loi type sur les signatures électroniques[6] et de la Loi type sur les

[1] *Documents officiels de l'Assemblée générale, soixante et onzième session, Supplément n° 17* (A/71/17), par. 235 et 236.

[2] Ibid., *soixante-dix-septième session, Supplément n° 17* (A/77/17), chap. VI.

[3] Ibid., annexe II.

[4] Résolution 60/21, annexe ; voir également Nations Unies, *Recueil des Traités*, vol. 2898, n° 50525.

[5] Résolution 51/162, annexe.

[6] Résolution 56/80, annexe.

documents transférables électroniques[7] lorsqu'ils modifieront leur législation régissant le commerce électronique ou en adopteront une ;

5. *Engage* les organismes concernés des Nations Unies et les autres organisations internationales et régionales intéressées à coordonner leurs activités juridiques dans le domaine du commerce électronique avec celles de la Commission, notamment au sujet de la facilitation du commerce sans papier, pour éviter les doubles emplois et faire en sorte que la modernisation et l'harmonisation des législations en matière de commerce électronique se fassent de manière efficiente, homogène et cohérente.

47e séance plénière
7 décembre 2022

[7] *Documents officiels de l'Assemblée générale, soixante-douzième session, Supplément n° 17* (A/72/17), annexe I.

Décision de la Commission des Nations Unies pour le droit commercial international

La Commission des Nations Unies pour le droit commercial international,

Rappelant la résolution 2205 (XXI) de l'Assemblée générale en date du 17 décembre 1966, qui porte création de la Commission des Nations Unies pour le droit commercial international afin d'encourager l'harmonisation et l'unification progressives du droit commercial international dans l'intérêt de tous les peuples, particulièrement ceux des pays en développement,

Consciente du fait que la Loi type de la CNUDCI sur les documents transférables électroniques[8], la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (2005)[9], la Loi type de la CNUDCI sur les signatures électroniques (2001)[10] et la Loi type de la CNUDCI sur le commerce électronique (1996)[11] sont d'une utilité certaine pour les États en ce qu'elles permettent et facilitent le recours au commerce électronique dans les échanges internationaux,

Consciente également qu'il importe d'asseoir la confiance mutuelle sur une base juridique pour promouvoir la confiance dans le commerce électronique, en particulier au niveau international, et que la gestion de l'identité et les services de confiance revêtent à cette fin une pertinence croissante,

Convaincue que la sécurité juridique et la prévisibilité commerciale du commerce électronique, notamment au niveau international, se trouveront renforcées par l'harmonisation de certaines règles applicables à la reconnaissance juridique de la gestion de l'identité et des services de confiance sur une base technologiquement neutre et, selon qu'il convient, conformément à l'approche fondée sur l'équivalence fonctionnelle,

---

[8] *Documents officiels de l'Assemblée générale, soixante-douzième session, Supplément n° 17* (A/72/17), annexe I.

[9] Résolution 60/21 de l'Assemblée générale, annexe.

[10] Résolution 56/80 de l'Assemblée générale, annexe.

[11] Résolution 51/162 de l'Assemblée générale, annexe.

Estimant qu'une loi type de la CNUDCI sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance complétera utilement les textes existants de la CNUDCI dans le domaine du commerce électronique en aidant de façon appréciable les États à renforcer la législation régissant le recours à la gestion de l'identité et aux services de confiance, ou à légiférer lorsqu'une telle législation n'existe pas encore, s'agissant en particulier des aspects internationaux,

Rappelant qu'à sa quarante-neuvième session, en 2016, elle avait chargé le Groupe de travail IV (Commerce électronique) d'entreprendre des travaux sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance[12],

Ayant examiné, à sa cinquante-cinquième session, en 2022, un projet de loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance et la note explicative y relative, tous deux élaborés par le Groupe de travail[13], ainsi que des observations sur ce projet reçues de gouvernements et d'organisations internationales[14],

Remerciant le Groupe de travail IV des travaux qu'il a réalisés pour mettre au point le projet de loi type de la CNUDCI sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance, ainsi que les organisations intergouvernementales et les organisations non gouvernementales invitées de leur soutien et de leur participation à ces travaux,

1. *Adopte* la Loi type de la CNUDCI sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance, telle qu'elle figure à l'annexe II du rapport sur les travaux de sa cinquante-cinquième session ;

2. *Approuve* en principe le projet de note explicative relative à la Loi type de la CNUDCI sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance, demande au Secrétariat d'y mettre la dernière main en tenant compte des délibérations tenues et des décisions prises à sa cinquante-cinquième session, et autorise le Groupe de travail IV (Commerce électronique) à revoir, à sa soixante-quatrième session, en 2022, les parties ayant trait aux délibérations et aux décisions de la cinquante-cinquième session de la Commission ;

3. *Prie* le Secrétaire général de publier la Loi type de la CNUDCI sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance et sa note explicative, y compris sous forme électronique, dans les six langues officielles de l'Organisation des Nations Unies, et de les diffuser largement auprès des gouvernements et d'autres organismes intéressés ;

---

[12] *Documents officiels de l'Assemblée générale, soixante et onzième session, Supplément n° 17* (A/71/17), par. 235 et 236.

[13] A/CN.9/1112, annexes I et II.

[14] A/CN.9/1113 et A/CN.9/1113/Add.1.

4. *Recommande* à tous les États de prendre dûment en considération la Loi type de la CNUDCI sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance lorsqu'ils modifieront leur législation relative à la gestion de l'identité et aux services de confiance ou en adopteront une, et invite les États qui auront utilisé la Loi type à l'en informer.

1170e séance
7 juillet 2022

Loi type de la CNUDCI sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance

Chapitre premier. Dispositions générales

Article premier. Définitions

Aux fins de la présente Loi :

a) Par « attribut », on entend un élément d'information ou de donnée associé à une personne ;

b) Par « message de données », on entend l'information créée, transmise, reçue ou conservée par des moyens électroniques, magnétiques ou optiques ou des moyens analogues ;

c) Par « identification électronique », dans le cadre des services de gestion de l'identité, on entend un processus utilisé pour obtenir une garantie suffisante du lien unissant une personne à une identité ;

d) Par « identité », on entend un ensemble d'attributs qui permet à une personne d'être identifiée de manière unique dans un contexte particulier ;

e) Par « justificatifs d'identité », on entend les données, ou l'objet matériel sur lequel elles peuvent se trouver, qu'une personne peut présenter à des fins d'identification électronique ;

f) Par « services de gestion de l'identité », on entend des services consistant à gérer la confirmation d'identité et l'identification électronique ;

g) Par « prestataire de services de gestion de l'identité », on entend la personne qui conclut un accord avec un abonné en vue de la fourniture de tels services ;

h) Par « système de gestion de l'identité », on entend un ensemble de fonctions et de fonctionnalités permettant de gérer la confirmation d'identité et l'identification électronique ;

i) Par « confirmation d'identité », on entend le processus consistant à réunir, à vérifier et à valider suffisamment d'attributs pour établir et confirmer l'identité d'une personne dans un contexte particulier ;

j) Par « partie utilisatrice », on entend une personne qui agit sur la base du résultat d'un service de gestion de l'identité ou d'un service de confiance ;

k) Par « abonné », on entend une personne qui conclut un accord avec un prestataire de services de gestion de l'identité ou un prestataire de services de confiance en vue de la fourniture de tels services ;

l) Par « service de confiance », on entend un service électronique qui garantit certaines qualités d'un message de données et comprend les méthodes utilisées pour créer et gérer les signatures électroniques, les cachets électroniques, les horodatages électroniques, l'authentification de site Web, l'archivage électronique et les services d'envoi recommandé électroniques ;

m) Par « prestataire de services de confiance », on entend la personne qui conclut un accord avec un abonné en vue de la fourniture de tels services.

Article 2. Champ d'application

1. La présente Loi s'applique à l'utilisation et à la reconnaissance internationale de la gestion de l'identité et des services de confiance dans le cadre d'activités commerciales et de services touchant au commerce.

2. Aucune disposition de la présente Loi n'exige l'identification d'une personne.

3. Aucune disposition de la présente Loi n'a d'incidence sur une exigence légale selon laquelle une personne doit être identifiée ou un service de confiance être utilisé suivant une procédure définie ou prescrite par la loi.

4. Rien dans la présente Loi, en dehors de ce qui y est disposé, n'a d'incidence sur l'application aux services de gestion de l'identité ou aux services de confiance de toute loi applicable à la protection et à la confidentialité des données.

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

1. Aucune disposition de la présente Loi n'oblige une personne à utiliser un service de gestion de l'identité ou un service de confiance, ou à utiliser un service de gestion de l'identité ou un service de confiance particulier, sans son consentement.

2. Aux fins du paragraphe 1, le consentement peut être déduit du comportement de la personne.

Article 4. Interprétation

1. Pour l'interprétation de la présente Loi, il est tenu compte de son origine internationale et de la nécessité de promouvoir l'uniformité de son application ainsi que d'assurer le respect de la bonne foi dans le commerce international.

2. Les questions concernant les matières régies par la présente Loi qui ne sont pas expressément réglées par elle sont tranchées selon les principes généraux dont elle s'inspire.

Chapitre II. Gestion de l'identité

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

Sous réserve du paragraphe 3 de l'article 2, le résultat de l'identification électronique n'est pas privé de ses effets juridiques, de sa validité, de sa force exécutoire ou de sa recevabilité comme preuve au seul motif que :

a) La confirmation d'identité et l'identification électronique se font sous forme électronique ; ou

b) Le service de gestion de l'identité n'est pas désigné conformément à l'article 11.

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

Le prestataire de services de gestion de l'identité est tenu, au minimum :

a) D'avoir en place des règles, politiques et pratiques de fonctionnement adaptées à l'objet et à la conception du système de gestion de l'identité, pour répondre, au minimum, aux exigences s'agissant :

i) D'inscrire les personnes, en ayant notamment soin :

a. De collecter et d'enregistrer les attributs ;

b. De confirmer et de vérifier l'identité ; et

c. D'attacher les justificatifs d'identité à la personne ;

ii) De mettre à jour les attributs ;

iii) De gérer les justificatifs d'identité, en ayant notamment soin :

a. D'émettre, de délivrer et d'activer les justificatifs ;

b. De suspendre, de révoquer et de réactiver les justificatifs ; et

c. De renouveler et de remplacer les justificatifs ;

iv) De gérer l'identification électronique des personnes, en ayant notamment soin :

a. De gérer les facteurs d'identification électronique ; et

b. De gérer les mécanismes d'identification électronique ;

b) D'agir conformément à ses règles, politiques et pratiques de fonctionnement, et à toute déclaration qu'il fait à leur égard ;

c) De garantir la disponibilité en ligne et le bon fonctionnement du système de gestion de l'identité ;

d) De rendre ses règles, politiques et pratiques de fonctionnement facilement accessibles aux abonnés, aux parties utilisatrices et aux autres tiers ;

e) De fournir des moyens facilement accessibles pour permettre à une partie utilisatrice de déterminer, le cas échéant :

i) Toute restriction quant aux fins ou à la valeur pour lesquelles le service de gestion de l'identité peut être utilisé ; et

ii) Toute restriction quant à l'étendue de la responsabilité stipulée par le prestataire de services de gestion de l'identité ; et

f) De fournir et mettre à la disposition du public les moyens que l'abonné peut utiliser pour informer le prestataire de services de gestion de l'identité de toute atteinte à la sécurité conformément à l'article 8.

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

1. En cas d'atteinte à la sécurité ou de perte d'intégrité ayant une incidence importante sur le système de gestion de l'identité, notamment sur les attributs qui y sont gérés, le prestataire de services de gestion de l'identité est tenu, conformément à la loi :

a) De prendre toutes les mesures raisonnables pour mettre fin à l'atteinte ou à la perte, y compris, le cas échéant, de suspendre le service concerné ou de révoquer les justificatifs d'identité concernés ;

b) De remédier à l'atteinte ou à la perte ; et

c) De notifier l'atteinte ou la perte.

2. Si une personne lui notifie une atteinte à la sécurité ou une perte d'intégrité, le prestataire de services de gestion de l'identité est tenu :

a) D'examiner l'éventuelle atteinte ou perte ; et

b) De prendre toute autre mesure appropriée conformément au paragraphe 1.

Article 8. Obligations incombant aux abonnés

L'abonné avise le prestataire de services de gestion de l'identité, en utilisant les moyens mis à sa disposition par celui-ci conformément à l'article 6 ou en utilisant d'une autre manière des moyens raisonnables, si :

a) Il sait que ses justificatifs d'identité ont été compromis ; ou

b) Il estime, au regard des circonstances connues de lui, qu'il y a un risque important que ses justificatifs d'identité aient été compromis.

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

Sous réserve du paragraphe 3 de l'article 2, lorsque la loi exige l'identification d'une personne à une fin particulière ou prévoit des conséquences en l'absence d'identification, cette exigence est satisfaite dans le cas des services de gestion de l'identité si une méthode fiable, conformément au paragraphe 1 ou au paragraphe 4 de l'article 10, est employée pour la confirmation d'identité et l'identification électronique de cette personne à cette fin.

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

1. Aux fins de l'article 9, la méthode :

a) Est suffisamment fiable au regard de l'objet pour lequel le service de gestion de l'identité est utilisé ; ou

b) Est réputée suffisamment fiable s'il a été démontré dans les faits, par ou devant un tribunal ou un organe décisionnel compétent, qu'elle a, par elle-même ou avec d'autres preuves, rempli la fonction décrite à l'article 9.

2. Pour déterminer la fiabilité de la méthode, toutes les circonstances pertinentes sont prises en considération, notamment :

a) Le respect, par le prestataire de services de gestion de l'identité, des obligations énoncées à l'article 6 ;

b) La conformité des règles, politiques et pratiques de fonctionnement du prestataire de services de gestion de l'identité aux normes et procédures internationalement reconnues applicables qui sont pertinentes pour la fourniture de tels services, notamment au cadre relatif aux niveaux de garantie, en particulier aux règles relatives à :

i) La gouvernance ;

ii) La publication d'avis et les informations relatives aux utilisateurs ;

iii) La gestion de la sécurité de l'information ;

iv) La conservation des documents ;

v) Les installations et le personnel ;

vi) Les contrôles techniques ; et

vii) Le contrôle et l'audit ;

c) Toute supervision ou toute certification fournie concernant le service de gestion de l'identité ;

d) Tout niveau pertinent de garantie de la méthode utilisée ;

e) La fin à laquelle l'identification est utilisée ; et

f) Toute convention pertinente conclue entre les parties, y compris toute limite fixée en ce qui concerne l'objet ou la valeur des transactions pour lesquelles le service de gestion de l'identité peut être utilisé.

3. Pour déterminer la fiabilité de la méthode, il n'est pas tenu compte :

a) Du lieu où le service de gestion de l'identité est fourni ; ou

b) Du lieu où se trouve l'établissement du prestataire de services de gestion de l'identité.

4. Une méthode utilisée par un service de gestion de l'identité désigné conformément à l'article 11 est présumée fiable.

5. Le paragraphe 4 ne limite pas la capacité d'une personne :

a) D'établir par tout autre moyen la fiabilité d'une méthode ; ou

b) D'apporter des preuves de la non-fiabilité d'une méthode utilisée par un service de gestion de l'identité désigné conformément à l'article 11.

Article 11. Désignation de services de gestion de l'identité fiables

1. [*Toute personne, tout organe ou toute autorité, de droit public ou privé, indiqué(e) par l'État adoptant comme compétent(e) en la matière*] peut désigner les services de gestion de l'identité qui sont présumés fiables.

2. [*La personne, l'organe ou l'autorité, de droit public ou privé, indiqué(e) par l'État adoptant comme compétent(e) en la matière*] est tenu(e) :

a) De prendre en considération toutes les circonstances pertinentes, y compris les facteurs énumérés à l'article 10, pour désigner un service de gestion de l'identité ; et

b) De publier une liste des services de gestion de l'identité désignés, en mentionnant notamment les coordonnées des prestataires de tels services.

3. Toute désignation effectuée en vertu du paragraphe 1 doit être conforme aux normes et procédures internationalement reconnues qui sont pertinentes pour l'exécution du processus de désignation, notamment au cadre relatif aux niveaux de garantie.

4. Pour désigner un service de gestion de l'identité, il n'est pas tenu compte :

a) Du lieu où le service de gestion de l'identité est fourni ; ou

b) Du lieu où se trouve l'établissement du prestataire de services de gestion de l'identité.

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

1. Le prestataire de services de gestion de l'identité est tenu responsable des pertes causées à l'abonné ou à la partie utilisatrice en raison d'un manquement aux obligations qui lui incombent en vertu des articles 6 et 7.

2. Le paragraphe 1 s'applique conformément aux règles prévues par la loi en matière de responsabilité et est sans préjudice :

a) De tout autre fondement de la responsabilité prévu par la loi, y compris la responsabilité pour non-respect des obligations contractuelles ; ou

b) De toute autre conséquence juridique découlant d'un manquement du prestataire de services de gestion de l'identité aux obligations qui lui incombent en vertu de la présente Loi.

3. Nonobstant les dispositions du paragraphe 1, le prestataire de services de gestion de l'identité n'est pas responsable envers l'abonné des pertes découlant de l'utilisation d'un tel service dans la mesure où :

a) Cette utilisation dépasse les limites fixées en ce qui concerne l'objet ou la valeur des transactions pour lesquelles le service de gestion de l'identité est utilisé ; et

b) Ces limites sont contenues dans l'accord conclu entre le prestataire de services de gestion de l'identité et l'abonné.

4. Nonobstant les dispositions du paragraphe 1, le prestataire de services de gestion de l'identité n'est pas responsable envers la partie utilisatrice des pertes découlant de l'utilisation d'un tel service dans la mesure où :

a) Cette utilisation dépasse les limites fixées en ce qui concerne l'objet ou la valeur des transactions pour lesquelles le service de gestion de l'identité est utilisé ; et

b) Le prestataire de services de gestion de l'identité s'est acquitté des obligations qui lui incombent en vertu de l'article 6 e en ce qui concerne cette transaction.

Chapitre III. Services de confiance

Article 13. Reconnaissance juridique des services de confiance

Le résultat de l'utilisation d'un service de confiance n'est pas privé de ses effets juridiques, de sa validité, de sa force exécutoire ou de sa recevabilité comme preuve au seul motif que :

a) Il se présente sous forme électronique ; ou

b) Le service de confiance n'est pas désigné conformément à l'article 23.

Article 14. Obligations incombant aux prestataires de services de confiance

1. Le prestataire de services de confiance est tenu, au minimum :

a) D'avoir en place des règles, politiques et pratiques de fonctionnement, notamment un plan visant à assurer la continuité en cas de cessation d'activité, adaptées à l'objet et à la conception du service de confiance ;

b) D'agir conformément à ses règles, politiques et pratiques de fonctionnement, et à toute déclaration qu'il fait à leur égard ;

c) De rendre ses règles, politiques et pratiques de fonctionnement facilement accessibles aux abonnés, aux parties utilisatrices et aux autres tiers ;

d) De fournir et mettre à la disposition du public les moyens que l'abonné peut utiliser pour informer le prestataire de services de confiance de toute atteinte à la sécurité conformément à l'article 15 ; et

e) De fournir des moyens facilement accessibles pour permettre à une partie utilisatrice de déterminer, le cas échéant :

i) Toute restriction quant aux fins ou à la valeur pour lesquelles le service de confiance peut être utilisé ; et

ii) Toute restriction quant à l'étendue de la responsabilité stipulée par le prestataire de services de confiance.

2. En cas d'atteinte à la sécurité ou de perte d'intégrité ayant une incidence importante sur un service de confiance, le prestataire de ce service est tenu, conformément à la loi :

a) De prendre toutes les mesures raisonnables pour mettre fin à l'atteinte ou à la perte, y compris, le cas échéant, de suspendre ou de révoquer le service concerné ;

b) De remédier à l'atteinte ou à la perte ; et

c) De notifier l'atteinte ou la perte.

Article 15. Obligations incombant aux abonnés

L'abonné avise le prestataire de services de confiance, en utilisant les moyens mis à sa disposition par celui-ci conformément au paragraphe 1 de l'article 14 ou en utilisant d'une autre manière des moyens raisonnables, si :

a) Il sait que les données ou les moyens qu'il a utilisés pour accéder au service de confiance et l'utiliser ont été compromis ; ou

b) Il estime, au regard des circonstances connues de lui, qu'il y a un risque important que le service de confiance ait été compromis.

Article 16. Signatures électroniques

Lorsque la loi exige la signature d'une personne, ou prévoit des conséquences en l'absence de signature, cette exigence est satisfaite dans le cas d'un message de données si une méthode fiable, conformément au paragraphe 1 ou au paragraphe 4 de l'article 22, est employée pour :

a) Identifier la personne ; et

b) Indiquer la volonté de cette personne concernant l'information contenue dans le message de données.

Article 17. Cachets électroniques

Lorsque la loi exige qu'une personne morale appose un cachet, ou prévoit des conséquences en l'absence de cachet, cette exigence est satisfaite dans le cas d'un message de données si une méthode fiable, conformément au paragraphe 1 ou au paragraphe 4 de l'article 22, est employée pour :

a) Fournir une garantie fiable de l'origine du message de données ; et

b) Détecter toute altération du message de données après la date et l'heure de l'apposition du cachet, exception faite de l'ajout de tout endossement et de toute modification intervenant dans le cours normal de la communication, du stockage et de l'affichage.

Article 18. Horodatages électroniques

Lorsque la loi exige que des documents, documents d'activité, informations ou données soient accompagnés d'une indication de date et d'heure, ou prévoit des conséquences en l'absence de date et d'heure, cette exigence est satisfaite dans le cas d'un message de données si une méthode fiable, conformément au paragraphe 1 ou au paragraphe 4 de l'article 22, est employée pour :

a) Indiquer la date et l'heure, en précisant notamment le fuseau horaire ; et

b) Associer au message de données la date et l'heure indiquées.

Article 19. Archivage électronique

Lorsque la loi exige que des documents, documents d'activité ou informations soient conservés, ou prévoit des conséquences en l'absence de leur conservation, cette exigence est satisfaite dans le cas d'un message de données si une méthode fiable, conformément au paragraphe 1 ou au paragraphe 4 de l'article 22, est employée pour :

a) Rendre l'information contenue dans ce message accessible pour être consultée ultérieurement ;

b) Indiquer la date et l'heure de l'archivage et associer au message de données la date et l'heure indiquées ;

c) Conserver le message de données dans le format sous lequel il a été créé, transmis ou reçu, ou dans un autre format dont il peut être démontré qu'il permet de détecter toute altération du message après cette date et cette heure, exception faite de l'ajout de tout endossement et de toute modification intervenant dans le cours normal de la communication, du stockage et de l'affichage ; et

d) Conserver les informations qui permettent de déterminer l'origine et la destination du message de données, ainsi que les indications de date et d'heure de la transmission ou de la réception, si elles existent.

Article 20. Services d'envoi recommandé électroniques

Lorsque la loi exige que des documents, documents d'activité ou informations soient envoyés par courrier recommandé ou au moyen d'un service similaire, ou prévoit des conséquences en l'absence de leur remise, cette exigence est satisfaite dans le cas d'un message de données si une méthode fiable, conformément au paragraphe 1 ou au paragraphe 4 de l'article 22, est employée pour :

a) Indiquer la date et l'heure auxquelles le message de données a été reçu pour envoi et la date et l'heure auxquelles il a été remis ;

b) Détecter toute modification du message de données entre la date et l'heure auxquelles le message de données a été reçu pour envoi et la date et l'heure auxquelles il a été remis, exception faite de l'ajout de tout endossement ou de toute information requis par le présent article, et de toute modification intervenant dans le cours normal de la communication, du stockage et de l'affichage ; et

c) Identifier l'expéditeur et le destinataire.

Article 21. Authentification de site Web

Lorsque la loi exige l'authentification du site Web, ou prévoit des conséquences en l'absence d'authentification, cette exigence est satisfaite si une méthode fiable, conformément au paragraphe 1 ou au paragraphe 4 de l'article 22, est employée pour :

a) Identifier la personne qui détient le nom de domaine du site Web ; et

b) Associer cette personne au site Web.

Article 22. Critères de fiabilité pour les services de confiance

1. Aux fins des articles 16 à 21, la méthode :

a) Est suffisamment fiable au regard de l'objet pour lequel le service de confiance est utilisé ; ou

b) Est réputée suffisamment fiable s'il a été démontré dans les faits, par ou devant un tribunal ou un organe décisionnel compétent, qu'elle a, par elle-même ou avec d'autres preuves, rempli les fonctions décrites dans l'article.

2. Pour déterminer la fiabilité de la méthode, toutes les circonstances pertinentes sont prises en considération, notamment :

a) Le respect, par le prestataire de services de confiance, des obligations énoncées à l'article 14 ;

b) La conformité des règles, politiques et pratiques de fonctionnement du prestataire de services de confiance aux normes et procédures internationalement reconnues applicables qui sont pertinentes pour la fourniture de tels services ;

c) Tout niveau pertinent de fiabilité de la méthode utilisée ;

d) Toute norme sectorielle applicable ;

e) La sûreté du matériel et des logiciels ;

f) Les ressources financières et humaines, y compris l'existence d'avoirs ;

g) La régularité et l'étendue des audits réalisés par un organisme indépendant ;

h) L'existence d'une déclaration faite par un organisme de supervision, un organisme d'accréditation ou un programme volontaire concernant la fiabilité de la méthode ;

i) La fin à laquelle le service de confiance est utilisé ; et

j) Toute convention pertinente conclue entre les parties, y compris toute limite fixée en ce qui concerne l'objet ou la valeur des transactions pour lesquelles le service de confiance peut être utilisé.

3. Pour déterminer la fiabilité de la méthode, il n'est pas tenu compte :

a) Du lieu où le service de confiance est fourni ; ou

b) Du lieu où se trouve l'établissement du prestataire de services de confiance.

4. Une méthode utilisée par un service de confiance désigné conformément à l'article 23 est présumée fiable.

5. Le paragraphe 4 ne limite pas la capacité d'une personne :

a) D'établir par tout autre moyen la fiabilité d'une méthode ; ou

b) D'apporter des preuves de la non-fiabilité d'une méthode utilisée par un service de confiance désigné conformément à l'article 23.

Article 23. Désignation de services de confiance fiables

1. [*Toute personne, tout organe ou toute autorité, de droit public ou privé, indiqué(e) par l'État adoptant comme compétent(e) en la matière*] peut désigner les services de confiance qui sont présumés fiables.

2. [*La personne, l'organe ou l'autorité, de droit public ou privé, indiqué(e) par l'État adoptant comme compétent(e) en la matière*] est tenu(e) :

a) De prendre en considération toutes les circonstances pertinentes, y compris les facteurs énumérés à l'article 22, pour désigner un service de confiance ; et

b) De publier une liste des services de confiance désignés, en mentionnant notamment les coordonnées des prestataires de tels services.

3. Toute désignation effectuée en vertu du paragraphe 1 doit être conforme aux normes et procédures internationalement reconnues qui sont pertinentes pour l'exécution du processus de désignation.

4. Pour désigner un service de confiance, il n'est pas tenu compte :

a) Du lieu où le service de confiance est fourni ; ou

b) Du lieu où se trouve l'établissement du prestataire de services de confiance.

Article 24. Responsabilité des prestataires de services de confiance

1. Le prestataire de services de confiance est tenu responsable des pertes causées à l'abonné ou à la partie utilisatrice en raison d'un manquement aux obligations qui lui incombent en vertu de l'article 14.

2. Le paragraphe 1 s'applique conformément aux règles prévues par la loi en matière de responsabilité et est sans préjudice :

a) De tout autre fondement de la responsabilité prévu par la loi, y compris la responsabilité pour non-respect des obligations contractuelles ; ou

b) De toute autre conséquence juridique découlant d'un manquement du prestataire de services de confiance aux obligations qui lui incombent en vertu de la présente Loi.

3. Nonobstant les dispositions du paragraphe 1, le prestataire de services de confiance n'est pas responsable envers l'abonné des pertes découlant de l'utilisation d'un tel service dans la mesure où :

a) Cette utilisation dépasse les limites fixées en ce qui concerne l'objet ou la valeur des transactions pour lesquelles le service de confiance est utilisé ; et

b) Ces limites sont contenues dans l'accord conclu entre le prestataire de services de confiance et l'abonné.

4. Nonobstant les dispositions du paragraphe 1, le prestataire de services de confiance n'est pas responsable envers la partie utilisatrice des pertes découlant de l'utilisation d'un tel service dans la mesure où :

a) Cette utilisation dépasse les limites fixées en ce qui concerne l'objet ou la valeur des transactions pour lesquelles le service de confiance est utilisé ; et

b) Le prestataire de services de confiance s'est acquitté des obligations qui lui incombent en vertu du paragraphe 1 e de l'article 14 en ce qui concerne cette transaction.

Chapitre IV. Reconnaissance internationale

Article 25. Reconnaissance internationale du résultat de l'identification électronique

1. Le résultat de l'identification électronique fournie en dehors de [*l'État adoptant*] a les mêmes effets juridiques dans cet État que l'identification électronique fournie dans [*l'État adoptant*], à condition que la méthode utilisée par le système de gestion de l'identité, le service de gestion de l'identité ou le justificatif d'identité, selon le cas, offre :

a) Un niveau de garantie au moins équivalent, lorsque les niveaux de garantie reconnus par ces États sont identiques ; ou

b) Un niveau de garantie substantiellement équivalent ou supérieur, dans tous les autres cas.

2. Pour déterminer si les exigences du paragraphe 1 sont satisfaites, il est tenu compte des normes internationalement reconnues.

3. Le système de gestion de l'identité, le service de gestion de l'identité ou le justificatif d'identité est présumé satisfaire aux exigences du paragraphe 1 si [*la personne, l'organe ou l'autorité indiqué(e) par l'État adoptant conformément à l'article 11*] a déterminé l'équivalence, en tenant compte du paragraphe 2 de l'article 10.

Article 26. Reconnaissance internationale du résultat découlant de l'utilisation d'un service de confiance

1. Le résultat découlant de l'utilisation d'un service de confiance fourni en dehors de [*l'État adoptant*] a les mêmes effets juridiques dans cet État que le résultat découlant de l'utilisation d'un tel service qui serait fourni dans [*l'État adoptant*], à condition que la méthode utilisée par ce service offre :

a) Un niveau de fiabilité au moins équivalent, lorsque les niveaux de fiabilité reconnus par ces États sont identiques ; ou

b) Un niveau de fiabilité substantiellement équivalent ou supérieur, dans tous les autres cas.

2. Pour déterminer si les exigences du paragraphe 1 sont satisfaites, il est tenu compte des normes internationalement reconnues.

3. Le service de confiance est présumé satisfaire aux exigences du paragraphe 1 si [*la personne, l'organe ou l'autorité indiqué(e) par l'État adoptant conformément à l'article 23*] a déterminé l'équivalence, en tenant compte du paragraphe 2 de l'article 22.

Article 27. Coopération

[*La personne, l'organe ou l'autorité indiqué(e) par l'État adoptant comme compétent(e) en la matière*] peut coopérer avec des entités étrangères en échangeant des informations, des données d'expérience et des bonnes pratiques ayant trait à la gestion de l'identité et aux services de confiance, notamment en ce qui concerne :

a) La reconnaissance des effets juridiques de systèmes de gestion de l'identité et de services de confiance étrangers, qu'elle soit accordée unilatéralement ou d'un commun accord ;

b) La désignation de systèmes de gestion de l'identité et de services de confiance ; et

c) La définition de niveaux de garantie pour les systèmes de gestion de l'identité et de niveaux de fiabilité pour les services de confiance.

Guide pour l'incorporation de la Loi type de la CNUDCI sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance

Introduction

A. Objet du Guide

1. En élaborant et adoptant sa Loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance (ci-après la « Loi type »), la Commission des Nations Unies pour le droit commercial international (la « CNUDCI ») a estimé que celle-ci contribuerait mieux à l'harmonisation et à la modernisation de la législation si elle s'accompagnait d'informations sur les travaux préparatoires et d'explications.

2. Le présent Guide, qui se fonde sur les travaux préparatoires de la Loi type, vise à aider les personnes intéressées par l'adoption, l'utilisation et l'interprétation uniforme de la Loi type, telles que les décideurs, les législateurs, les universitaires, les praticiens, les juges, les arbitres, ainsi que les opérateurs commerciaux et les utilisateurs de la gestion de l'identité et des services de confiance. Ainsi, les informations contenues dans le présent Guide pourraient aider les États, au moment d'adopter une législation fondée sur la Loi type, à adapter celle-ci à leurs besoins, en ayant notamment à l'esprit l'interaction entre les dispositions de la Loi type et le régime réglementaire relatif à la gestion de l'identité et aux services de confiance.

B. Objectifs

3. Au cours des 20 dernières années, la valeur des activités commerciales en ligne (c'est-à-dire transactions électroniques entre entreprises, entre entreprises et consommateurs, et entre entreprises et États) a crû de manière exponentielle. Cette croissance,

encore accélérée par la nécessité d'atténuer les effets de la pandémie de COVID-19[15], s'est accompagnée d'une hausse similaire des transactions de données, et nécessite la mise en place d'un cadre juridique et technique adéquat.

4. La croissance des activités commerciales en ligne repose sur la confiance – et doit être soutenue par un sentiment de confiance continu – dans l'environnement électronique. 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 cette confiance. L'importance de l'identité est soulignée par l'objectif de développement durable n° 16, dont la cible 9 appelle à la fourniture d'une identité juridique pour tous les êtres humains, y compris sous forme électronique. Dans l'économie numérique, cela revient au droit à une identité numérique.

5. Au fil des années, diverses solutions ont été proposées pour répondre au besoin d'identification en ligne, ce qui a conduit à la mise au point de systèmes, méthodes, technologies et dispositifs afin de créer et de gérer les identités numériques des 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 les secteurs privé ou public.

6. Un autre élément essentiel à la confiance en ligne est la nécessité de pouvoir se fier avec suffisamment de certitude à la qualité des données, qui sous-tend les échanges de données. Les services de confiance qui fournissent des garanties quant aux caractéristiques d'un message de données, telles que son origine, son intégrité et le moment où certaines actions connexes sont exécutées, apparaissent comme des solutions susceptibles d'assurer cette confiance.

7. Les obstacles à une utilisation plus large de la gestion de l'identité et des services de confiance peuvent être de plusieurs natures. Ainsi, l'accès à la gestion de l'identité et aux services de confiance peut être limité en raison du coût, du manque de connaissances et des contraintes techniques. Parmi les obstacles de nature juridique figurent notamment : *a)* l'absence de législation conférant des effets juridiques à la gestion de l'identité et aux services de confiance ; *b)* l'existence d'approches juridiques divergentes en matière de gestion de l'identité, notamment de lois fondées sur des exigences spécifiques à une technologie ; *c)* l'application de lois exigeant des documents d'identité papier pour la conclusion d'opérations commerciales en ligne ; et *d)* l'absence de mécanismes permettant la reconnaissance juridique internationale de la gestion de l'identité et des services de confiance (A/CN.9/965, par. 52).

[15] *Rapport sur l'économie numérique 2021 : Flux transfrontières de données et développement : À qui profitent ces flux ?* (UNCTAD/DER/2021), p. 16 et 17.

8. La Loi type vise avant tout à surmonter ces obstacles par l'élaboration de règles juridiques uniformes ayant plusieurs objectifs. Ces règles uniformes peuvent : renforcer l'efficacité en favorisant l'acceptation, par tous les systèmes, du résultat de l'application de la gestion de l'identité et des services de confiance ; réduire les coûts de transaction en facilitant le respect des exigences réglementaires ; renforcer la prévisibilité et la sécurité juridiques des opérations électroniques sur la base d'un traitement commun des questions, notamment par des mécanismes de reconnaissance internationale ; et contribuer à réduire la fracture numérique grâce à une plus grande disponibilité de solutions communes.

9. En particulier, l'établissement d'un cadre juridique relatif à la gestion de l'identité et aux services de confiance contribuera à sécuriser le fonctionnement de l'identité numérique et des transactions de données. 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. De plus, comme on l'a noté au paragraphe 4 ci-dessus, la gestion de l'identité est directement liée à la réalisation de la cible 16.9, qui consiste à garantir à tous une identité juridique, car l'identité en ligne est un moyen de prouver son identité personnelle.

10. La gestion de l'identité contribue également à la réalisation de plusieurs autres cibles des objectifs de développement durable. Par exemple, en matière d'accès au financement, elle peut être utilisée pour satisfaire aux exigences de connaissance du client dans le domaine bancaire et pour tenir des registres de crédit et des registres fonciers efficaces, activités qui sont pertinentes pour la réalisation de la cible 1.4, qui prévoit de faire en sorte que tous les hommes et les femmes aient accès, entre autres, aux nouvelles technologies et aux services financiers. Une utilisation efficace de la gestion de l'identité pour satisfaire aux exigences de connaissance du client peut également contribuer à réduire les coûts de transaction des envois de fonds, ainsi que les flux financiers illicites, qui sont les objectifs des cibles 10.c et 16.4, respectivement.

11. Les services de confiance sont pertinents pour toutes les activités liées à l'innovation, car les nouvelles technologies telles que l'intelligence artificielle sont alimentées par de vastes jeux de données fiables. Par conséquent, ils sont pertinents pour la réalisation de la cible 9.b, qui consiste à soutenir la recherche-développement et l'innovation technologiques dans les pays en développement.

C. Champ d'application

12. La Loi type s'applique à l'utilisation et à la reconnaissance internationale de la gestion de l'identité et des services de confiance dans le cadre d'activités commerciales et de services touchant au commerce. Les États adoptants peuvent par ailleurs décider d'étendre son champ d'application aux activités non commerciales.

13. De nombreux textes législatifs différents peuvent être pertinents pour les échanges de données. La Loi type n'a pas d'incidences sur les lois existantes, notamment celles applicables à la protection et à la confidentialité des données. Elle n'introduit pas non plus l'obligation d'utiliser des services de gestion de l'identité ou des services de confiance, ni un service de gestion de l'identité ou un service de confiance particulier, et n'a pas d'incidence sur une exigence à cet effet (voir par. 106 à 108 ci-dessous).

14. Les dispositions relatives à la gestion de l'identité de la Loi type s'appliquent à l'identification des personnes physiques et morales. Les dispositions relatives aux services de confiance s'appliquent à toutes les informations qui se présentent sous la forme de messages de données. Les deux séries de dispositions s'appliquent indépendamment de la nature privée ou publique du prestataire de services, de l'abonné et de la partie utilisatrice.

D. Structure

15. La Loi type comprend quatre chapitres, traitant respectivement des dispositions générales, de la gestion de l'identité, des services de confiance et de la reconnaissance internationale. Les chapitres I et IV s'appliquent à la fois à la gestion de l'identité et aux services de confiance. Par ailleurs, la structure et le contenu des chapitres II et III présentent d'importantes analogies. Par conséquent, les précisions données sur une disposition du chapitre II peuvent être pertinentes pour la disposition correspondante du chapitre III, dans la mesure où les dispositions coïncident. Cette remarque vaut particulièrement pour les articles 13, 14, 15, 22, 23 et 24, qui correspondent aux articles 5, 6, 7, 8, 10, 11 et 12.

16. Le chapitre premier contient les définitions de certains termes utilisés dans la Loi type ; délimite le champ d'application ; contient des dispositions relatives à l'utilisation volontaire des services de gestion de l'identité et des services de confiance, y compris de services particuliers ; définit la relation entre la Loi type 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 de la Loi type compte tenu de son caractère uniforme et de son origine internationale, notamment en cas de lacunes.

17. 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 de ces prestataires. L'article 5 établit les principes de la reconnaissance juridique de la gestion de l'identité et de la non-discrimination à l'égard de l'identification électronique. L'article 6 énonce les principales obligations qui incombent aux prestataires de services de gestion de l'identité, qui correspondent

aux éléments de base des systèmes de gestion de l'identité et aux 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 énonce une règle d'équivalence fonctionnelle entre l'identification hors ligne et l'identification effectuée au moyen de la gestion de l'identité, qui exige l'utilisation d'une méthode fiable. La fiabilité de la méthode est évaluée au moyen d'une détermination *ex post* effectuée sur la base des circonstances visées à l'article 10 ou au moyen d'une désignation *ex ante* effectuée conformément à l'article 11. Enfin, l'article 12 traite de la responsabilité des prestataires de services de gestion de l'identité.

18. Le chapitre III définit les 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 remplies par certains services de confiance mentionnés (signatures électroniques, cachets électroniques, horodatages électroniques, archivage électronique, services d'envoi recommandé électroniques et authentification de sites Web) et les exigences qui y sont associées, y compris 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, comme certains services de confiance n'ont pas d'équivalent papier, une règle d'équivalence fonctionnelle n'est pas systématiquement requise. 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 traite de la responsabilité des prestataires de services de confiance.

19. 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 de la Loi type. Cette dernière n'envisage pas la création d'un organisme qui serait chargé d'accorder cette reconnaissance, mais prévoit plusieurs mécanismes en se fondant sur une approche décentralisée. Outre les articles 25 à 27, les dispositions spécifiques des articles 10-3, 11-4, 22-3 et 23-4, relatives à la non-discrimination à l'égard de l'origine 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 pertinentes. Les accords contractuels peuvent également être pertinents pour l'utilisation de la gestion de l'identité et des services de confiance à l'échelle internationale.

E. Généralités

1. Historique

20. La Loi type trouve son origine dans une demande formulée par la Commission à sa quarante-huitième session, en 2015. À cette session, la Commission avait prié le secrétariat de mener des travaux préparatoires sur les aspects juridiques de la gestion de l'identité et des services de confiance, y compris en organisant des colloques et des réunions d'experts, en vue des travaux que le Groupe de travail IV (Commerce électronique) pourrait réaliser à ce sujet. Elle l'avait aussi prié de communiquer les résultats de ces travaux préparatoires au Groupe de travail afin d'obtenir des recommandations sur la portée exacte, la méthodologie et les priorités qui pourraient être envisagées, recommandations qu'elle examinerait par la suite[16].

21. Comme suite à cette demande, la Commission était saisie, à sa quarante-neuvième session, en 2016[17], d'une note du Secrétariat portant sur les questions juridiques liées à la gestion de l'identité et aux services de confiance (A/CN.9/891), qui résumait les débats tenus pendant le colloque de la CNUDCI organisé sur ce thème à Vienne les 21 et 22 avril 2016. Elle est convenue que les questions de la gestion de l'identité et des services de confiance devaient rester inscrites au programme du Groupe de travail[18].

22. Conformément au mandat reçu de la Commission, le Groupe de travail a tenu des discussions préliminaires sur le sujet lors de sa cinquante-quatrième session, qui s'est tenue à Vienne du 31 octobre au 4 novembre 2016. Il est convenu que ses travaux futurs sur la gestion de l'identité et les services de confiance devraient se limiter à l'utilisation commerciale des systèmes de gestion de l'identité et englober les prestataires de services de gestion de l'identité tant privés que publics. Il est également convenu que, même si les travaux pouvaient s'attacher à la gestion de l'identité en premier lieu, puis aux services de confiance en deuxième lieu, les termes pertinents pour ces deux domaines devraient être déterminés et définis simultanément étant donné que les deux sujets étaient étroitement liés. Enfin, il est convenu de mettre l'accent sur les systèmes de gestion de l'identité multipartites et sur l'identification des personnes physiques et morales, et de poursuivre ses travaux en précisant plus avant les objectifs et la portée du projet, en recensant les principes généraux applicables et en élaborant les définitions nécessaires (A/CN.9/897, par. 118 à 120 et 122).

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

[17] Ibid., *soixante et onzième session, Supplément n° 17* (A/71/17), par. 228 et 229.

[18] Ibid., par. 235 et 236.

23. Conformément à ses décisions antérieures, le Groupe de travail a notamment examiné, à sa cinquante-cinquième session (New York, 24-28 avril 2017), les objectifs et la portée de ses travaux sur la gestion de l'identité et les services de confiance, ainsi que les principes généraux applicables (A/CN.9/902, par. 29 à 85).

24. À sa cinquantième session, en 2017, la Commission a réaffirmé le mandat confié au Groupe de travail (voir par. 20 ci-dessus) et a demandé au secrétariat d'envisager de convoquer des réunions de groupes d'experts. Les États et les organisations internationales ont été invités à partager leurs connaissances[19]. Le secrétariat a ainsi convoqué une réunion d'experts consacrée aux aspects juridiques de la gestion de l'identité et des services de confiance, qui s'est tenue à Vienne les 23 et 24 novembre 2017.

25. Se fondant sur les conclusions de la réunion d'experts, le Groupe de travail a estimé, à sa cinquante-sixième session (New York, 16-20 avril 2018), qu'il serait pertinent d'examiner, dans le cadre des débats sur les aspects juridiques de la gestion de l'identité et des services de confiance, les questions ci-après : portée des travaux ; principes généraux ; définitions ; exigences et mécanismes de reconnaissance mutuelle ; certification des services de gestion de l'identité et des services de confiance ; niveaux de garantie pour la gestion de l'identité et les services de confiance ; responsabilité ; mécanismes de coopération institutionnelle ; transparence ; obligation d'identification ; conservation des données ; et surveillance des prestataires de services (A/CN.9/936, par. 61 à 94).

26. Sur la recommandation du Groupe de travail (A/CN.9/936, par. 95), la Commission, à sa cinquante et unième session, en 2018, a prié celui-ci de travailler à l'élaboration d'un texte destiné à faciliter la reconnaissance internationale de la gestion de l'identité et des services de confiance, sur la base des principes qu'il avait établis et des questions qu'il avait recensées (voir par. 25 ci-dessus)[20].

27. En conséquence, le Groupe de travail a poursuivi l'examen des questions qu'il avait recensées (A/CN.9/965, par. 10 à 129) à sa cinquante-septième session, qui s'est tenue à Vienne du 19 au 23 novembre 2018.

28. Un premier projet de dispositions sur la reconnaissance internationale de la gestion de l'identité et des services de confiance (A/CN.9/WG.IV/WP.157), accompagné de remarques explicatives (A/CN.9/WG.IV/WP.158), a été soumis au Groupe de travail, afin qu'il l'examine à sa cinquante-huitième session (New York, 8-12 avril 2019). Il a examiné les projets de dispositions portant sur le champ d'application, la reconnaissance et la fiabilité des systèmes de gestion de l'identité et des services de confiance, les types de services de confiance visés, et les obligations et responsabilités des prestataires de services de gestion de l'identité et de services de confiance (A/CN.9/971, par. 13 à 153).

[19] Ibid., *soixante-douzième session, Supplément n° 17* (A/72/17), par. 127.
[20] Ibid., *soixante-treizième session, Supplément n° 17* (A/73/17), par. 159.

29. À ladite session, le Groupe de travail a demandé au secrétariat d'élaborer, en consultation avec des experts, des propositions concrètes sur les questions relatives à la fiabilité des systèmes de gestion de l'identité (A/CN.9/971, par. 67). Pour donner suite à cette demande, le secrétariat a convoqué à Vienne, les 22 et 23 juillet 2019, une réunion d'experts chargée d'examiner les normes et procédures qu'un système de gestion de l'identité devrait respecter pour être reconnu légalement ainsi que d'autres questions contenues dans le projet de dispositions, notamment la fiabilité des systèmes de gestion de l'identité et les obligations et responsabilités des prestataires de services de gestion de l'identité.

30. À sa cinquante-deuxième session, en 2019, la Commission a salué les progrès effectués par le Groupe de travail[21]. Par ailleurs, elle a noté qu'il faudrait que celui-ci s'emploie à élaborer un instrument qui pourrait s'appliquer à l'utilisation de la gestion de l'identité et des services de confiance à l'échelle tant interne qu'internationale, et que les résultats des travaux menés auraient des incidences sur certaines questions qui sortaient du cadre des transactions commerciales[22].

31. À sa cinquante-neuvième session, qui s'est tenue à Vienne du 25 au 29 novembre 2019, le Groupe de travail était saisi d'un projet révisé de dispositions (A/CN.9/WG.IV/WP.160), qui tenait compte des résultats des consultations menées avec des experts (voir par. 29 ci-dessus). Il a procédé à une lecture complète du projet de texte, en s'attachant plus particulièrement aux dispositions relatives aux services de confiance (A/CN.9/1005, par. 10 à 122). Il a également tenu des discussions préliminaires sur la forme de l'instrument, dont s'est dégagée une nette préférence en faveur de l'élaboration d'une loi type, plutôt que d'une convention (ibid., par. 123).

32. À sa cinquante-troisième session, en 2020, la Commission s'est à nouveau déclarée satisfaite des progrès réalisés par le Groupe de travail et a confirmé que ce dernier devrait poursuivre l'élaboration d'une loi type portant sur les questions juridiques liées à la gestion de l'identité et aux services de confiance[23].

33. Ayant été saisi d'un deuxième projet révisé de dispositions (A/CN.9/WG.IV/WP.162), le Groupe de travail a procédé à une lecture complète de ces dispositions (A/CN.9/1045, par. 16 à 138) à sa soixantième session, tenue à Vienne du 19 au 23 octobre 2020. Par ailleurs, il a accepté la possibilité de tenir des consultations informelles pour discuter des points en suspens.

34. Du 15 au 17 mars 2021, des consultations informelles ont ainsi été organisées à distance avec des représentants et des observateurs pour examiner les points suivants : responsabilité, relation du projet de dispositions avec les textes existants de

[21] Ibid., *soixante-quatorzième session, Supplément n° 17* (A/74/17), par. 175.

[22] Ibid., par. 172.

[23] Ibid., *soixante-quinzième session, Supplément n° 17* (A/75/17), deuxième partie, par. 41 et 51 d).

la CNUDCI, reconnaissance internationale, ainsi que définitions et autres questions terminologiques.

35. Le Groupe de travail a été informé du résultat des consultations informelles à sa soixante et unième session, tenue à New York du 6 au 9 avril 2021. Compte tenu des limites associées au format hybride de la session (notamment la réduction du temps de réunion), il a axé l'examen du troisième projet révisé de dispositions (A/CN.9/WG.IV/WP.167) sur les questions examinées lors de ces consultations (A/CN.9/1051, par. 13 à 67).

36. À sa cinquante-quatrième session, en 2021, la Commission a appris que, malgré la réduction du temps de réunion, le Groupe de travail avait beaucoup progressé dans la mise au point de l'instrument. Elle s'est déclarée satisfaite de ces progrès et a encouragé le Groupe de travail à terminer ses travaux et à lui en présenter les résultats, afin qu'elle les examine à sa cinquante-cinquième session, en 2022[24].

37. À sa soixante-deuxième session, tenue à Vienne du 22 au 26 novembre 2021, le Groupe de travail a procédé à une nouvelle lecture du projet de dispositions (A/CN.9/1087, par. 12 à 114), en se fondant sur un projet révisé de dispositions (A/CN.9/WG.IV/WP.170), accompagné d'une note explicative (A/CN.9/WG.IV/WP.171). Il a prié le secrétariat de réviser le projet de dispositions et le projet de note explicative en tenant compte de ses délibérations et décisions et de communiquer le texte ainsi modifié à la Commission, sous la forme d'une loi type, afin qu'elle l'examine à sa cinquante-cinquième session, en 2022. Le secrétariat a été prié de communiquer le texte révisé à tous les gouvernements et aux organisations internationales compétentes, afin qu'ils fassent part de leurs observations, et de compiler les observations reçues en vue d'un examen par la Commission (A/CN.9/1087, par. 11). Toujours à sa soixante-deuxième session, le Groupe de travail est convenu que certaines questions en suspens seraient examinées dans le cadre de consultations informelles intersessions et que le secrétariat devrait lui faire rapport à ce sujet à sa soixante-troisième session, en vue de la poursuite des débats (A/CN.9/1087, par. 113).

38. À sa soixante-troisième session, tenue à New York du 4 au 8 avril 2022, le Groupe de travail a entendu le rapport en question et s'est penché sur les questions en suspens (A/CN.9/1093, par. 14 à 44). Lors de cette session, l'avis a été exprimé que d'autres questions importantes étaient également en suspens. Aucune décision n'a été prise sur les questions en suspens et les délégations ont de nouveau été invitées à soumettre à la Commission des commentaires sur ces questions.

39. À sa cinquante-cinquième session, en 2022, la Commission a examiné le texte du projet de loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance et de la note explicative y relative

[24] Ibid., *soixante-seizième session, Supplément n° 17* (A/76/17), chap. IX.

(A/CN.9/1112, annexes I et II), qui tenait compte des discussions et délibérations tenues par le Groupe de travail jusqu'à sa soixante-deuxième session, ainsi qu'une compilation des commentaires reçus des États et des organisations internationales compétentes (A/CN.9/1113 et A/CN.9/1113/Add.1).

40. La Commission a constitué un Comité plénier chargé d'examiner le projet de loi type (A/77/17, par. 13). À sa 1170e séance, le 7 juillet 2022, elle a examiné et adopté le rapport du Comité plénier, adopté par consensus la Loi type et approuvé en principe la note explicative y relative (A/77/17, par. 149). Elle a également demandé au secrétariat de parachever la note explicative en tenant compte des délibérations qu'elle avait tenues et des décisions qu'elle avait prises à sa cinquante-cinquième session, et a autorisé le Groupe de travail à examiner, à sa soixante-quatrième session, les parties de la note explicative concernées par ces délibérations et décisions (ibid.). Le Groupe de travail a revu ces parties en conséquence (A/CN.9/1125, par. 91 à 100).

2. Relation avec les textes existants de la CNUDCI

41. Les textes antérieurs de la CNUDCI ne traitent pas des services de confiance. Cependant, ils contiennent des règles d'équivalence fonctionnelle qui peuvent être pertinentes pour certains services de confiance. L'article 7 de la Loi type de la CNUDCI sur le commerce électronique[25], l'article 6 de la Loi type de la CNUDCI sur les signatures électroniques[26], l'article 9-3 de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux[27] et l'article 9 de la Loi type de la CNUDCI sur les documents transférables électroniques[28] énoncent les exigences auxquelles les signatures électroniques doivent satisfaire pour être fonctionnellement équivalentes aux signatures papier. Ces dispositions exigent l'identification du signataire, ce qui peut impliquer le recours à l'identification électronique et, de manière plus générale, à la gestion de l'identité. L'article 16 de la Loi type se fonde sur l'article 9 de la Loi type sur les documents transférables électroniques.

42. De même, l'article 19 de la Loi type se fonde sur l'article 10-1 de la Loi type sur le commerce électronique, qui énonce les règles d'équivalence fonctionnelle applicables à la conservation des données. D'autres dispositions de la CNUDCI qui ont été utilisées comme sources d'articles de la Loi type sont mentionnées dans le commentaire relatif à l'article concerné. Toutefois, il n'est pas nécessaire d'avoir recours à un service de

[25] *Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation 1996, avec le nouvel article 5* bis *tel qu'adopté en 1998* (1999), publication des Nations Unies, numéro de vente : F.99.V.4.

[26] *Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation (2001)*, publication des Nations Unies, numéro de vente : F.02.V.8.

[27] Nations Unies, *Recueil des Traités*, vol. 2898, n° 50525.

[28] *Loi type de la CNUDCI sur les documents transférables électroniques*, publication des Nations Unies (2018).

confiance mentionné dans la Loi type pour satisfaire aux règles d'équivalence fonctionnelle énoncées dans des textes antérieurs de la CNUDCI.

43. Plusieurs questions pertinentes pour la Loi type, telles que l'évaluation de la fiabilité, la responsabilité et les mécanismes de reconnaissance internationale, ont été examinées en détail dans un document d'orientation consacré à l'utilisation internationale des signatures électroniques[29].

F. Concepts et principes fondamentaux

44. La présente section explique plusieurs concepts et principes fondamentaux qui sous-tendent la Loi type. Les termes définis dans la Loi type sont expliqués plus avant dans le commentaire sur l'article premier ci-dessous, tandis qu'une liste plus exhaustive de termes et notions 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

45. Tout comme certains textes antérieurs de la CNUDCI, la Loi type 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 certaines modifications (A/CN.9/902, par. 52 et 63).

46. Le principe de l'autonomie des parties permet aux parties à un contrat de choisir les règles applicables, dans les limites du droit impératif. Il reconnaît que ces parties sont peut-être les mieux placées pour déterminer les règles qui sont les mieux adaptées à une transaction donnée.

47. Le principe de la non-discrimination, formulé pour la première fois à l'article 5 de la Loi type sur le commerce électronique et connu également sous le nom de principe de la reconnaissance juridique, garantit qu'une information n'est pas privée de ses effets juridiques, de sa validité ou de sa force exécutoire au seul motif qu'elle se présente sous forme électronique.

[29] *Promouvoir la confiance dans le commerce électronique : questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques*, publication des Nations Unies, numéro de vente : F.09.V.4.

48. Le principe de la neutralité technologique garantit que la loi n'impose pas, ni ne favorise, l'utilisation d'une technologie ou d'une méthode particulière, ce qui permet aux lois de résister à l'épreuve du temps. La neutralité technologique est nécessaire pour assurer l'interopérabilité, indispensable aux flux de données. Ce principe trouve son fondement juridique dans la définition large du « message de données », énoncée pour la première fois à l'article 2 a de la Loi type sur le commerce électronique, qui vise à englober toutes les technologies existantes et futures.

49. Le principe de l'équivalence fonctionnelle définit les critères en vertu desquels les transactions électroniques sont réputées satisfaire aux exigences de forme applicables aux documents papier, comme l'exigence tendant à ce qu'un document soit écrit, original ou signé. Ce principe présuppose l'existence d'exigences légales qui prévoient directement ou indirectement l'exécution d'une opération physique ou sur papier, telle que l'utilisation de justificatifs papier pour identifier une personne. Il exige ensuite que soient analysés les objectifs et les fonctions de ces exigences en vue de déterminer comment atteindre ces objectifs ou remplir ces fonctions par des moyens électroniques.

50. Bien que la Loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance ne les énonce pas expressément, ces principes généraux encadrent les principales dispositions du texte. Le principe de l'autonomie des parties est contenu à l'article 3, et le principe de la non-discrimination, tel qu'il s'applique à la gestion de l'identité et aux services de confiance, est contenu aux articles 5 et 13, respectivement. En outre, le principe de l'équivalence fonctionnelle sous-tend l'article 9, sur l'identification effectuée au moyen de la gestion de l'identité, et les articles 16 à 21, consacrés à certains services de confiance mentionnés dans la Loi type. Toutefois, il se peut que certains des services de confiance visés par la Loi type n'aient pas d'équivalent papier. Le principe de l'équivalence fonctionnelle ne leur serait donc pas applicable.

2. Gestion de l'identité

51. L'identification est le processus qui consiste à distinguer de manière unique une personne parmi d'autres dans un contexte particulier, sur la base d'informations la concernant (à savoir des attributs). Ces informations peuvent être recueillies ou observées. L'identification consiste à vérifier que les attributs recueillis ou observés correspondent à une « identité » préalablement établie pour la personne identifiée. Ainsi, elle est souvent effectuée lorsqu'une personne invoque une identité particulière et présente des attributs en vue de sa vérification.

52. L'identification est particulièrement importante pour instaurer la confiance dans les opérations en ligne[30]. Elle consiste essentiellement à vérifier que les attributs recueillis ou observés correspondent à une « identité » préalablement établie pour la personne identifiée (on parle de « confirmation d'identité » lorsqu'il s'agit d'établir l'identité unique d'une personne ; et d'« identification électronique », ou d'« authentification » dans certains pays, lorsqu'il s'agit de vérifier a posteriori des justificatifs attestant de cette identité dans une opération particulière).

53. Par conséquent, la Loi type distingue deux étapes (ou phases) dans la gestion de l'identité : tout d'abord, la délivrance de justificatifs d'identité, c'est-à-dire de données qui peuvent être présentées à des fins d'identification électronique ; ensuite, la présentation et la vérification de ces justificatifs par des moyens électroniques pour une transaction donnée (c'est-à-dire l'identification électronique) :

a) La première étape de la gestion de l'identité consiste à recueillir les attributs qui peuvent constituer l'« identité fondamentale » d'une personne c'est-à-dire les attributs de base qui sont généralement enregistrés par des organismes publics dans les registres et statistiques de l'état civil ou dans les systèmes d'identification fondamentale 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 ou reconnus par les administrations publiques (par exemple, un certificat d'enregistrement) et vérifiés auprès de l'organisme émetteur. La mesure dans laquelle un justificatif peut être reconnu dépend de l'objet pour lequel celui-ci a été émis. Ce processus, qui peut être exécuté par des moyens électroniques ou 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 les présentant est bien celle à laquelle ceux-ci ont été délivrés lors de la première étape.

54. 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 délivrés et les moyens employés 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, un système de gestion de l'identité peut proposer différents services. Les parties (c'est-à-dire la partie qui cherche à identifier et celle qui cherche à être identifiée) peuvent sélectionner le service approprié en fonction de leurs besoins.

[30] Banque mondiale, *Rapport sur le développement dans le monde 2021 : « Des données au service d'une vie meilleure »* (Washington, 2021).

55. Les systèmes de gestion de l'identité peuvent être exploités par des entités publiques ou privées. Dans la pratique, les systèmes publics correspondent généralement à un service unique de gestion de l'identité, tandis que les systèmes privés peuvent correspondre à plusieurs services offrant différents niveaux de fiabilité. Les systèmes de gestion de l'identité peuvent aussi être classés en fonction de leur caractère centralisé ou décentralisé. En application du principe de la neutralité technologique (voir par. 48 ci-dessus), la Loi type ne présuppose pas l'utilisation d'une technologie ou d'un modèle particulier et peut donc s'appliquer à tous les types de systèmes et de services de gestion de l'identité.

56. 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 participant puissent être compris et reconnus par toutes les parties utilisatrices participantes. Cet arrangement est connu sous le nom de « fédération d'identité » et les règles du système, qui sont de nature contractuelle, sous le nom de « 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 peut contribuer à réduire les coûts et, partant, à assurer la viabilité à long terme du système.

3. Services de confiance

57. Les services de confiance sont des services en ligne qui fournissent des garanties quant à certaines caractéristiques des messages de données, telles que l'origine, l'intégrité et le moment où une action précise est exécutée en relation avec ces données. Les garanties relatives à la qualité des données sont essentielles pour établir la confiance dans les échanges de données, qui constituent le pilier du commerce numérique. La Loi type mentionne un certain nombre de services de confiance couramment utilisés, tout en reconnaissant qu'il peut en exister d'autres ou que d'autres services pourraient être mis au point à l'avenir.

58. La notion de service de confiance telle qu'employée dans la Loi type vise la prestation d'un service plutôt que le service lui-même. Par exemple, une signature électronique peut être apposée au moyen d'un service qui utilise des méthodes pour créer et gérer les signatures électroniques. Pour éviter les doutes, chaque disposition de la Loi type précise si elle s'intéresse aux méthodes utilisées pour la prestation du service de signature électronique, ou à la signature électronique qui résulte de l'application de ce service.

4. Évaluation de la fiabilité

59. Conformément aux textes antérieurs de la CNUDCI, plusieurs dispositions de la Loi type font référence à l'utilisation d'une méthode fiable pour la fourniture de services de gestion de l'identité et de services de confiance. La Loi type prévoit deux mécanismes pour déterminer la fiabilité de la méthode : les articles 10 et 22 fournissent des listes indicatives de facteurs pertinents pour déterminer la fiabilité, tandis que les articles 11 et 23 prévoient un mécanisme pour désigner des méthodes fiables.

a) Désignation *ex ante* de services fiables

60. Pour évaluer la fiabilité d'une méthode, on peut procéder à une évaluation « *ex ante* », c'est-à-dire précédant l'utilisation de la méthode, en se fondant sur une liste de circonstances prédéterminées, et ce de manière générale et non par référence à une opération particulière. La Loi type parle à ce sujet de désignation de services fiables et énumère aux articles 11 (applicable aux services de gestion de l'identité) et 23 (applicable aux services de confiance) les exigences relatives à cette désignation, qui incluent les mêmes circonstances que celles s'appliquant à la détermination de la fiabilité.

61. La désignation ne vise alors pas des types génériques de services de gestion de l'identité et de services de confiance ni l'ensemble des services de gestion de l'identité et des services de confiance offerts par un prestataire particulier, mais plutôt un service déterminé fourni par un prestataire de services donné.

62. Cette approche *ex ante* offre plus de sécurité juridique et de prévisibilité en ce qui concerne les effets juridiques des services de gestion de l'identité et des services de confiance, y compris lorsqu'ils sont utilisés à l'échelle internationale, par le biais des présomptions et du renversement de la charge de la preuve. En règle générale, les méthodes utilisées pour fournir les services désignés sont présumées fiables, ce qui dispense la partie concernée de prouver leur fiabilité et transfère cette charge à la partie qui allègue leur manque de fiabilité. Toutefois, le fonctionnement de ce mécanisme *ex ante* présuppose l'existence d'un mécanisme institutionnel, c'est-à-dire d'une entité compétente pour administrer le processus de désignation.

63. L'État adoptant qui souhaite appliquer l'approche *ex ante* doit déterminer l'entité qui sera chargée de la désignation, laquelle peut être un organisme privé ou public. Ces entités peuvent être accréditées conformément aux normes techniques applicables aux organismes qui certifient les produits, processus et services. La certification (y compris l'autocertification) est utile pour évaluer les services sur la base de normes axées sur les résultats et peut donc être pertinente pour leur désignation.

64. La Loi type présuppose l'existence du mécanisme institutionnel nécessaire à la mise en œuvre de l'approche *ex ante* mais ne contient pas de dispositions relatives à sa mise en place ou à son administration. Ce mécanisme doit comprendre divers éléments tels que les critères d'évaluation des services, les détails du processus d'évaluation utilisé dans la prise de décisions et les sources de financement. En fonction de plusieurs facteurs, notamment des dispositifs institutionnels, la gouvernance de ce mécanisme peut être complexe et coûteuse. Pour cette raison, on pourra privilégier la désignation pour les services qui offrent un niveau de garantie et de fiabilité plus élevé et qui sont donc utilisés pour des opérations de valeur supérieure.

65. Le mécanisme de désignation devrait pouvoir rapidement s'adapter à toute évolution technologique afin de ne pas entraver l'innovation. Autrement, on risque la discrimination à l'égard de services de gestion de l'identité et de services de confiance qui, bien que disponibles et fondés sur des méthodes fiables, n'ont pas été pas désignés. Par ailleurs, le fait de préciser plus avant les conditions de désignation ne devrait pas conduire à l'imposition d'exigences spécifiques à une technologie.

b) Détermination *ex post* de la fiabilité

66. Une autre approche possible pour évaluer la fiabilité d'une méthode consiste à différer ladite évaluation jusqu'au moment où un éventuel différend éclate au sujet de cette fiabilité. Dans ce cas, l'évaluation intervient après l'utilisation de la méthode (« *ex post* »). La Loi type désigne cette approche par l'expression « détermination de la fiabilité » et énumère aux articles 10 (applicable aux services de gestion de l'identité) et 22 (applicable aux services de confiance) les exigences y relatives, y compris en dressant des listes non exhaustives de circonstances pertinentes.

67. L'approche *ex post* permet donc de manière générale de réaliser des opérations de gestion de l'identité sans procéder à une évaluation préalable de la fiabilité, et limite la nécessité d'évaluer celle-ci aux cas réels de litiges. Elle offre également aux parties une grande souplesse dans le choix de technologies et de méthodes. En outre, elle peut être gérée de manière décentralisée et ne requiert pas la mise en place d'un mécanisme institutionnel, évitant ainsi les coûts susceptibles d'en découler.

68. Toutefois, l'approche *ex post* ne permet pas de prévoir avec exactitude la validité de la méthode employée avant son utilisation effective, ce qui expose les parties au risque de non-fiabilité de la méthode. De plus, la détermination de la fiabilité fait l'objet d'une décision prise par un tiers, processus qui peut prendre du temps et ne garantit pas la cohérence des décisions rendues.

c) Approche combinée

69. La Loi type associe les mécanismes de la détermination et de la désignation, et permet ainsi la reconnaissance de tout service de gestion de l'identité et tout service de confiance, tout en fournissant des indications sur les services qui offrent un degré plus élevé de confiance quant à leur fiabilité (approche à deux niveaux). Ce faisant, elle ne favorise pas un mécanisme par rapport à l'autre, mais cherche à combiner les avantages des deux mécanismes tout en minimisant leurs inconvénients respectifs et à créer les conditions requises pour la solution retenue par les parties.

70. Les textes de la CNUDCI 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. L'approche combinée adoptée dans la Loi type se fonde sur les articles 6 et 7 de la Loi type sur les signatures électroniques.

5. Questions de responsabilité

71. Le régime de responsabilité peut avoir une incidence importante sur la promotion de l'utilisation de la gestion de l'identité et des services de confiance et constitue un élément central de la Loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance. Par le passé, les législateurs ont adopté différentes solutions, qui vont de l'absence de régime de responsabilité spécifique à l'adoption de dispositions relatives aux normes de conduite et aux règles de responsabilité applicables soit aux seuls prestataires de services, soit à toutes les parties concernées (prestataires de services, abonnés et parties utilisatrices)[31]. C'est cette dernière approche qui a été adoptée dans la Loi type sur les signatures électroniques[32].

72. Les responsabilités relatives aux services de gestion de l'identité et aux services de confiance sont principalement réparties par voie contractuelle ou législative. On peut préférer la seconde voie afin d'empêcher les parties d'exclure certaines dispositions par voie contractuelle. De plus, les règles établies par la loi peuvent s'appliquer en l'absence d'accord contractuel, c'est-à-dire à l'égard des parties utilisatrices.

73. Les articles 12 et 24 établissent un régime de responsabilité uniforme des prestataires de services à l'égard des abonnés et des parties utilisatrices, selon lequel le prestataire de services doit être tenu responsable des conséquences de tout manquement à l'obligation de fournir ses services conformément à la loi. Ces articles établissent par conséquent un fondement légal de la responsabilité qui fonctionne

[31] *Promouvoir la confiance dans le commerce électronique*, par. 175.

[32] Pour plus d'informations, voir *Guide pour l'incorporation de la Loi type de la CNUDCI sur les signatures électroniques (2001)*, par. 77 à 81.

en parallèle à la responsabilité contractuelle et extracontractuelle. Par ailleurs, la Loi type permet aux prestataires de services de limiter leur responsabilité à l'égard tant des abonnés que des parties utilisatrices, sous certaines conditions. L'État adoptant peut autoriser de telles limitations, qui ne sauraient toutefois être contraires à sa législation sur l'ordre public.

74. La Loi type ne traite ni du degré de faute requis pour engager la responsabilité, ni du type et du montant des dommages-intérêts susceptibles d'être recouvrés[33]. Les règles ordinaires de l'État adoptant s'appliqueront donc à ces questions si aucune règle spéciale applicable aux prestataires de services de gestion de l'identité et de services de confiance n'a été adoptée lors de l'incorporation de la Loi type dans le droit interne.

6. Reconnaissance internationale

75. La dimension internationale est essentielle à l'utilisation des services de gestion de l'identité et des services de confiance et, plus généralement, des opérations électroniques. Deux types d'obstacles peuvent toutefois entraver cette utilisation : les incompatibilités techniques entraînant un manque d'interopérabilité, et les obstacles juridiques à la reconnaissance internationale[34].

76. Les obstacles juridiques peuvent découler d'approches contradictoires adoptées par les États, notamment lorsque la loi impose ou favorise une technologie, une méthode ou un produit particulier. Dans ce cas, les exigences légales imposées à l'échelle nationale peuvent empêcher la reconnaissance des types de services de gestion de l'identité et de services de confiance jugés non conformes. En outre, l'émergence de normes techniques nationales – qui peut également découler de l'approche « à deux niveaux », lorsque ces normes sont associées à des présomptions juridiques – peut conduire à l'existence d'exigences disparates, qui ont également pour effet d'entraver l'utilisation internationale de ces services.

77. La facilitation, sur le plan légal, de l'utilisation internationale de la gestion de l'identité et des services de confiance est l'un des principaux objectifs de la Loi type. Pour ce faire, elle applique les principes de la neutralité technologique et de la non-discrimination à l'égard de l'origine géographique[35], qui sous-tendent les articles 10-3, 11-4, 22-3 et 23-4 de la Loi type. En outre, le chapitre IV traite spécifiquement des

[33] Sur ces questions, voir *Promouvoir la confiance dans le commerce électronique*, par. 177 à 193 (fondement de la responsabilité : négligence ordinaire, présomption de négligence et responsabilité objective) et par. 194 à 201 (parties en droit de réclamer réparation et étendue de celle-ci).

[34] *Promouvoir la confiance dans le commerce électronique*, par. 137 à 152.

[35] La publication *Promouvoir la confiance dans le commerce électronique* (par. 149) notait déjà que les principes de la neutralité technologique et de la non-discrimination à l'égard des signatures et des services étrangers sous-tendaient le consensus qui se dégageait au sujet des mécanismes juridiques nécessaires à la reconnaissance internationale des signatures électroniques.

questions liées à la reconnaissance internationale. En conséquence, la Loi type non seulement décourage l'adoption de législations axées sur une technologie particulière, mais aussi encourage l'élaboration de normes techniques interopérables, notamment par le biais de la coopération.

78. La Loi type, conformément à l'approche adoptée dans certains textes antérieurs de la CNUDCI, ne se contente pas de mentionner le lieu d'origine comme étant un facteur pertinent pour accorder la reconnaissance juridique aux services de gestion de l'identité et aux services de confiance étrangers. Plus précisément, elle exige une détermination *ex post* de la fiabilité des services étrangers effectuée sur la base des mêmes circonstances que celles qui s'appliquent aux services similaires fournis au niveau national. Elle prévoit également des mécanismes permettant de désigner *ex ante* des services de gestion de l'identité et des services de confiance étrangers fiables sur la base des mêmes circonstances que celles qui s'appliquent aux services similaires fournis au niveau national. En résumé, c'est la fiabilité technique, plutôt que le lieu d'origine, qui devrait déterminer si la reconnaissance juridique doit être accordée.

79. La Loi type 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 la Loi type comme modèle pour établir un dispositif institutionnel avec des partenaires internationaux, notamment dans le cadre d'un accord spécifique.

80. Les chapitres consacrés au commerce électronique figurant dans les accords de libre-échange contiennent généralement des dispositions sur les signatures électroniques ou d'autres formes d'identification électronique, souvent appelées « méthodes d'authentification », et exigent de plus en plus la reconnaissance mutuelle des méthodes d'identification électronique. De leur côté, les accords sur l'économie numérique comportent un module consacré à l'identité numérique qui vise à permettre l'interopérabilité au plan international. L'incorporation de la Loi type dans le droit interne peut faciliter la mise en œuvre de ces dispositions contenues dans les accords de libre-échange et les accords sur l'économie numérique.

II. Commentaire par article

Chapitre premier. Dispositions générales

Article premier. Définitions

81. L'article premier contient des définitions de termes utilisés dans la Loi type.

Attribut

82. 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 peuvent être notamment la raison sociale, le siège social, le nom d'enregistrement et le pays d'enregistrement. La notion d'attribut est utilisée dans la définition du terme « identité ».

83. Les attributs peuvent contenir des données personnelles dont le traitement est soumis à la loi sur la confidentialité et la protection des données. La Loi type ne traite pas de ces sujets et préserve expressément l'application de cette loi.

Référence

A/CN.9/WG.IV/WP.150, par. 13.

Message de données

84. La définition du terme « message de données » se retrouve dans tous les textes existants de la CNUDCI sur le commerce électronique, où elle est utilisée pour mettre en œuvre le principe de la neutralité technologique (voir par. 48 ci-dessus). Ce terme est le principal point de référence pour définir les exigences relatives aux services de confiance puisque l'utilisation d'un tel service permet de fournir des garanties quant aux caractéristiques d'un message de données.

Référence

A/CN.9/1045, par. 40.

Identification électronique

85. Par « identification électronique », on entend la vérification du lien entre l'identité prétendue d'une personne physique ou morale et les justificatifs présentés, ce qui constitue la seconde étape de la gestion de l'identité. Ce terme a été retenu plutôt que le terme « authentification » pour répondre aux préoccupations concernant les multiples significations données à ce dernier. Du point de vue technique, le terme « authentification » désigne la présentation d'une preuve de l'identité.

86. La divulgation du nom de la personne physique ou morale peut ne pas être nécessaire pour satisfaire aux exigences en matière d'identification électronique lorsque la vérification d'autres attributs est suffisante. C'est conforme à l'approche adoptée dans des textes antérieurs de la CNUDCI, notamment la Loi type sur les signatures électroniques, selon laquelle, « aux fins de la définition du terme « signature électronique » dans la Loi type, le terme « identification » [peut] être plus large que la simple identification du signataire par un nom »[36].

87. 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 et 136 ; A/CN.9/1051, par. 67.

« Identité »

88. 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

89. Par « justificatifs d'identité », on entend les données, ou l'objet matériel contenant ces données, présentés aux fins de la confirmation 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

[36] *Guide pour l'incorporation de la Loi type de la CNUDCI sur les signatures électroniques (2001)*, par. 117.

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[37].

Références

A/CN.9/1005, par. 109 et 110 ; A/CN.9/1045, par. 137.

Services de gestion de l'identité

90. 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) : la « confirmation d'identité » et l'« identification électronique ». Ce terme renvoie aux services qui interviennent dans l'une ou l'autre des étapes ou dans les deux. 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/77/17, par. 114 ; A/CN.9/1005, par. 84 et 112 ; A/CN.9/1087, par. 19.

Prestataire de services de gestion de l'identité

91. Le prestataire de services de gestion de l'identité est la personne physique ou morale qui fournit de tels services 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 n'exécute pas nécessairement chacune des fonctions énumérées. La référence à l'accord conclu avec l'abonné vise à rappeler que le prestataire de services de gestion de l'identité est responsable pour l'intégralité des services fournis, indépendamment du fait de savoir s'il exerce directement ou confie à des tiers les fonctions connexes.

92. Le prestataire de services de gestion de l'identité peut également être une partie utilisatrice s'il déploie le service de gestion de l'identité à ses propres fins (par exemple, pour l'identification de ses employés). Dans ce cas, les obligations associées à chaque rôle s'appliqueraient.

[37] 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 ») (*Journal officiel de l'Union européenne,* L257, 28 août 2014).

Références

A/77/17, par. 115 ; A/CN.9/971, par. 97 ; A/CN.9/1005, par. 111 ; A/CN.9/1045, par. 88 ; A/CN.9/1087, par. 22.

Système de gestion de l'identité

93. La définition du terme « système de gestion de l'identité » fait référence au système utilisé pour gérer l'identité en procédant à la confirmation d'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 ; A/CN.9/1087, par. 19.

Confirmation d'identité

94. Le terme « confirmation 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 allégations faites par un sujet concernant son identité avant de lui délivrer un justificatif. Le sujet peut être une personne physique ou morale. On a décidé d'utiliser « confirmation d'identité » plutôt que « identification » pour répondre aux préoccupations concernant les multiples significations données au second terme.

Référence

A/CN.9/1005, par. 84.

Partie utilisatrice

95. Par « partie utilisatrice », on entend une personne physique ou morale qui agit en se fiant au résultat d'un service de gestion de l'identité ou d'un service de confiance. Par exemple, la partie utilisatrice peut être une personne qui agit sur la base d'une signature électronique, et non du service de confiance utilisé pour générer cette signature. Cette définition se fonde sur celle contenue à l'article 2 f de la Loi type sur les signatures électroniques.

96. La Loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance n'impose pas d'obligations aux parties

utilisatrices. Toutefois, ces obligations peuvent découler d'autres lois ou accords, y compris d'un accord conclu entre l'abonné et la partie utilisatrice. L'une de ces obligations peut consister à prendre des mesures raisonnables pour évaluer la fiabilité des méthodes utilisées aux fins de la prestation du service en question, par exemple en vérifiant la désignation *ex ante* du service. Une autre peut avoir trait au respect des procédures de sécurité et des politiques et pratiques du prestataire de services.

97. Le prestataire de services peut limiter sa responsabilité envers la partie utilisatrice pour les pertes résultant de l'utilisation du service si cette utilisation a dépassé les limites fixées en ce qui concerne l'objet ou la valeur des transactions pour lesquelles le service peut être utilisé, et s'il s'est acquitté de son obligation de permettre à la partie utilisatrice de déterminer ces restrictions (articles 12-4 et 24-4). Cette dernière a donc intérêt à vérifier toute restriction quant aux fins ou à la valeur de la transaction pour laquelle le service est utilisé, et à s'y conformer.

98. La partie utilisatrice peut être liée en vertu d'un contrat par les règles de fonctionnement prévues à l'article 6, ou être un tiers dans la relation entre l'abonné et le prestataire de services telle qu'elle est définie par ces règles de fonctionnement. En outre, le prestataire de services peut également être une partie utilisatrice s'il déploie le service à ses propres fins (par exemple, pour l'identification de ses employés). Dans ce cas, les obligations associées à chaque rôle s'appliqueraient.

Références

A/77/17, par. 115 et 147 ; A/CN.9/1087, par. 55 et 72 ; A/CN.9/1125, par. 94.

Abonné

99. Le terme « abonné » désigne la personne à laquelle les services sont fournis et n'inclut pas les parties utilisatrices. Il présuppose l'existence d'une relation entre le prestataire de services et l'abonné, qui peut être de nature contractuelle ou autre (par exemple, imposée par la loi). Par exemple, le signataire d'une signature électronique entre dans la définition du terme « abonné ».

Références

A/CN.9/1005, par. 38 à 40 et 96 ; A/CN.9/1045, par. 18 et 22 ; A/CN.9/1087, par. 23.

Service de confiance

100. La définition du terme « service de confiance » associe une description abstraite de l'objet des services de confiance, qui consiste essentiellement à garantir la qualité des données, notamment leur véracité et leur authenticité, à une liste non exhaustive des services de confiance qui sont mentionnés dans la Loi type. Le caractère

non exhaustif de cette liste permettra d'appliquer les règles générales relatives aux services de confiance aux types de services susceptibles d'apparaître à l'avenir.

101. La référence aux « méthodes utilisées pour créer et gérer » 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

102. Le prestataire de services de confiance est une personne physique ou morale qui fournit des services de confiance. Ainsi, un prestataire de services de certification au sens de la Loi type sur les signatures électroniques est un exemple de prestataire d'un service de confiance ayant trait aux signatures électroniques. La Loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance ne détermine pas les fonctions dont doivent s'acquitter les prestataires de services de confiance. La référence à l'accord conclu avec l'abonné vise à rappeler que le prestataire de services de confiance est responsable pour l'intégralité des services fournis, indépendamment de savoir s'il exerce directement ou confie à des tiers les fonctions connexes.

103. La Loi type n'exige pas le recours à un tiers prestataire de services de confiance comme condition de la reconnaissance juridique. S'il n'est pas fait appel à un tel tiers, la même entité peut exercer les rôles de prestataire de services de confiance et d'abonné.

Référence

A/CN.9/1087, par. 22.

Article 2. Champ d'application

104. L'article 2 définit le champ d'application de la Loi type par référence à l'utilisation et à la reconnaissance internationale de la 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 transactions qui sont étroitement liées au commerce, mais sans être de nature commerciale. Celles-ci peuvent faire intervenir des entités publiques, comme les autorités douanières qui gèrent un guichet unique pour les formalités d'importation et d'exportation.

105. Étant donné que l'utilisation de la gestion de l'identité et de services de confiance a des incidences qui vont au-delà des transactions commerciales, les États adoptants peuvent étendre le champ d'application de la Loi type à d'autres types de transactions électroniques impliquant des entreprises, des administrations et des consommateurs.

106. 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 précise que la Loi type n'introduit aucune nouvelle obligation en matière d'identification.

107. 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. À titre d'exemple de ces exigences, qui sont d'ordre généralement réglementaire, on mentionnera l'obligation de présenter un document d'identité particulier (par exemple, un passeport) ou un document d'identité doté de certaines caractéristiques correspondant à des attributs pertinents (par exemple, une carte d'identité avec photo et date de naissance du titulaire). Il peut également être exigé que l'identification soit effectuée par une certaine personne exerçant des fonctions spécifiques. Lorsque l'identification électronique est autorisée, les organismes de réglementation 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.

108. Compte tenu de sa nature habilitante, la Loi type, à l'instar des textes législatifs existants de la CNUDCI sur le commerce électronique, est sans incidence sur l'application aux services de gestion de l'identité et aux services de confiance d'autres lois susceptibles de régir ces activités ou certains aspects essentiels des transactions 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 ; A/CN.9/1087, par. 27.

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

109. L'article 3 indique que la Loi type n'impose pas l'utilisation de services de gestion de l'identité ou de services de confiance à une personne qui n'a pas accepté de les utiliser. 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. Il peut être déduit de circonstances telles que le niveau de connaissances et l'expérience d'une partie dans l'utilisation de la gestion de l'identité et des services de confiance, ainsi que le type de transaction, cette déduction pouvant être réfutée.

110. Le principe de l'utilisation volontaire des services de 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 ces services 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.

111. L'article 3, qui se fonde sur l'article 8-2 de la Convention sur les communications électroniques, s'abstient d'imposer 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.

112. De plus, en indiquant que la Loi type n'exige pas l'utilisation d'un service de gestion de l'identité ou d'un service de confiance particulier, l'article 3 met en œuvre le principe de la neutralité technologique, notamment en ce qui concerne la neutralité des modèles et des systèmes.

113. L'obligation d'utiliser des services de gestion de l'identité et des services de confiance, ou un service de gestion de l'identité ou un service de confiance particulier, peut exister dans d'autres lois. Elle peut être imposée, par exemple, dans les transactions effectuées avec des entités publiques ou impliquant le respect d'obligations réglementaires.

Références

A/77/17, par. 147 ; A/CN.9/965, par. 22 et 110 ; A/CN.9/1005, par. 116 ; A/CN.9/1045, par. 79 ; A/CN.9/1087, par. 27 et 28.

Article 4. Interprétation

114. 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 Loi type sur le commerce électronique ; art. 4 de la Loi type sur les signatures électroniques ; art. 5 de la Convention sur les communications électroniques ; art. 3 de la Loi type sur les documents transférables électroniques).

115. Le paragraphe 1 vise à promouvoir une interprétation uniforme dans les États adoptants en appelant l'attention des tribunaux et autres organes décisionnels sur le fait que les textes qui incorporent la Loi type 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 dans d'autres États lorsqu'ils statuent sur une affaire, afin de contribuer à promouvoir une interprétation uniforme à l'échelle internationale.

116. Le paragraphe 2 vise à préserver l'interprétation et l'application uniformes des dispositions incorporant la Loi type en prévoyant que les questions qui ne sont pas expressément tranchées par celle-ci seront réglées selon les principes généraux dont elle s'inspire, plutôt que selon les principes établis par le droit interne, sans préjudice de l'application de règles impératives.

117. Comme d'autres textes législatifs de la CNUDCI sur le commerce électronique, la Loi type n'énonce pas expressément les principes généraux sur lesquels elle 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, qui sous-tendent généralement les textes législatifs de la CNUDCI sur le commerce électronique, ont également été jugés pertinents pour la Loi type, sous réserve de certains ajustements (voir par. 45 à 50 ci-dessus). Par exemple, si l'autonomie des parties est un principe fondamental du droit commercial, son application est soumise aux limites fixées par le droit impératif, y compris les dispositions de la Loi type auxquelles les parties ne peuvent déroger. Par ailleurs, comme on l'a indiqué au paragraphe 50 ci-avant, le principe de l'équivalence fonctionnelle ne s'applique pas nécessairement lorsqu'il n'existe pas d'équivalent hors ligne.

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.

Chapitre II. Gestion de l'identité

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

118. L'article 5 accorde une reconnaissance juridique à la gestion de l'identité, en prévoyant que la forme électronique de la confirmation d'identité et de l'identification ne les prive pas, en soi, de leurs effets juridiques, de leur validité, de leur force exécutoire ou de leur recevabilité comme preuve. Il 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.

119. L'article 5 interdit toute discrimination à l'égard de la reconnaissance juridique du résultat de l'application des deux étapes du processus de gestion de l'identité, c'est-à-dire la confirmation d'identité et l'identification électronique. Son titre fait référence à la « reconnaissance juridique » et non à la « non-discrimination », afin de préserver l'uniformité avec le titre des dispositions correspondantes figurant dans les textes existants de la CNUDCI.

120. L'alinéa b précise que le fait qu'un 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 *ex ante* et à ceux qui ne le sont pas et font donc l'objet d'une évaluation *ex post*. La Loi type adopte donc une position neutre en ce qui concerne l'approche choisie pour évaluer la fiabilité. Toutefois, l'alinéa b n'implique pas que tout service de gestion de l'identité utilise des méthodes fiables et offre donc un niveau de garantie suffisant pour l'identification effectuée au moyen de la gestion de l'identité : pour parvenir à ce résultat, la fiabilité de la méthode utilisée doit être évaluée conformément aux articles 10 et 11, selon le cas.

121. La référence au paragraphe 3 de l'article 2 figurant dans le chapeau de l'article 5 souligne que cet article ne remet pas en cause une éventuelle exigence légale selon laquelle toute personne doit être identifiée suivant une procédure définie ou prescrite par la loi. Ce paragraphe s'applique non seulement à l'article 5 mais aussi à toutes les autres dispositions de la Loi type.

Références

A/77/17, par. 117 et 118 ; 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 ; A/CN.9/1093, par. 16 ; A/CN.9/1125, par. 92.

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

122. L'article 6 énonce les obligations qui incombent aux prestataires de services de gestion de l'identité. Il énumère les principales obligations du prestataire de services, qui peuvent être complétées par des obligations légales ou contractuelles supplémentaires. Les mots « au minimum » figurant dans le chapeau de l'article 6 indiquent que le prestataire ne peut pas déroger à ces obligations fondamentales et qu'il reste responsable envers les abonnés et les parties utilisatrices, même s'il fait appel à des sous-traitants pour fournir ces services. En outre, il ne saurait être dérogé par voie contractuelle aux obligations visées à l'article 6, dans la mesure où elles peuvent s'appliquer à un système de gestion de l'identité et à un prestataire de services de gestion de l'identité particuliers. Le non-respect de ces obligations peut engager la responsabilité du prestataire en vertu de l'article 12 et compromettre la fiabilité des services de gestion de l'identité, même s'ils ont été désignés.

123. Les obligations énoncées à l'article 6 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.

124. 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 sous-traitants ou d'autres prestataires de services dans le cadre de systèmes multipartites de gestion de l'identité du secteur privé. Par conséquent, les mots « au minimum » figurant à l'alinéa a indiquent que le prestataire de services de gestion de l'identité est tenu d'avoir en place des règles, politiques et pratiques pour répondre aux exigences relatives à l'exercice des fonctions énumérées. L'article 6 n'empêche pas le prestataire de services d'externaliser des fonctions, ni de répartir les risques entre ses sous-traitants ou d'autres partenaires commerciaux.

125. Le principe tendant à ce que le prestataire de services soit lié par ses déclarations et ses engagements est déjà énoncé à l'article 9-1 a) de la Loi type sur les signatures électroniques, qui prévoit que « le prestataire de services de certification agit en conformité avec les déclarations qu'il fait concernant ses politiques et pratiques ».

126. Les systèmes de gestion de l'identité peuvent varier de manière non négligeable quant à leur objet et leur conception, ainsi qu'aux services fournis. La conception du système de gestion de l'identité peut également être fonction du modèle choisi. Par conséquent, 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 donné. Cette souplesse dans la conception des systèmes de gestion de l'identité se reflète dans les mots « adaptées à l'objet et à la conception ».

127. Dans la pratique commerciale, 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 d'« avoir en place des règles, politiques et pratiques de fonctionnement » traduit cette pratique commerciale. En raison de l'importance juridique et pratique qu'elles revêtent, l'alinéa d exige que les règles, politiques et pratiques de fonctionnement soient facilement accessibles aux abonnés, aux parties utilisatrices et aux autres tiers. La référence à la facilité d'accès, également mentionnée à l'alinéa e, vise la facilitation de l'accès à l'information des parties, telles que les micro- ou petites entreprises, qui peuvent moins bien connaître les questions techniques. La référence aux parties utilisatrices est destinée à dissiper tout doute quant à l'applicabilité de l'alinéa d à celles-ci, qui sont un sous-ensemble de tiers.

128. L'alinéa e définit les obligations que les prestataires de services de gestion de l'identité doivent remplir pour limiter leur responsabilité à l'égard des parties utilisatrices, complétant ainsi l'article 12. Ce mécanisme vise à prévenir les difficultés qu'il y a à exiger l'identification de toutes les parties utilisatrices possibles avant que celles-ci ne se fient au résultat de l'utilisation du service.

129. Les alinéas d et e identifient chacun la catégorie d'utilisateurs ciblée, ce qui contribue à augmenter le niveau de respect de ces dispositions par les prestataires de services de gestion de l'identité. Étant donné qu'en vertu de la Loi type, ces prestataires ne sont pas responsables envers les tiers (c'est-à-dire les parties qui ne sont ni prestataires de services ni abonnés) qui ne sont pas des parties utilisatrices, l'alinéa e ne s'applique pas à ces derniers, tandis que l'alinéa d s'applique à l'ensemble des tiers.

130. L'alinéa f complète l'article 8 en définissant les obligations qui incombent au prestataire de services de gestion de l'identité en ce qui concerne la notification, par un abonné, d'une atteinte à la sécurité.

Références

A/77/17, par. 119 ; A/CN.9/936, par. 69 ; A/CN.9/1045, par. 85 à 95 ; A/CN.9/1087, par. 30 à 33, 55 et 61 ; A/CN.9/1093, par. 35, 36 et 40.

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

131. 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.

132. 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 aussi être définie dans la loi sur la confidentialité et la protection des données.

133. La notion d'« incidence importante » est utilisée dans des lois régionales[38] et nationales. Plusieurs facteurs peuvent contribuer à l'évaluation de cette incidence. Des formulaires de notification peuvent aider à évaluer cette 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 auprès des autorités chargées de la protection et de la confidentialité des données.

134. Reconnaissant que des mesures autres que la suspension totale pourraient être appropriées, l'article 7 prévoit que le prestataire de services de gestion de l'identité doit prendre « toutes les mesures raisonnables » pour répondre à une atteinte à la sécurité et en limiter les effets.

135. 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 le fonctionnement des systèmes et augmenter le niveau de confiance dans les services de gestion de l'identité et les services de confiance.

136. L'article 7 s'applique en parallèle avec la loi sur la confidentialité et la protection des données ainsi qu'avec toute autre loi applicable à l'événement concerné. Les notifications relatives aux violations des données présentent des points communs avec celles relatives aux atteintes à la sécurité, mais aussi de grandes différences.

[38] Article 19-2 du Règlement eIDAS.

137. 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 de l'atteinte et de ses détails techniques, peuvent être spécifiés dans d'autres lois (à savoir la loi sur la confidentialité et la protection des données), dans les accords contractuels et dans les règles, politiques et pratiques de fonctionnement du prestataire de services de gestion de l'identité. Le cas échéant, toutes les mesures visées, et pas seulement les notifications, doivent être prises conformément à la loi applicable.

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 ; A/CN.9/1087, par. 35.

Article 8. Obligations incombant aux abonnés

138. L'article 8 énonce les obligations qui incombent aux abonnés en matière de notification des atteintes, ou de tout risque d'atteinte, visant les justificatifs d'identité. Celles-ci complètent les obligations qui incombent au prestataire de services de gestion de l'identité, lequel est tenu de fournir des moyens permettant de notifier les atteintes à la sécurité [art. 6 f)] et de réagir en cas d'atteinte à la sécurité ou de perte d'intégrité (art. 7).

139. L'obligation qui incombe à l'abonné en cas d'une atteinte à la sécurité s'applique lorsque les justificatifs d'identité ont été compromis ou qu'il y a un risque important de compromission. Cet événement déclencheur diffère par conséquent de celui qui établit les obligations incombant au prestataire de services de gestion de l'identité en cas de violation des données, à savoir une atteinte à la sécurité ou une perte d'intégrité ayant une incidence importante sur le système de gestion de l'identité. Le manquement de l'abonné aux obligations qui lui incombent au titre de l'article 8 n'exonère pas nécessairement le prestataire de services de sa responsabilité.

140. Le contrat conclu entre l'abonné et le prestataire de services de gestion de l'identité peut énoncer des obligations supplémentaires pour l'abonné. Il peut également contenir des informations supplémentaires sur la manière de satisfaire à l'obligation de notification prévue à l'article 8.

141. 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 prévues par le prestataire de services de gestion de l'identité. La notion de « justificatifs d'identité compromis » renvoie aux cas d'accès non autorisé à ces justificatifs.

142. L'alinéa b vise les cas où l'abonné n'a pas effectivement connaissance de la compromission mais a des raisons de croire qu'elle a pu se produire. Il s'inspire de l'article 8-1 b ii de la Loi type sur les signatures électroniques, qui prévoit des obligations similaires pour le signataire, et vise à garantir qu'aucune attente déraisonnable en matière d'expertise technique ne sera imposée à l'abonné. L'obligation de notification devrait uniquement s'imposer dans des circonstances connues de l'utilisateur qui font naître un doute justifié quant au bon fonctionnement des justificatifs d'identité.

Références

A/CN.9/936, par. 89 ; A/CN.9/971, par. 88 à 97 ; A/CN.9/1005, par. 37 à 43, 95 et 96 ; A/CN.9/1045, par. 102 à 105 ; A/CN.9/1087, par. 36 et 37.

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

143. 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 s'il existe un équivalent de l'identification hors ligne. Il constitue néanmoins une disposition essentielle pour la mise en place d'un régime juridique régissant la gestion de l'identité.

144. La méthode utilisée pour satisfaire à la règle de l'article 9 doit être fiable conformément au paragraphe 1 ou au paragraphe 4 de l'article 10. La fiabilité de la méthode peut être évaluée *ex post* ou dans le cadre d'une désignation *ex ante*. La norme de fiabilité n'est pas absolue mais dépend de l'objet visé.

145. 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 hors ligne, l'article 9 traite de 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.

146. L'article 9 fait référence à l'utilisation de services de gestion de l'identité pour indiquer que les exigences en matière d'équivalence sont satisfaites par l'utilisation de justificatifs d'identité, plutôt que par celle de systèmes de gestion de l'identité ou de l'identité même.

147. L'article 9 n'a pas d'incidence sur les exigences d'identification selon une procédure ou méthode particulière, comme le prévoit le paragraphe 3 de l'article 2. 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. 107 ci-dessus).

148. 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 ou papier. 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 ne traitent pas de la vérification d'attributs particuliers, car elles portent sur les processus intervenant dans la gestion des justificatifs d'identité plutôt que sur les attributs contenus dans ces justificatifs.

149. Les articles 9 et 16 à 21 de la Loi type renvoient à des cas de figure dans lesquels la loi exige une action ou prévoit des conséquences en l'absence de celle-ci. Cette formulation, qui est reprise de l'article 9 de la Convention sur les communications électroniques, a été utilisée afin de tenir compte des règles d'équivalence fonctionnelle lorsque la loi autorise certaines actions, sans toutefois les exiger, et prévoit les conséquences juridiques y relatives.

Références

A/77/17, par. 124 à 126 ; 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 ; A/CN.9/1087, par. 38 à 41 ; A/CN.9/1125, par. 95.

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

150. 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*). Il fait référence à la méthode utilisée dans un service, plutôt que dans un système de gestion de l'identité, car un système unique peut prendre en charge plusieurs services utilisant des méthodes aux niveaux de fiabilité différents.

151. Le paragraphe 1 a met en œuvre l'approche *ex post* en indiquant que la méthode doit être « suffisamment fiable au regard de l'objet pour lequel le service de gestion de l'identité est utilisé ». Cette disposition traduit l'idée selon laquelle la fiabilité est une

notion relative. Toutefois, contrairement à certains services de confiance qui peuvent remplir plusieurs fonctions, l'identification électronique n'en remplit qu'une, 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.

152. Le paragraphe 1 b contient une clause visant à empêcher la répudiation du service de gestion de l'identité et à limiter les actions en justice abusives. La répudiation se produit lorsqu'un sujet déclare ne pas avoir effectué une action. S'agissant des services de gestion de l'identité, le risque est qu'après l'aboutissement de l'identification d'une partie dans les faits, cette partie ou une autre puisse contester juridiquement la fiabilité de la méthode de façon abstraite et puisse, par cette contestation, invalider l'identification de fait.

153. Pour que le mécanisme prévu au paragraphe 1 b fonctionne, il faut que la méthode 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. La Loi type exige l'utilisation de méthodes fiables, et le paragraphe 1 b ne devrait pas être interprété à tort comme tolérant ou validant l'utilisation de méthodes non fiables. Il reconnaît plutôt que, d'un point de vue technique, la fonction (à savoir l'identification dans le cas de l'article 9) et la fiabilité sont deux attributs distincts.

154. Le paragraphe 1 b s'inspire de l'article 9-3 b ii de la Convention sur les communications électroniques, auquel il ajoute deux éléments. Le premier est qu'une méthode dont il est démontré qu'elle permet d'aboutir à une identification dans les faits, par elle-même ou avec d'autres preuves, est réputée suffisamment fiable, et satisfait donc aux exigences de fiabilité de la méthode prévues à l'article 9. Le second est que le fait que la méthode ait rempli la fonction d'identification doit être déterminé par un organe décisionnel, qui peut être une juridiction étatique, un tribunal administratif, un tribunal arbitral ou toute autre entité chargée de régler des différends. Les mots « par ou devant » tiennent compte de toutes les options disponibles en droit interne aux fins de la présentation et de l'évaluation des preuves et de l'établissement des faits, qui peuvent être effectués par l'organe décisionnel lui-même ou par les parties.

155. Le paragraphe 2 énonce une liste de circonstances, décrites en termes technologiquement neutres, qui peuvent 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 d'une convention conclue entre les parties peut fortement varier en fonction du degré de reconnaissance que l'État concerné accorde à l'autonomie des parties dans le domaine de l'identification. De plus, les conventions contractuelles peuvent être sans incidence sur les tiers, auquel cas cette circonstance ne sera pas pertinente dans les cas faisant intervenir des tiers.

156. 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 Loi type sur les signatures électroniques, qui établit une règle générale de non-discrimination pour la détermination des effets juridiques d'un certificat ou d'une signature électronique[39].

157. Selon le paragraphe 4, la désignation d'un service de gestion de l'identité fiable conformément à l'article 11 confère 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 non désignés. En outre, selon le paragraphe 5 b, la présomption de fiabilité liée à la désignation peut être réfutée.

158. Le paragraphe 5 précise la relation entre les articles 10 et 11 en indiquant 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 Loi type sur les signatures électroniques.

a) Cadre relatif aux niveaux de garantie

159. Les articles 10 et 11 font référence à la notion de « cadre relatif aux niveaux de garantie » ou à des cadres similaires désignés par d'autres termes. Les cadres relatifs aux niveaux de garantie 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. La Loi type utilise l'expression « niveau de garantie » en ce qui concerne la gestion de l'identité et l'expression « niveau de fiabilité » (voir par. 226 ci-dessous) en ce qui concerne les services de confiance.

160. Plus précisément, on entend par « niveau de garantie » le degré de confiance dans les processus de confirmation d'identité et d'identification électronique, c'est-à-dire : *a)* le degré de confiance dans le processus de validation utilisé pour établir l'identité d'un sujet auquel un justificatif a été délivré ; et *b)* le degré de confiance dans le fait que le sujet qui utilise le justificatif est celui à qui ce dernier a été délivré. Le niveau de garantie reflète par conséquent la fiabilité des méthodes, des processus et des technologies utilisés.

161. Le cadre relatif aux niveaux de garantie donne des indications aux parties utilisatrices sur le degré de confiance qu'elles peuvent accorder aux processus de confirmation d'identité et d'identification électroniques et les aide à déterminer si ceux-ci

[39] Pour en savoir plus sur l'interaction entre les articles 12-1 et 12-2 de la Loi type sur les signatures électroniques, voir A/CN.9/483, par. 28 à 36.

sont adéquats à des fins spécifiques. La Loi type ne définit pas de niveaux de garantie ni n'exige la définition ou l'utilisation de tels niveaux. Néanmoins, une telle définition pourrait faciliter la reconnaissance internationale des services de gestion de l'identité.

162. Les cadres relatifs aux niveaux de garantie prévoient différents niveaux de garantie qui sont associés à différentes exigences. Ceux-ci peuvent être désignés par un nombre (par exemple de 1 à 4) ou par un qualificatif (par exemple « faible », « modéré » et « élevé »). Les niveaux de garantie devraient être décrits en termes génériques afin de préserver la neutralité technologique.

163. Les cadres relatifs aux niveaux de garantie peuvent être utilisés pour répondre au besoin du marché de connaître le degré de fiabilité du service de gestion de l'identité proposé. Un prestataire de services de gestion de l'identité qui ne fait aucune référence aux niveaux de garantie dans ses règles, politiques et pratiques de fonctionnement sera probablement considéré comme offrant des services d'un niveau de garantie très faible. Cependant, il se peut qu'il n'existe pas encore de définition acceptée au niveau mondial du cadre relatif aux niveaux de garantie, et que l'on doive utiliser différentes définitions nationales ou régionales.

164. 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 tel cadre. Les systèmes et services spécifiques 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 le type de transaction en question.

b) Certification et supervision

165. L'article 10 mentionne, parmi les circonstances qui peuvent être pertinentes, « [t]oute supervision ou toute certification fournie concernant le service 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 aux fins de l'évaluation de la fiabilité de la méthode utilisée, car elles sont associées à un certain niveau d'objectivité dans cette évaluation. Cette circonstance est déjà mentionnée à l'article 12 a vi de la Loi type sur les documents transférables électroniques et à l'article 10 f de la Loi type sur les signatures électroniques.

166. Parmi les options de certification figurent 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 recherché 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.

167. 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 organisme de supervision a des répercussions administratives et financières qui peuvent être lourdes.

168. Il existe différentes approches en ce qui concerne la participation d'organismes publics à la certification et à la supervision, qui est une décision politique appartenant à l'État adoptant. Lorsque des entités publiques font à la fois office d'organismes de certification ou de supervision et de 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.

169. La Loi type n'impose pas, ni ne facilite, la mise en place d'un régime de supervision. L'approche qui y est adoptée est fondée sur la neutralité du modèle et les références à la certification et à la supervision n'excluent pas les régimes d'autocertification.

170. Dans certains cas, par exemple lorsque certains types de technologies de registre distribué sont utilisées, les solutions présupposant l'existence d'un organisme central de certification, d'accréditation ou de supervision peuvent 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 difficultés.

Références

A/77/17, par. 127 à 132 ; 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.9/1087, par. 42 à 46, 105 et 106 ; A/CN.9/1093, par. 34 ; A/CN.9/WG.IV/WP.153, par. 74 et 75 ; A/CN.9/1125, par. 96.

Article 11. Désignation de services de gestion de l'identité fiables

171. L'article 11 complète l'article 10 en offrant la possibilité de désigner des services de gestion de l'identité. Plus précisément, il énumère les conditions auxquelles un tel service doit satisfaire pour figurer sur la liste de services de gestion de l'identité désignés. Comme l'article 10, il se réfère à la méthode utilisée dans un service, plutôt que dans un système de gestion de l'identité, car un système unique peut prendre en charge plusieurs services offrant des niveaux de fiabilité différents et qui peuvent, par conséquent, être ou non désignés.

172. La désignation de 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 qui sont prises en considération 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 désignées comme étant fiables *ex ante* et celles déterminées comme étant 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.

173. La diffusion d'informations sur les services de gestion de l'identité désignés est essentielle pour faire connaître leur existence aux abonnés potentiels. L'entité de désignation est tenue de publier une liste des services désignés, en indiquant notamment les coordonnées des prestataires de services, par exemple sur son site Web. 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. D'autres méthodes peuvent être utilisées pour informer le public au sujet des services désignés, mais celles-ci devraient compléter plutôt que remplacer la publication d'une liste.

174. Le paragraphe 2 a renvoie aux normes et procédures pertinentes pour déterminer la fiabilité et vise à assurer une certaine uniformité entre les résultats des évaluations *ex ante* et *ex post* de la fiabilité. Le paragraphe 3 quant à lui fait expressément 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*.

175. Comme le paragraphe 3 de l'article 10, le paragraphe 4 précise que le lieu où le service de gestion de l'identité est fourni et celui où se trouve l'établissement du prestataire de services ne sont pas pertinents pour la désignation d'un service fiable. Il s'inspire de l'article 12-1 de la Loi type sur les signatures électroniques, qui établit une règle générale de non-discrimination pour la détermination des effets juridiques d'un certificat ou d'une signature électronique. Dans la 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 ces services.

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 ; A/CN.9/1087, par. 47 à 49.

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

176. Comme indiqué au paragraphe 73 ci-dessus, l'article 12 établit un régime de responsabilité uniforme fondé sur le principe selon lequel le prestataire de services de gestion de l'identité doit être tenu responsable des conséquences de tout manquement à l'obligation de fournir des services aux abonnés et aux parties utilisatrices. Il a pour objectif de reconnaître que le prestataire de services peut être tenu responsable en cas de manquement aux obligations lui incombant en vertu de la Loi type, que ces obligations aient ou non un fondement contractuel. Cette disposition s'applique indépendamment de la nature publique ou privée du prestataire de services de gestion de l'identité.

177. L'article 12 se fonde 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 de la Loi type ; *b)* il établit la responsabilité du prestataire en cas de manquement à ses obligations impératives, que ces obligations aient ou non un fondement contractuel ; et *c)* il reconnaît la possibilité de limiter la responsabilité dans certaines conditions.

178. La responsabilité visée à l'article 12 découle de la loi et fonctionne par conséquent en parallèle à la responsabilité contractuelle et extracontractuelle. Par conséquent, comme indiqué au paragraphe 2 a, l'article 12 est sans incidence sur l'application des dispositions de droit interne relatives à la responsabilité contractuelle et extracontractuelle pertinentes pour les prestataires de services de gestion de l'identité.

179. La responsabilité des prestataires de services de gestion de l'identité peut découler de l'utilisation de services tant désignés que non désignés. Toutefois, elle n'est pas absolue. Par exemple, un prestataire de services peut ne pas être responsable envers un abonné si la perte a été entraînée par l'utilisation d'un justificatif dont l'abonné savait, ou aurait dû savoir, qu'il était compromis.

180. Les questions relatives à la responsabilité qui ne sont pas traitées à l'article 12 relèvent de la loi applicable en dehors de la Loi type. Parmi ces questions figurent notamment le degré de diligence, le degré de faute, la charge de la preuve et la détermination du montant des dommages et de l'indemnisation.

181. L'article 12 reconnaît la possibilité de limiter la responsabilité dans certaines conditions. Les limitations de responsabilité peuvent être nécessaires pour contenir le coût de l'assurance, entre autres, et sont généralement indiquées dans les règles, politiques et pratiques de fonctionnement du prestataire de services. L'article 12 reconnaît également la pratique consistant, pour les prestataires de services de gestion de l'identité, à limiter leur responsabilité de manière différente selon la partie (c'est-à-dire l'abonné ou la partie utilisatrice) et le type de service concerné (par exemple, valeur

faible ou élevée de la transaction). Il n'a pas d'incidence sur la capacité du prestataire de services de se fonder sur d'autres lois pour invoquer un plafond de responsabilité, pour autant que celui-ci respecte les obligations qui lui incombent au titre de la Loi type, y compris celles relatives à la limitation de responsabilité.

182. Le paragraphe 3 permet de limiter la responsabilité du prestataire de services de gestion de l'identité envers l'abonné à deux conditions. Premièrement, l'utilisation du service dépasse les limites fixées en ce qui concerne l'objet ou la valeur de la transaction et en ce qui concerne l'étendue de la responsabilité qui s'applique à la transaction pour laquelle le service de gestion de l'identité est utilisé. Deuxièmement, ces limites sont contenues dans l'accord conclu entre le prestataire de services de gestion de l'identité et l'abonné. Conformément à la définition du terme « abonné », la référence à l'« accord » vise à englober tous les types de relations qui peuvent exister entre les prestataires de services de gestion de l'identité et les abonnés, qu'elles soient de nature contractuelle ou autre.

183. De même, le paragraphe 4 permet de limiter la responsabilité du prestataire de services de gestion de l'identité envers la partie utilisatrice à deux conditions. Premièrement, l'utilisation du service dépasse les limites fixées en ce qui concerne l'objet ou la valeur de la transaction et en ce qui concerne l'étendue de la responsabilité qui s'applique à la transaction pour laquelle le service de gestion de l'identité est utilisé. Deuxièmement, le prestataire de services de gestion de l'identité s'est acquitté des obligations qui lui incombent en vertu de l'article 6 e en fournissant des moyens facilement accessibles pour permettre à la partie utilisatrice de déterminer les restrictions relatives à la transaction en question.

184. L'article 12 ne traite que de la responsabilité des prestataires de services de gestion de l'identité envers les abonnés et les parties utilisatrices. Toute autre partie qui subit une perte résultant de l'utilisation de tels services 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 pourra alors se retourner contre le prestataire de services de gestion de l'identité.

185. L'article 12 s'applique aux prestataires de services de gestion de l'identité, indépendamment de leur nature publique ou privée. L'État adoptant devra peut-être adapter cette disposition à toute règle particulière relative à 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 et 131 ; A/CN.9/1051, par. 13 à 29 ; A/CN.9/1087, par. 52 à 73.

Chapitre III. Services de confiance

Article 13. Reconnaissance juridique des services de confiance

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

187. L'article 13 s'applique aux services de confiance, qu'ils soient ou non mentionnés dans la Loi type, 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.

Article 14. Obligations incombant aux prestataires de services de confiance

188. L'article 14 établit les principales obligations qui incombent aux prestataires de services de confiance, que ces services soient ou non mentionnés dans la Loi type. 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. Comme c'est le cas des obligations mentionnées au paragraphe 1 de l'article 7, celles énumérées au paragraphe 2 de l'article 14 doivent être satisfaites conformément à la loi applicable, le cas échéant.

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

190. L'obligation de mettre les politiques et pratiques également à la disposition des tiers, y compris des parties utilisatrices (voir par. 127 ci-dessus) 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 d'un service de confiance, conformément au principe de l'utilisation volontaire de ces services (par. 1 de l'art. 3).

191. Le paragraphe 1 e établit un mécanisme permettant aux parties utilisatrices de prendre connaissance de toute restriction quant aux fins ou à la valeur pour lesquelles le service de confiance peut être utilisé, et de toute restriction quant à l'étendue de la responsabilité, qui est similaire à celui contenu à l'article 6 e et complète l'article 24.

192. Le paragraphe 2 définit les obligations incombant aux prestataires de services de confiance en cas de violation des données. Il présuppose une atteinte à la sécurité ou une perte d'intégrité ayant une incidence importante sur le service de confiance.

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 ; A/CN.9/1087, par. 74 à 76.

Article 15. Obligations incombant aux abonnés

193. L'article 15 énonce les obligations qui incombent aux abonnés lorsque le service de confiance est compromis. La notion sous-jacente de « service de confiance compromis » renvoie aux cas d'accès non autorisé à un service et présuppose la survenue d'un événement qui en affecte la fiabilité.

194. L'article 15 reconnaît qu'il est peu probable que l'abonné prenne immédiatement connaissance de problèmes affectant le service de confiance dans son ensemble, mais qu'il peut être conscient de la compromission d'informations visibles et, éventuellement, de risques concernant des informations qui ne sont pas directement visibles, comme des clefs privées. C'est pourquoi les alinéas a et b renvoient à des choses différentes.

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

196. La Loi type ne prévoit pas d'obligations supplémentaires pour les abonnés en relation avec l'utilisation de services de confiance. On trouve des exemples de telles obligations à l'article 8-1 a et c de la Loi type sur les signatures électroniques.

197. La Loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance ne contient pas de règles relatives à la responsabilité des abonnés. Par conséquent, ce sont les dispositions contractuelles, qui peuvent prévoir des obligations supplémentaires à leur égard, et les règles de responsabilité générale qui détermineront la responsabilité de l'abonné.

198. Contrairement à l'article 11 de la Loi type sur les signatures électroniques, l'article 15 n'établit pas d'obligations pour les parties utilisatrices, dont la responsabilité peut être engagée en vertu d'autres lois ou accords.

Références

A/CN.9/1005, par. 37 à 43 ; A/CN.9/1045, par. 22 à 26 ; A/CN.9/1087, par. 77 et 78.

Article 16. Signatures électroniques

199. 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[40]. La formulation de l'article 16 s'inspire de celle de l'article 9 de la Loi type sur les documents transférables électroniques, qui s'inspire elle-même de celle de l'article 9-3 de la Convention sur les communications électroniques, et définit les exigences concernant l'équivalence fonctionnelle entre les signatures manuscrites et électroniques. Par conséquent, le verbe « [i]dentifier » employé à l'article 16 doit être interprété selon le sens qui lui a été donné dans d'autres dispositions similaires de la CNUDCI et dans les textes qui incorporent celles-ci dans le droit interne.

200. L'exigence d'une signature papier est satisfaite si une méthode fiable (voir par. 223 ci-dessous) est utilisée pour identifier le signataire du message de données et indiquer sa volonté concernant le message de données signé. La référence à la méthode utilisée « dans le cas d'un message de données » s'applique tant à l'identification de la personne qu'à l'indication de sa volonté.

201. Les signatures électroniques peuvent être utilisées à diverses fins, notamment pour identifier l'auteur d'un message et l'associer au contenu de ce dernier. 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 compte tenu des coûts, du niveau de sécurité recherché, de la répartition des risques et d'autres considérations. Des textes antérieurs de la CNUDCI examinent en détail les objectifs et les méthodes des signatures électroniques[41].

[40] Voir également *Promouvoir la confiance dans le commerce électronique*.

[41] *Guide pour l'incorporation de la Loi type de la CNUDCI sur les signatures électroniques (2001)*, par. 29 à 62 ; et *Promouvoir la confiance dans le commerce électronique*, 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 ; A/CN.9/1087, par. 82 à 84.

Article 17. Cachets électroniques

202. Les cachets électroniques permettent de garantir l'origine et l'intégrité d'un message de données provenant d'une personne morale. Dans la pratique, ils associent la fonction d'une signature électronique générique en ce qui concerne l'origine, et celle de certains types de signatures, généralement basés sur l'utilisation de clefs cryptographiques, en ce qui concerne l'intégrité. Ces signatures électroniques sont prévues à l'article 6-3 d de la Loi type sur les signatures électroniques. Par conséquent, la description de l'exigence d'intégrité énoncée à l'article 17 se fonde sur cet article.

203. L'article 17 s'inspire d'une législation régionale, à savoir le considérant 65 du Règlement eIDAS, selon lequel « [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 ».

204. La garantie quant à l'origine du message de données peut être obtenue par la détermination de sa provenance, ce qui exige d'identifier la personne morale à l'origine dudit message. Dans la pratique, la méthode fiable utilisée pour identifier la personne morale qui appose le cachet est identique à celle employée pour identifier un signataire, et les dispositions du droit interne transposant les dispositions de la CNUDCI sur les signatures électroniques s'appliquent généralement tant aux personnes physiques qu'aux personnes morales.

205. 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 Loi type sur les signatures électroniques 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.

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

Intégrité

207. 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 antérieurs de la CNUDCI, elle est exigée pour assurer l'équivalence fonctionnelle avec la notion d'« original » dans l'environnement papier (art. 8 de la Loi type sur le commerce électronique). Les articles 17 et 19 s'inspirent de l'article 8-3 de la Loi type sur le commerce électronique 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, 56 et 58 ; A/CN.9/1045, par. 35 et 36 ; A/CN.9/1087, par. 85 et 86.

Article 18. Horodatages électroniques

208. Les horodatages électroniques fournissent la preuve de la date et de l'heure auxquelles le sceau a été associé à certaines 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 degré de certitude suffisant. Par exemple, il est parfois nécessaire de prouver la date de conclusion d'un contrat à des fins d'opposabilité.

209. Les sceaux d'horodatage sont généralement apposés en relation avec certaines actions telles que la génération d'un document électronique sous sa forme finale, la signature, l'expédition et la réception d'une communication électronique. L'exigence d'indiquer un fuseau horaire peut, mais ne doit pas nécessairement, être satisfaite par référence au temps universel coordonné (UTC).

210. L'article 18 mentionne non seulement les « documents, documents d'activité [et] 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 ou document d'activité 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.

Article 19. Archivage électronique

211. L'article 19 traite des services d'archivage électronique, qui assurent la sécurité juridique quant à la validité des documents électroniques conservés. La méthode fiable utilisée pour l'archivage électronique garantit l'intégrité des documents électroniques

archivés, ainsi que la date et l'heure de l'archivage. En outre, les informations archivées doivent être accessibles conformément à l'exigence d'équivalence fonctionnelle avec la notion de « forme écrite » dans l'environnement papier (art. 6-1 de la Loi type sur le commerce électronique).

212. L'article 19 s'inspire, entre autres, de l'article 10 de la Loi type sur le commerce électronique, qui traite de la conservation des messages de données. Toutefois, ce dernier parle de « conservation » des messages de données parce qu'il s'agit de satisfaire à l'obligation légale de conserver les documents dans l'environnement 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).

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

214. Pour des raisons techniques, il peut être nécessaire, pour transmettre et conserver des messages de données, d'ajouter des informations aux messages 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. L'alinéa c autorise les déplacements de fichiers et les changements de format qui interviennent dans le cours normal de la conservation des données. Son libellé se fonde sur l'article 8-3 a de la Loi type sur le commerce électronique.

215. L'article 19 ne traite pas de la question de savoir si les documents électroniques archivés doivent pouvoir être déplacés pour rester accessibles en dépit de l'obsolescence technologique. Cette exigence 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'une information doit être présentée, celle-ci doit pouvoir être montrée à la personne concernée [art. 8-1 b)] de la Loi type sur le commerce électronique).

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.

Article 20. Services d'envoi recommandé électroniques

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

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

218. L'article 20 ne fait pas référence à des notions utilisées dans des textes antérieurs de la CNUDCI, telles que l'« expédition » et la « réception » (voir art. 10 de la Convention sur les communications électroniques), car il a été élaboré pour mettre l'accent sur l'équivalence fonctionnelle entre les services d'envoi recommandé postal 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.

Article 21. Authentification de site Web

219. L'article 21 traite de l'authentification de site Web, qui a pour principale fonction 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.

220. L'article 21 n'énonce pas de règle d'équivalence fonctionnelle puisque les sites Web existent uniquement sous forme électronique et leur authentification n'a donc pas d'équivalent hors ligne.

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

222. 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 préserver 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.

Article 22. Critères de fiabilité pour les services de confiance

223. Conformément à l'approche adoptée en ce qui concerne les services de gestion de l'identité (art. 10), l'article 22 exige l'utilisation de méthodes fiables pour la fourniture de services de confiance. La méthode utilisée doit être fiable conformément au paragraphe 1 ou au paragraphe 4 de l'article 22. La fiabilité de la méthode peut être évaluée *ex post* ou dans le cadre d'une désignation *ex ante*. La norme de fiabilité n'est pas absolue mais dépend de l'objet visé. L'article 22 dresse une liste non exhaustive de circonstances qui peuvent être pertinentes pour déterminer la fiabilité de la méthode utilisée conformément à l'approche *ex post*. Celle-ci s'inspire des listes figurant à l'article 10 de la Loi type sur les signatures électroniques et à l'article 12 de la Loi type sur les documents transférables électroniques.

224. Tout comme la notion de méthode fiable utilisée pour les services de gestion de l'identité (voir par. 150 et 151 ci-dessus), la notion de méthode fiable utilisée pour 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 ». Le paragraphe 1 b vise à empêcher la répudiation des services de confiance qui ont démontré qu'ils avaient rempli leur fonction et, ainsi, à limiter les actions en justice abusives (voir par. 152 à 154 ci-dessus). Il renvoie aux fonctions décrites aux articles 16 à 21 qui sont pertinentes pour la transaction en question.

225. Les dispositions de la Loi type n'ont pas vocation à modifier les textes antérieurs de la CNUDCI ni à en interpréter les dispositions. À cet égard, l'article 22-1 b en relation avec l'article 16, d'une part, et l'article 9-3 b de la Convention sur les communications électroniques, d'autre part, présentent différents niveaux de détail. En outre, les dispositions de la Loi type régissent les services de confiance, qui fournissent des garanties quant à la qualité des données, et en tant que telles peuvent trouver une application également en l'absence d'exigences de forme.

Niveaux de fiabilité

226. La Loi type sur les signatures électroniques et plusieurs lois régionales et nationales sur les signatures électroniques établissent une distinction entre les services de confiance en fonction de leur niveau de fiabilité. Plus précisément, ces lois confèrent des effets juridiques plus importants aux signatures électroniques qui satisfont à certaines exigences et sont donc réputées offrir un niveau de fiabilité plus élevé. En outre, certaines lois peuvent exiger que seules les signatures électroniques offrant un niveau de fiabilité plus élevé puissent être désignées. Cette approche n'a pas été suivie dans la Loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance, puisque les services de confiance peuvent être désignés à tout niveau approprié de fiabilité qu'ils offrent.

227. Étant donné que des justificatifs d'identité offrant un niveau de garantie élevé peuvent être utilisés pour des services de confiance présentant différents niveaux de fiabilité, une corrélation directe entre le niveau de garantie d'un service de gestion de l'identité et le niveau de fiabilité d'un service de confiance n'est pas nécessaire.

Références

A/77/17, par. 135 à 137 ; A/CN.9/965, par. 106 ; A/CN.9/971, par. 120 et 121 ; A/CN.9/1005, par. 67 et 68 ; A/CN.9/1045, par. 18 à 21, 27 à 29, 52 à 57 et 61 ; A/CN.9/1051, par. 45 et 46 ; A/CN.9/1087, par. 87, 105 et 106 ; A/CN.9/1125, par. 99.

Article 23. Désignation de services de confiance fiables

228. 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 confiance doit remplir pour figurer sur la liste de services désignés qui sont présumés fiables aux fins des articles 16 à 21.

229. L'article 23 porte sur la désignation de services de confiance, étant entendu que le processus de désignation suppose nécessairement une évaluation des méthodes utilisées. 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 vise pas des types génériques de services de confiance ni l'ensemble des services de confiance offerts par un prestataire particulier, mais plutôt un service de confiance déterminé fourni par un prestataire de services donné.

230. 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 précédemment désignés, mais qui ont perdu cette désignation, ne permet certes pas à la partie concernée de se prévaloir de cette présomption, mais n'a pas de conséquences sur la détermination *ex post* de la fiabilité de la méthode.

231. L'article 23 exige que l'autorité de désignation publie une liste des services de confiance désignés, en indiquant notamment les coordonnées des prestataires de services. Cette obligation vise à promouvoir la transparence et à informer les abonnés potentiels d'un service de confiance donné. Les États adoptants pourraient envisager de regrouper ces listes de manière à ce que les informations puissent être consultées 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.

Article 24. Responsabilité des prestataires de services de confiance

232. 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, se conjuguent pour déterminer l'étendue de cette responsabilité.

233. L'article 24 est rédigé de manière similaire à l'article 12, relatif à la responsabilité des prestataires de services de gestion de l'identité, et les considérations évoquées en relation avec l'article 12 peuvent également valoir pour l'article 24. En particulier, l'article 24, tout comme l'article 12, établit un fondement légal de la responsabilité qui fonctionne en parallèle à la responsabilité contractuelle et extracontractuelle, et l'application des dispositions de droit interne relatives à la responsabilité contractuelle et extracontractuelle pertinentes pour les prestataires de services de confiance n'est pas affectée par l'article 24, comme indiqué au paragraphe 2 a.

234. Dans certains cas, l'identification du prestataire de services de confiance peut s'avérer difficile, voire impossible (par exemple, services d'horodatage utilisés en conjonction avec une technologie de registre distribué), 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.

235. S'agissant des textes antérieurs de la CNUDCI, la Loi type sur les signatures électroniques comporte des dispositions traitant des effets juridiques liés à la conduite 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 Loi type sur les signatures électroniques prévoit en outre la possibilité que les prestataires de services de certification limitent la portée ou l'étendue de leur responsabilité[42].

Références

A/CN.9/1005, par. 74 à 76 ; A/CN.9/1045, par. 62 à 66 ; A/CN.9/1087, par. 89.

[42] Pour un examen de cas particuliers de responsabilité dans le contexte d'une infrastructure à clefs publiques, voir la publication *Promouvoir la confiance dans le commerce électronique*, par. 211 à 232.

Chapitre IV. Reconnaissance internationale

Article 25. Reconnaissance internationale du résultat de l'identification électronique

236. L'article 25 établit un mécanisme de reconnaissance juridique internationale de la gestion de l'identité qui vise à accorder le même traitement juridique aux systèmes de gestion de l'identité, services de gestion de l'identité et justificatifs d'identité nationaux et étrangers. Il se fonde sur le principe de non-discrimination à l'égard de l'origine géographique et met l'accent sur le résultat de l'utilisation de systèmes de gestion de l'identité, de services de gestion de l'identité et de justificatifs d'identité. Étant donné que les différentes fonctions exercées dans le cadre de la prestation d'un service de gestion de l'identité (telles que celles énumérées à l'article 6) pourraient l'être dans différents pays, l'article 25 peut s'appliquer à toutes les fonctions exercées par le prestataire de services de gestion de l'identité ou seulement à certaines d'entre elles, en fonction du lieu où chacune d'entre elles est exercée.

237. L'un des objectifs de l'article 25 est d'éviter aux prestataires de services d'avoir à demander la désignation de leurs services, conformément à l'article 11, dans plusieurs pays. Cela peut être particulièrement utile pour les pays qui emploient des normes techniques internes, qui risquent par conséquent de ne pas être identiques aux normes étrangères. La reconnaissance mutuelle de la certification, lorsqu'elle existe, peut jouer un rôle important dans la mise en œuvre de cette disposition.

238. Les niveaux de garantie définis dans les différents pays peuvent ou non correspondre exactement, car si des définitions des niveaux spécifiques de garantie peuvent faire consensus dans certaines régions, aucune n'est reconnue à l'échelle mondiale.

239. Le paragraphe 1 a s'applique lorsque les définitions des niveaux spécifiques de garantie reconnues par les deux pays sont identiques. Dans ce cas, la méthode utilisée doit offrir « un niveau de garantie au moins équivalent » afin d'empêcher l'utilisation de méthodes offrant un niveau de garantie inférieur à celui requis pour produire un effet juridique particulier dans le pays où est accordée la reconnaissance.

240. Pour favoriser la reconnaissance internationale lorsque les définitions des niveaux spécifiques de garantie reconnues par les deux pays ne sont pas identiques, le paragraphe 1 b renvoie à la notion de « niveau de garantie substantiellement équivalent ou supérieur », qui couvre les niveaux de garantie semblables, sans être identiques, ou supérieurs à ceux requis dans le pays où est accordée la reconnaissance. La notion de « substantiellement équivalent » ne doit donc pas être interprétée comme imposant le respect d'exigences techniques strictes, ce qui pourrait entraîner des obstacles à la reconnaissance mutuelle et, en fin de compte, au commerce. Pour la même raison,

le terme « niveau de garantie » ne doit pas être interprété d'une manière étroite qui exclut certains niveaux de garantie atteints par l'application de critères de garantie, étant donné que les niveaux peuvent être définis différemment selon les systèmes juridiques. Cette notion pourrait perdre de sa pertinence une fois que des définitions des niveaux de garantie auront été établies au niveau mondial.

241. Le membre de phrase « le système de gestion de l'identité, le service de gestion de l'identité ou le justificatif d'identité, selon le cas » vise à englober tous les aspects qui peuvent être pertinents pour la reconnaissance internationale de la gestion de l'identité. Dans la pratique, il peut être préférable de se concentrer sur un service particulier et de ne pas reconnaître tous les services pris en charge par un système de gestion de l'identité donné comme étant également fiables alors qu'un ou plusieurs d'entre eux offrent peut-être un niveau de garantie inférieur. En outre, il faudrait éviter de reconnaître les justificatifs d'identité qui sont restés inchangés alors que le service de gestion de l'identité utilisé pour les délivrer a été compromis.

242. La reconnaissance de systèmes de gestion de l'identité, services de gestion de l'identité et justificatifs d'identité 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.

243. 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 le mécanisme visé au paragraphe 4 de l'article 11, qui prévoit la non-discrimination à l'égard de l'origine géographique dans le processus de désignation, en permettant à l'autorité de désignation de l'État adoptant de se fier à la désignation effectuée par une autorité étrangère et en incluant les systèmes de gestion de l'identité et les justificatifs d'identité parmi les objets susceptibles d'être désignés. Le paragraphe 3 met donc en œuvre l'approche *ex ante*.

244. Pour déterminer l'équivalence, l'autorité compétente doit tenir compte de la liste des circonstances pertinentes pour déterminer la fiabilité des méthodes utilisées par les services de gestion de l'identité, énoncée au paragraphe 2 de l'article 10, afin de garantir la cohérence entre les processus de détermination de la fiabilité.

245. La détermination de la fiabilité d'un service de gestion de l'identité, d'un système de gestion de l'identité ou d'un justificatif d'identité est un exercice qui demande beaucoup de temps et de ressources, et tous les pays ne disposent pas nécessairement des ressources adéquates. Les pays moins bien dotés peuvent tout particulièrement bénéficier de la possibilité de reconnaître les services et systèmes de gestion de l'identité et les justificatifs d'identité étrangers en se fiant aux processus de détermination et de désignation appliqués à l'étranger. Des mécanismes fondés sur le paragraphe 3

peuvent également remplacer les dispositions prises en relation avec la conclusion d'accords ponctuels de reconnaissance mutuelle entre organismes de supervision.

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

Références

A/77/17, par. 138 à 144 ; 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 ; A/CN.9/1087, par. 90 à 101 ; A/CN.9/1093, par. 17 ; A/CN.9/1125, par. 92 et 100.

Article 26. Reconnaissance internationale du résultat découlant de l'utilisation d'un service de confiance

247. L'article 26 introduit un mécanisme de reconnaissance internationale du résultat découlant de l'utilisation de services de confiance qui est similaire à celui établi à l'article 25 pour la gestion de l'identité. En conséquence, les considérations faites au titre de l'article 25 peuvent s'appliquer à l'article 26.

248. L'article 26 est généralement compatible avec l'utilisation des mécanismes existants permettant la reconnaissance internationale du résultat découlant de l'utilisation de services de confiance, comme la reconnaissance croisée et la certification croisée entre infrastructures à clef publique[43].

Référence

A/CN.9/1087, par. 90 à 101.

[43] Pour plus d'informations sur la reconnaissance croisée et la certification croisée, voir la publication intitulée *Promouvoir la confiance dans le commerce électronique*, par. 163 à 172.

Article 27. Coopération

249. Les mécanismes de coopération institutionnelle peuvent 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, en particulier en ce qui concerne les exigences techniques, notamment les niveaux de garantie et les niveaux de fiabilité.

250. En outre, l'article 27 peut contribuer à la définition commune de normes techniques, y compris des niveaux de garantie et des niveaux de fiabilité, qui sont appliquées pour déterminer l'équivalence. Dans la pratique commerciale, les notions de niveau de garantie et de niveau de fiabilité sont les termes consacrés pour l'évaluation, respectivement, des services de gestion de l'identité et des services de confiance. Étant donné la difficulté qu'il y a à convenir de définitions reconnues à l'échelle mondiale, la Loi type n'établit pas d'ensemble commun de niveaux de garantie pour les systèmes de gestion de l'identité ni de niveaux de fiabilité pour les services de confiance. De plus, les lois et les pratiques commerciales dictant la formulation de ces définitions varient d'un pays à l'autre, notamment en ce qui concerne le rôle des autorités centrales par rapport au rôle joué par les accords contractuels.

251. La coopération devrait se faire sur une base volontaire et dans le respect des lois et règlements applicables à l'échelle nationale. La référence aux « entités étrangères » vise à englober toutes les entités, indépendamment de leur nature juridique, qui peuvent contribuer à la réalisation des objectifs envisagés.

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 ; A/CN.9/1087, par. 108 et 109.

2300891