Nations Unies A/CN.9/WG.IV/WP.157

Assemblée générale

Distr. limitée
28 janvier 2019
Français
Original : anglais

Commission des Nations Unies pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Cinquante-huitième session
New York, 8-12 avril 2019

Projet de dispositions relatives à la reconnaissance internationale de la gestion de l'identité et des services de confiance

Note du Secrétariat

Table des matières

V.19-00494 (F)

I. Introduction

1. À la cinquante-septième session du Groupe de travail, il a été demandé que le Secrétariat établisse un document contenant des projets de dispositions portant sur les aspects fondamentaux des questions juridiques liées à la gestion de l'identité et aux services de confiance, de manière à faciliter l'avancée des travaux du Groupe de travail en la matière.

2. Donnant suite à cette demande, l'annexe I à la présente note contient des projets de dispositions sur un certain nombre de questions déjà examinées par le Groupe de travail. Dans la mesure du possible, ces dispositions s'appuient sur les débats menés par le Groupe de travail à sa cinquante-septième session (A/CN.9/WG.IV/WP.153). On trouvera des observations supplémentaires sur ces questions, ainsi que sur d'autres points pertinents, dans le document de travail A/CN.9/WG.IV/WP.158.

Annexe I

Projet de dispositions relatives à la reconnaissance internationale de la gestion de l'identité et des services de confiance

Chapitre I. Domaine d'application

Article 1. Champ d'application

[Option A pour le paragraphe 1)

1. Le présent [projet d'instrument] s'applique à l'utilisation de systèmes de gestion de l'identité et de services de confiance dans le cadre de transactions commerciales entre des parties ayant leur établissement dans des États différents [lorsque les règles du droit international privé mènent à l'application de la loi d'un État adoptant].

[Option B pour le paragraphe 1)

1. Le présent [projet d'instrument] s'applique à la reconnaissance internationale de [systèmes de gestion de l'identité] [justificatifs d'identité] et de services de confiance qui sont utilisés dans le cadre d'activités commerciales[1].

2. Le présent [projet d'instrument] s'applique aussi à l'utilisation de systèmes de gestion de l'identité et de services de confiance dans le cadre des services publics touchant au commerce[2].

3. Le présent [projet d'instrument] s'applique à la vérification de l'identité des personnes physiques et morales, ainsi que des objets matériels et numériques.

Article 2. Questions sur lesquelles le présent [projet d'instrument] est sans incidence

1. Aucune disposition du présent [projet d'instrument] n'oblige quiconque à vérifier l'identité d'un sujet ou à utiliser un service de confiance, ni à vérifier l'identité d'un sujet ou à utiliser un service de confiance offrant un niveau particulier de fiabilité.

2. Sous réserve de ce que prévoient ses dispositions, rien dans le présent [projet d'instrument] n'a d'incidence sur l'application à [la gestion de l'identité et aux services de confiance] des règles de droit relatives à [la gestion de l'identité et aux services de confiance] [y compris celles applicables au respect de la vie privée et à la protection des données][3].

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

1. Aucune disposition du présent [projet d'instrument] n'exige d'un sujet qu'il [utilise un système de gestion de l'identité] [accepte des justificatifs d'identité] ou recoure à un service de confiance sans son consentement.

---

[1] Différents points de vue ont été exprimés au sein du Groupe de travail quant à l'« objet » de la reconnaissance juridique aux fins des travaux de celui-ci sur la gestion de l'identité. À sa cinquante-septième session, le Groupe de travail a envisagé les systèmes de gestion de l'identité, les justificatifs d'identité et les transactions liées à l'identité comme objets possibles de la reconnaissance juridique.

[2] Ce projet de disposition vise à souligner que la gestion de l'identité et les services de confiance peuvent être utilisés en dehors d'un cadre purement commercial.

[3] Les termes « y compris celles applicables au respect de la vie privée et à la protection des données » visent à répondre aux préoccupations du groupe de travail sur l'application de la législation relative à ces questions.

2. Aux fins du paragraphe 1, le consentement d'un sujet peut être déduit de son comportement [et d'autres circonstances][4].

Chapitre II. Dispositions générales

Article 4. Définitions

Aux fins du présent [projet d'instrument] :

a) Par « attribut », on entend une donnée ou un élément d'information associé à un sujet[5] ;

b) Par « identification », on entend le processus consistant à réunir, à vérifier et à valider suffisamment d'attributs se rapportant à un sujet pour établir et confirmer son identité dans un contexte donné[6] ;

c) Par « identité », on entend un ensemble d'attributs se rapportant à un sujet qui [permet d'identifier celui-ci de manière suffisante] [le décrit [de façon unique]] dans un contexte donné[7] ;

d) Par « justificatifs d'identité », on entend [un ensemble de données présenté comme preuve d'une identité déclarée] [les données, ou l'objet matériel sur lequel elles se trouvent, qu'un sujet peut présenter pour permettre de vérifier ou d'authentifier son identité dans un environnement en ligne][8, 9] ;

e) Par « gestion de l'identité [électronique] », on entend un ensemble de processus servant à gérer l'identification, l'authentification [et l'autorisation] de sujets dans un environnement en ligne[10] ;

f) Par « opérateur de système de gestion de l'identité », on entend une personne qui exploite un système de gestion de l'identité ;

---

[4] Les termes « et d'autres circonstances » renvoient aux cas où le sujet n'est pas capable d'un comportement autonome, c'est-à-dire lorsqu'il s'agit d'un objet matériel ou numérique. En pareil cas, le consentement ne sera pas attribuable au sujet, mais à la personne physique ou morale qui en est juridiquement responsable (A/CN.9/965, par. 109).

[5] Voir A/CN.9/WG.IV/WP.150, par. 13.

[6] Voir A/CN.9/WG.IV/WP.150, par. 29. Le Groupe de travail voudra peut-être examiner la question de savoir si cette définition devrait être libellée de manière à inclure l'inscription à un système de gestion de l'identité et la délivrance de justificatifs d'identité.

[7] Voir A/CN.9/WG.IV/WP.150, par. 38. Lorsqu'il examinera la définition de l'« identité », le Groupe de travail voudra peut-être se demander s'il est nécessaire de poser l'exigence de l'unicité aux fins de ses travaux sur le sujet, étant donné que : a) l'unicité est un attribut de l'identité fondamentale, et que b) l'identité fondamentale est actuellement exclue du champ des travaux (A/CN.9/965, par. 10).

[8] Cette définition est inspirée de la définition figurant aux articles 59.1 à 550 de la loi de l'État de Virginie sur la gestion de l'identité électronique (Titre 59.1, Chap. 50 du Code de l'État de Virginie).

[9] Voir A/CN.9/WG.IV/WP.150, par. 21. L'expression « justificatifs d'identité » est pratiquement synonyme de celle de « moyens d'identification électronique » telle qu'elle est définie au paragraphe 2 de l'article 3 du règlement (UE) nº 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), à savoir « élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne ».

[10] Voir A/CN.9/WG.IV/WP.150, par. 35. À la cinquante-septième session du Groupe de travail, il a été dit que cette définition semblait impliquer que la référence cumulée à l'« identification », l'« authentification » et l'« autorisation » était indispensable pour définir le concept visé, alors que l'un ou l'autre des éléments énumérés y suffirait. Certains ont déclaré, pour cette raison, que la définition du terme « identification électronique » figurant dans le règlement eIDAS serait préférable (A/CN.9/965, par. 91). Au paragraphe 1 de l'article 3 du règlement eIDAS, l'« identification électronique » est définie comme « le processus consistant à utiliser des données d'identification personnelle [c'est-à-dire des « justificatifs d'identité » tels qu'ils sont définis dans le présent document] sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale ».

g) Par « niveau de garantie », on entend le degré de confiance dans les processus d'identification et d'authentification, à savoir : a) le degré de confiance dans le processus de validation utilisé pour établir l'identité d'un sujet à qui 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. La garantie traduit la fiabilité des méthodes, des processus et des technologies utilisés[11] ;

h) Par « partie utilisatrice », on entend une personne susceptible d'agir en se fiant à un dispositif de gestion de l'identité ou à un service de confiance ;

i) Par « sujet », on entend la personne ou l'objet identifié dans un justificatif donné, qui peut être authentifié par un fournisseur d'identité et dont ce dernier peut se porter garant[12] ;

j) Par « service de confiance »[13], on entend un service électronique qui offre un certain niveau de fiabilité en ce qui concerne la qualité des données ;

k) Par « prestataire de service de confiance » on entend une personne qui fournit un ou plusieurs services de confiance.

Article 5. Interprétation

1. L'interprétation du présent [projet d'instrument] est régie par les principes généraux ci-après :

a) Non-discrimination à l'égard de l'utilisation de moyens électroniques ;

b) Neutralité technologique ;

c) Équivalence fonctionnelle ;

d) […]

2. Pour l'interprétation du présent [projet d'instrument], il est tenu compte de son caractère international et de la nécessité de promouvoir l'uniformité de son application ainsi que d'assurer le respect de la bonne foi.

3. Les questions concernant les matières régies par le présent [projet d'instrument] qui ne sont pas expressément tranchées par lui sont réglées selon les principes généraux dont il s'inspire [ou, à défaut de ces principes, conformément à la loi applicable en vertu des règles du droit international privé][14].

Article 6. Non-discrimination à l'égard de l'utilisation de moyens électroniques

1. L'utilisation de [justificatifs d'identité] [systèmes de gestion de l'identité] n'est pas privée d'effets juridiques, de validité, de force exécutoire ou de caractère probant au seul motif que [les justificatifs d'identité] [les résultats de la vérification d'identité] [les systèmes de gestion de l'identité] se présentent sous une forme électronique[15].

---

[11] Voir A/CN.9/WG.IV/WP.150, par. 42.

[12] Voir A/CN.9/WG.IV/WP.150, par. 55.

[13] Le Groupe de travail voudra peut-être examiner la question de savoir s'il convient de faire référence en anglais aux « *trusted service* » pour éviter toute ambiguïté quant à la notion juridique bien établie de « *trust* » (A/CN.9/965, par. 14 et 101).

[14] L'ajout du membre de phrase « ou, à défaut de ces principes, conformément à la loi applicable en vertu des règles du droit international privé » pourrait s'avérer particulièrement utile dans un contexte international.

[15] Le choix à opérer entre les termes « justificatifs d'identité » et « système de gestion de l'identité » est lié au point de savoir si la reconnaissance juridique porte sur les justificatifs d'identité ou sur les systèmes de gestion de l'identité (voir, *supra*, note 1 et A/CN.9/WG.IV/WP.158, section sur la reconnaissance juridique). Si la reconnaissance juridique portait sur le résultat du processus d'identification (c'est-à-dire la « transaction liée à l'identité »), la présente disposition pourrait plutôt faire référence à ce processus.

2. Les services de confiance ne sont pas privés de leurs effets juridiques, de leur validité, de leur force exécutoire ou de caractère probant au seul motif qu'ils se présentent sous une forme électronique.

Article 7. Neutralité technologique

Aucune disposition du présent [projet d'instrument] n'est appliquée de manière à exclure, restreindre ou priver d'effets juridiques [une technologie, une méthode ou un système] quelconque utilisé pour la gestion de l'identité ou la fourniture de services de confiance satisfaisant aux exigences mentionnées dans le présent [projet d'instrument][ou autrement satisfaisant aux exigences de la loi applicable][16].

Chapitre III. Gestion de l'identité

Article 8. Reconnaissance juridique de la gestion de l'identité

[**Option A pour l'article 8**

Lorsque la loi ou une partie exige[17] l'identification d'un sujet selon une certaine méthode, cette exigence est satisfaite dans le cas de la gestion de l'identité si une méthode fiable est employée pour vérifier les attributs pertinents de ce sujet à un niveau équivalent à celui que garantit la méthode exigée[18].]

[**Option B pour l'article 8**

Lorsque les parties souhaitent procéder à l'identification d'un sujet ou y sont tenues par la loi, le recours à cette fin à un système de gestion de l'identité emporte un effet juridique équivalent à celui produit par l'application de procédures non électroniques reconnues à cet effet, pour autant que ledit système de gestion de l'identité emploie une méthode fiable pour vérifier les attributs du sujet pertinents aux fins de l'identification[19].]

Article 9. Normes de fiabilité pour la reconnaissance de la gestion de l'identité

Pour déterminer la fiabilité du système de gestion de l'identité aux fins de satisfaire à l'exigence visée à l'article 8, toutes les circonstances pertinentes sont prises en considération, notamment :

a) Tout accord entre les parties ;

b) Toute supervision ou toute certification fournie concernant le système de gestion de l'identité ;

c) Le niveau de garantie associé au système de gestion de l'identité[20] ;

d) […]

---

[16] Le membre de phrase « ou autrement satisfaisant aux exigences de la loi applicable », qui figure à l'article 3 de la Loi type sur les signatures électroniques (LTSE) (publication des Nations Unies, numéro de vente : F.02.V.8), renvoie à la possibilité qu'une loi autre que le projet d'instrument prescrive, dans certains cas précis, le respect d'exigences différentes de celles prévues dans le projet d'instrument.

[17] Le Groupe de travail voudra peut-être examiner la question de savoir si les dispositions sur l'équivalence fonctionnelle doivent couvrir les cas où la loi « permet » une chose, et confirmer que l'emploi du verbe « exige » renvoie implicitement aux conséquences juridiques découlant de l'absence de cette chose.

[18] Voir A/CN.9/965, par. 77. Le Groupe de travail voudra peut-être préciser si la référence à « une certaine méthode » vise à établir un lien avec les moyens d'identification sur support papier.

[19] Voir A/CN.9/965, par. 78.

[20] Cette disposition est conçue pour permettre une approche *ex post* de la reconnaissance.

Article 10. [Présomption de] fiabilité des systèmes de gestion de l'identité

1. Un système de gestion de l'identité [satisfait] [est présumé fiable aux fins de satisfaire] à l'exigence visée à l'article 8 si les conditions suivantes sont remplies :

a) [Description de l'ensemble minimum de règles appropriées sur la manière dont les systèmes de gestion de l'identité devraient fonctionner, notamment en matière d'audit, d'assurance, de certification, de responsabilité et de résiliation ou autres points pertinents pour déterminer le niveau de garantie] ;

b) [Description des mécanismes visant à garantir et à vérifier l'application de ces règles par les participants] ; et

c) [Description des mécanismes visant à assurer la publicité de la conformité du système de gestion de l'identité à l'ensemble minimum de règles appropriées][21].

[2. Le paragraphe 1 ne limite pas la possibilité pour quiconque :

a) D'établir par tout autre moyen, en vue de satisfaire à l'exigence visée à l'article 8, la fiabilité du système de gestion de l'identité ; ni

b) D'apporter des preuves de la non-fiabilité du système de gestion de l'identité.][22]

Article 11. Détermination de la fiabilité des systèmes de gestion de l'identité

1. [Toute personne, tout organe ou toute autorité, de droit public ou privé, indiqué[e] par l'État adoptant] peut déterminer quels systèmes de gestion de l'identité satisfont aux exigences visées à l'article 8[23].

2. Toute détermination arrêtée en vertu du paragraphe 1 doit être conforme aux normes internationales reconnues.

Article 12. Obligations incombant aux opérateurs de systèmes de gestion de l'identité

1. Les opérateurs de systèmes de gestion de l'identité sont tenus :

a) D'attribuer les justificatifs d'identité pertinents à la personne concernée[24] ;

b) De garantir la disponibilité en ligne et le bon fonctionnement des processus de gestion de l'identité.

2. Les opérateurs de systèmes de gestion de l'identité doivent notifier [à l'autorité de contrôle] [à leurs clients affectés[25] et aux parties utilisatrices], dans les meilleurs délais [et en tout état de cause dans les [...] jours après en avoir eu connaissance], toute atteinte à la sécurité ou perte d'intégrité ayant une incidence [importante] sur les justificatifs d'identité ou les processus d'authentification fournis ou sur les données à caractère personnel qui y sont conservées.

3. En cas d'atteinte à la sécurité ou perte d'intégrité importante, les opérateurs de systèmes de gestion de l'identité suspendent la fourniture des services concernés [jusqu'à […]].

---

[21] Cette disposition est compatible avec une approche *ex ante* comme avec une approche *ex post* de la reconnaissance.

[22] Ce projet de disposition est inspiré de l'article 6-3 de la LTSE. Il s'applique si le paragraphe 1 établit une présomption de fiabilité.

[23] Cette disposition, inspirée de l'article 7 de la LTSE, est conçue pour permettre une approche *ex ante* de la reconnaissance.

[24] Le Groupe de travail voudra peut-être examiner si cette obligation devrait être étendue à l'attribution des attributs.

[25] Le Groupe de travail souhaitera peut-être envisager de définir les notions d'« utilisateur » et de « client ».

4. Les utilisateurs[26] d'un système de gestion de l'identité informent l'opérateur du système si :

a) Les informations d'identification ou les processus d'authentification ont été compromis ; ou

b) Des circonstances dont ils ont connaissance engendrent un risque important que les justificatifs d'identité ou les processus d'authentification aient été compromis[27].

Article 13. Responsabilité des opérateurs de systèmes de gestion de l'identité

1. Sans préjudice de la responsabilité pouvant découler de la loi, les opérateurs de systèmes de gestion de l'identité [sont tenus responsables] [supportent les conséquences juridiques] des dommages causés [intentionnellement ou par négligence] à quiconque en raison de manquements à leurs obligations au titre du présent [projet d'instrument].

2. Les opérateurs de systèmes de gestion de l'identité ne sont pas tenus responsables des dommages découlant d'une utilisation des services dépassant les limitations fixées [en ce qui concerne l'objet ou la valeur des transactions pour lesquelles le système de gestion de l'identité peut être utilisé] s'ils ont fourni [aux utilisateurs[28] ou] aux tiers des moyens raisonnablement accessibles de déterminer ces limitations[29].

3. Les opérateurs de systèmes de gestion de l'identité [sont présumés dégagés de leur responsabilité] [sont dégagés de leur responsabilité] si [la délivrance du justificatif d'identité ou l'attribution d'un attribut d'identification] est effectuée conformément :

a) [Aux normes applicables en matière de gestion de l'identité ;]

b) [Aux conditions applicables en vertu d'un quelconque accord contractuel ; et]

c) [Aux règles et politiques écrites fixées par le cadre de confiance en matière d'identité dont ils sont membres].

[4. Le paragraphe 3 ne s'applique pas en cas d'acte ou d'omission de la part de l'opérateur de système de gestion de l'identité constitutif de [négligence grave ou de faute intentionnelle].]

---

[26] Le Groupe de travail souhaitera peut-être envisager de définir les notions d'« utilisateur » et de « client ».

[27] Le projet de disposition comporte des éléments facultatifs (entre crochets), qui visent à prévoir le délai dans lequel la notification doit être effectuée, à désigner les parties devant être informées et à établir le niveau d'incidence sur les services, les justificatifs d'identité ou les données à caractère personnel à partir duquel se déclenche l'obligation d'information. Il est également possible de définir une obligation de suspendre le dispositif de gestion de l'identité, soit jusqu'à ce qu'il ait été mis fin à l'atteinte ou à la perte, soit jusqu'à ce qu'un nouveau processus de certification (ou un processus similaire) ait été mis en place.

[28] Le Groupe de travail souhaitera peut-être envisager de définir les notions d'« utilisateur » et de « client ».

[29] Ce projet de disposition vise à tenir compte des clauses contractuelles de limitation de la responsabilité.

Chapitre IV. Services de confiance

Article 14. Reconnaissance juridique des services de confiance

Signatures électroniques[30]

[**Option A pour le paragraphe 1)**

1. Lorsque la loi exige[31] la signature d'une personne, cette exigence est satisfaite si une méthode fiable est employée pour identifier cette personne et pour indiquer sa volonté concernant l'information figurant dans la [communication électronique][32].]

[**Option B pour le paragraphe 1)**

1. Lorsque la loi exige la signature d'une personne, cette exigence est satisfaite si :

a) Une méthode est utilisée pour identifier la personne et pour indiquer la volonté de cette personne concernant l'information figurant dans la [communication électronique] ; et

b) La méthode utilisée est :

i) Soit une méthode dont la fiabilité est suffisante au regard de l'objet pour lequel la [communication électronique] a été créée ou transmise, compte tenu de toutes les circonstances, y compris toute convention en la matière ;

ii) Soit une méthode dont il est démontré dans les faits qu'elle a, par elle-même ou associée à d'autres preuves, rempli les fonctions visées à l'alinéa a) ci-dessus[33].]

Horodatages électroniques

2. Lorsque la loi exige que [certains documents, documents d'activité ou certaines informations] soient accompagnés d'une indication de date et d'heure, cette exigence est satisfaite [dans le cas d'une communication électronique] si une méthode fiable est utilisée pour qu'une indication de date et d'heure accompagne [celle-ci][34].

Archivage électronique

3. Lorsque la loi exige que [certain documents, documents d'activité ou certaines informations] soient conservés, cette exigence est satisfaite si ce sont des messages de données qui sont conservés, sous réserve des conditions suivantes :

a) L'information que contient le message de données doit être accessible pour être consultée ultérieurement ;

---

[30] Le Groupe de travail voudra peut-être examiner la question de savoir si les cachets électroniques devraient être considérés comme un service de confiance distinct ou comme un sous-ensemble de la catégorie des signatures électroniques.

[31] Le Groupe de travail voudra peut-être examiner la question de savoir si les dispositions sur l'équivalence fonctionnelle doivent couvrir les cas où la loi « permet » une chose et confirmer que l'emploi du verbe « exige » renvoie implicitement aux conséquences juridiques découlant de l'absence de cette chose.

[32] Ce projet de disposition, inspiré de l'article 9 de la Loi type de la CNUDCI sur les documents transférables électroniques (publication des Nations Unies, numéro de vente : E.17.V.5), peut être adapté de sorte qu'il vise les fonctions pour lesquelles chaque service de confiance est utilisé. Il ne donne pas d'indications sur les normes de fiabilité, qui pourraient faire l'objet d'une disposition distincte applicable à tous les services de confiance (voir, par exemple, art. 12 de la Loi type de la CNUDCI sur les documents transférables électroniques).

[33] Cette option, fondée sur l'article 9-3 de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (New York, 2005), donne des orientations générales sur les normes de fiabilité. L'alinéa b) ii) prévoit une clause de sauvegarde visant à éviter toute dénonciation lorsque la signature électronique a effectivement rempli sa fonction.

[34] Le Groupe de travail voudra peut-être examiner s'il convient de mentionner les communications électroniques, les messages de données ou d'autres notions.

b) Le message de données doit être conservé sous la forme sous laquelle il a été créé, envoyé ou reçu, ou sous une forme dont il peut être démontré qu'elle représente avec précision les informations créées, envoyées ou reçues ; et

c) 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 l'envoi ou de la réception, doivent être conservées si elles existent[35].

Services d'envoi recommandé électroniques

4. Lorsque la loi exige la preuve de la distribution et de la réception de [certains documents, documents d'activité ou de certaines informations], cette exigence est satisfaite [dans le cas d'une communication électronique] si une méthode fiable est utilisée pour transmettre [celle-ci][36].

Authentification de site Internet

5. Lorsque la loi exige l'identification du propriétaire d'un site Internet, cette exigence est satisfaite si une méthode fiable est utilisée pour identifier la personne qui possède le site Internet et pour associer celle-ci audit site.

Séquestre électronique

6. Lorsque la loi exige le recours à des services de séquestre, cette exigence est satisfaite si une méthode fiable est utilisée pour [placer les avoirs sous séquestre et les remettre à l'ayant droit].

Article 15. Présomption de fiabilité des services de confiance[37]

1. Une méthode est considérée comme fiable aux fins de satisfaire à l'exigence visée au paragraphe 14, si :

a) Les données afférentes à la création de signature sont, dans le contexte dans lequel elles sont utilisées, liées exclusivement au signataire ;

b) Les données afférentes à la création de signature étaient, au moment de la signature, sous le contrôle exclusif du signataire ;

c) Toute modification apportée à la signature électronique après le moment de la signature est décelable ; et

d) Dans le cas où l'exigence légale de signature a pour but de garantir l'intégrité de l'information à laquelle elle se rapporte, toute modification apportée à cette information après le moment de la signature est décelable[38].

2. Le paragraphe 1 ne restreint pas la possibilité pour quiconque :

a) D'établir de toute autre manière, aux fins de satisfaire à l'exigence visée au paragraphe 14, la fiabilité de la signature électronique ; ni

b) D'apporter des preuves de la non-fiabilité de la signature électronique[39].

---

[35] Cette condition ne s'étend pas aux informations qui n'ont d'autre objet que de permettre l'envoi ou la réception du message de données : voir le paragraphe 2 de l'article 10 de la Loi type de la CNUDCI sur le commerce électronique (publication des Nations Unies, numéro de vente : F.99.V.4).

[36] Le Groupe de travail voudra peut-être examiner s'il convient de mentionner les communications électroniques, les messages de données ou d'autres notions.

[37] Dans son libellé actuel, ce projet de disposition s'applique aux signatures électroniques, mais il pourrait être adapté pour s'appliquer à d'autres services de confiance.

[38] Ce projet de disposition pourrait être utile dans les cas où un service de confiance est tenu de donner des garanties d'intégrité.

[39] Ce projet de disposition est inspiré de l'article 6-3 de la LTSE. Il établit une présomption de fiabilité en faveur des signatures conformes à certaines normes. Parmi celles-ci figure notamment l'intégrité, lorsque l'exigence légale de signature a pour but de garantir l'intégrité de l'information à laquelle elle se rapporte.

Article 16. Détermination de la fiabilité des services de confiance[40]

1. [Toute personne, tout organe ou toute autorité, de droit public ou privé, indiqué[e] par l'État adoptant] peut déterminer quelles signatures électroniques satisfont aux dispositions de l'article 14.

2. Toute détermination arrêtée en vertu du paragraphe 1 doit être conforme aux normes internationales reconnues.

Article 17. Obligations incombant aux prestataires de services de confiance

1. Les prestataires de services de confiance veillent à la disponibilité et au bon fonctionnement des services de confiance qu'ils fournissent.

2. Les prestataires de services de confiance doivent notifier [à l'autorité de contrôle] [à leurs clients affectés[41] et aux parties utilisatrices], dans les meilleurs délais [et en tout état de cause dans les [...] jours après en avoir eu connaissance], toute atteinte à la sécurité ou perte d'intégrité ayant une incidence [importante] sur les services de confiance fournis ou sur les données à caractère personnel qui y sont conservées.

3. En cas d'atteinte à la sécurité ou perte d'intégrité importante, les prestataires de services de confiance suspendent la fourniture des services concernés [jusqu'à […]].

4. Les utilisateurs[42] d'un service de confiance informent le prestataire du service de confiance si :

a) Les données de création des services de confiance ont été compromises ; ou

b) Des circonstances dont ils ont connaissance engendrent un risque important que les données de création des services de confiance aient été compromises[43].

Article 18. Responsabilité des prestataires de services de confiance

1. Sans préjudice de la responsabilité pouvant découler de la loi, les prestataires de services de confiance [sont tenus responsables] [supportent les conséquences juridiques] des dommages causés [intentionnellement ou par négligence] à quiconque en raison de manquements à leurs obligations au titre du présent [projet d'instrument].

2. Les prestataires de services de confiance ne sont pas tenus responsables des dommages découlant d'une utilisation des services dépassant les limitations fixées [en ce qui concerne l'objet ou la valeur des transactions pour lesquelles le service de confiance peut être utilisé] s'ils ont fourni [aux utilisateurs[44] ou] aux tiers des moyens raisonnablement accessibles de déterminer ces limitations[45].

---

[40] Ce projet de disposition ménage la possibilité de mener une évaluation *ex ante* de la fiabilité de la signature électronique. Dans son libellé actuel il vise les signatures électroniques mais pourrait être adapté pour s'appliquer à d'autres services de confiance.

[41] Le Groupe de travail souhaitera peut-être envisager de définir les notions d'« utilisateur » et de « client ».

[42] Le Groupe de travail souhaitera peut-être envisager de définir les notions d'« utilisateur » et de « client ».

[43] Le projet de disposition comporte des éléments facultatifs (entre crochets), qui visent à prévoir le délai dans lequel la notification doit être effectuée, à désigner les parties devant être informées et à établir le niveau d'incidence sur les services ou les données à caractère personnel à partir duquel se déclenche l'obligation d'information. Il est également possible de définir une obligation de suspendre la fourniture des services de confiance, soit jusqu'à ce qu'il ait été mis fin à l'atteinte ou à la perte, soit jusqu'à ce qu'un nouveau processus de certification ou un processus similaire ait été mis en place.

[44] Le Groupe de travail souhaitera peut-être envisager de définir les notions d'« utilisateur » et de « client ».

[45] Ce projet de disposition vise à tenir compte des clauses contractuelles de limitation de la responsabilité.

Chapitre V. Aspects internationaux

Article 19. Reconnaissance juridique des systèmes de gestion de l'identité et des services de confiance étrangers

1. Pour déterminer si, ou dans quelle mesure, [un système de gestion de l'identité] [des justificatifs d'identité] ou un service de confiance produi[sen]t des effets juridiques, il n'est pas tenu compte :

a) Du lieu où [les justificatifs sont délivrés ou utilisés] [le système de gestion de l'identité est exploité] ou le service de confiance est fourni ;

b) Du lieu où se trouve l'établissement [de l'émetteur] [de l'opérateur de système de gestion de l'identité], du prestataire de service de confiance ou le sujet.

2. [Les systèmes de gestion de l'identité exploités] [Les justificatifs d'identité délivrés] ou les services de confiance fournis en dehors [de l'État adoptant] ont les mêmes effets juridiques dans [l'État adoptant] que [les systèmes de gestion de l'identité exploités] [les justificatifs d'identité délivrés] ou les services de confiance fournis dans [l'État adoptant], s'ils offrent [un niveau de fiabilité substantiellement équivalent] [le même niveau de fiabilité].

3. Pour déterminer si [des justificatifs d'identité] [un système de gestion de l'identité] ou un service de confiance offrent [un niveau de fiabilité substantiellement équivalent] [le même niveau de fiabilité], il est tenu compte [des normes internationalement reconnues][46].

Article 20. Coopération

[Toute personne, tout organe ou toute autorité, de droit public ou privé, indiqué[e] par l'État adoptant] [coopère] [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 certification des systèmes de gestion de l'identité et des services de confiance ;

b) La définition des niveaux de garantie des systèmes de gestion de l'identité et des niveaux de fiabilité des services de confiance ;

c) L'examen des évolutions pertinentes.

[46] Le Groupe de travail voudra peut-être confirmer que, si cette disposition était adoptée, elle aurait pour effet de prévoir l'application de toutes les dispositions du droit de l'État adoptant au système de gestion de l'identité ou aux justificatifs d'identité concernés, y compris, par exemple, les règles régissant les limitations de responsabilité prévues par des dispositions législatives ou contractuelles.