Nations Unies A/CN.9/WG.IV/WP.162

Assemblée générale

Distr. limitée
28 janvier 2020
Français
Original : anglais

Commission des Nations Unies pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Soixantième session
New York, 6-9 avril 2020

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

Note du Secrétariat

Table des matières

V.20-00756 (F)

I. Introduction

1. Le projet révisé de dispositions relatives à l'utilisation et à la reconnaissance internationale de la gestion de l'identité et des services de confiance figurant en annexe au présent document (le « présent projet ») prend en considération les débats qu'a eus le Groupe de travail à sa cinquante-neuvième session (Vienne, 25-29 novembre 2019), et dont il est rendu compte dans le document A/CN.9/1005. Dans les notes de bas de page accompagnant le présent projet, le projet de dispositions examiné par le Groupe de travail à sa cinquante-neuvième session, tel qu'il figure dans le document A/CN.9/WG.IV/WP.160, est appelé le « projet précédent ».

2. Le Groupe de travail voudra peut-être noter que le projet actuel contient des changements de terminologie visant à répondre aux préoccupations relatives à d'éventuelles interprétations divergentes. En particulier, le terme « authentification » a été remplacé par « identification électronique » et le processus précédemment désigné par le terme « identification » est désormais appelé « contrôle d'identité » (art. premier). Il s'ensuit que le processus de gestion des identités est désormais constitué de deux étapes (ou phases), le « contrôle d'identité » et l'« identification électronique ». Le terme « authentification » est désormais utilisé exclusivement dans le cadre des services de confiance (art. 21 et 22).

3. On trouvera un historique des travaux en cours du Groupe de travail IV dans le document A/CN.9/WG.IV/WP.161 (par. 6 à 18).

Annexe

Projet de dispositions[1] relatives à l'utilisation et à la reconnaissance internationale de la gestion de l'identité et des services de confiance

Chapitre premier. Dispositions générales

Article premier. Définitions

Aux fins du présent [instrument] :

a) Par « attribut », on entend un élément d'information ou de donnée associé à [un sujet][une personne][2] ;

b) Par « authentification », dans le cadre des services de confiance, on entend un processus utilisé pour attribuer un identifiant à un objet[3] ;

c) Par « message de données », on entend l'information créée, transmise, reçue ou conservée par des moyens électroniques, magnétiques ou optiques ou des moyens analogues[4] ;

---

[1] *Forme de l'instrument* : Lors des discussions préliminaires sur la question à la cinquante-neuvième session du Groupe de travail, il a été jugé nettement préférable que l'instrument prenne la forme d'une loi type plutôt que d'une convention (A/CN.9/1005, par. 123). Dans le présent projet, le terme « [instrument] » est employé en attendant que le Groupe de travail se prononce sur la question lorsqu'il transmettra l'instrument à la Commission pour adoption.

[2] *Définitions – « attribut »* : Cette définition s'inspire du document A/CN.9/WG.IV/WP.150, par. 13. Le terme est utilisé dans les définitions de « contrôle d'identité » et « identité » ainsi que dans les articles 6 et 7.
Pour l'utilisation des termes « sujet » et « personne », selon les résultats de l'examen de la définition du terme « sujet » par le Groupe de travail, voir la note de bas de page 14.

[3] *Définitions – « authentification »* : Une nouvelle définition du terme « authentification » a été insérée pour désigner le processus consistant à utiliser les services de confiance afin de confirmer l'identité des objets. Le Groupe de travail voudra peut-être examiner la définition conjointement avec les propositions visant à introduire une disposition générale sur l'authentification des objets (art. 22) et à exclure les objets du champ d'application des dispositions relatives à la gestion de l'identité (al. k) de l'article premier, définition du terme « sujet »).

[4] *Définitions – « message de données »* : Cette définition s'inspire des textes existants de la CNUDCI sur le commerce électronique, notamment la Loi type de la CNUDCI sur le commerce électronique (LTCE) (publication des Nations Unies, numéro de vente : F.99.V.4) et la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (CCE) (Nations Unies, *Recueil des Traités*, vol. 2898, nº 50525, p. 3). Le terme est utilisé pour définir les exigences des différents services de confiance énoncées au chapitre III. Comme le précise la définition de l'expression « services de confiance », ce sont les qualités particulières d'un message de données qui sont au centre de chaque service de confiance.

d) Par « identification électronique », dans le cadre des services de gestion de l'identité, on entend un processus utilisé pour obtenir une garantie suffisante quant au lien unissant [un sujet] [une personne] à une identité[5, 6, 7] ;

e) Par « identité », on entend un ensemble d'attributs qui permet à [un sujet][une personne] d'être identifié[e] de manière unique dans un contexte particulier[8] ;

f) Par « justificatifs d'identité », on entend les données, ou l'objet matériel sur lequel elles se trouvent, qu'[un sujet][une personne] peut présenter pour permettre l'identification électronique de son identité sous forme électronique[9].

---

[5] *Définitions – « identification électronique »* : Comme indiqué au paragraphe 2 ci-dessus, le présent projet utilise le terme « identification électronique » au lieu d'« authentification » pour répondre aux préoccupations concernant les significations multiples du terme « authentification ». À la cinquante-neuvième session du Groupe de travail, plusieurs questions ont été soulevées sur le point de savoir ce que l'on entendait par « authentification » et si le sens était le même dans les différents contextes où le terme était utilisé (A/CN.9/1005, par. 13, 84 à 85, 92). Le Groupe de travail a demandé au Secrétariat de veiller à ce que la terminologie soit utilisée de manière cohérente dans l'ensemble du document et conformément à la terminologie adoptée par l'Union internationale des télécommunications (UIT) (voir A/CN.9/1005, par. 86).
La définition de l'expression « identification électronique » s'inspire de celle du terme « authentification » figurant au paragraphe 15 du document A/CN.9/WG.IV/WP.150, qui est elle-même tirée de la recommandation UIT-T X.1252 de l'UIT. Le terme « garantie » est utilisé dans la définition au lieu du terme « confiance » pour les raisons suivantes : a) le terme « garantie » est utilisé dans le présent projet ; et b) la recommandation UIT-T X.1252 assimile « garantie » et « confiance » dans le cadre de l'authentification, ainsi que le montre la définition du « niveau de garantie », décrit comme le « niveau de confiance dans le lien entre une entité et l'information d'identité présentée ».
Dans le présent projet, la notion d'« identification électronique » ainsi définie est utilisée dans le cadre de la gestion de l'identité dans les définitions des termes « justificatifs d'identité », « services de gestion de l'identité », « système de gestion de l'identité », ainsi qu'aux articles 5, 6, 8 et 9.
Dans le projet d'instrument, le terme « authentification » fait référence au recours aux services de confiance pour identifier des objets, conformément au titre du service de confiance « authentification de site Internet ».

[6] *Définitions – « facteurs d'identification électronique »* : Le Groupe de travail voudra peut-être examiner s'il convient d'insérer la définition suivante dans le projet d'instrument : « Par "facteurs d'identification électronique", dans le cadre des services de gestion de l'identité, on entend les éléments d'information ou les processus utilisés pour identifier électroniquement un sujet. »
Ce faisant, le Groupe de travail voudra peut-être garder à l'esprit les définitions des termes « identification électronique » et « justificatifs d'identité ». La définition se fonde sur celle figurant dans le document A/CN.9/WG.IV/WP.150, par. 17. L'expression « facteurs d'identification électronique » est employée uniquement à l'article 6.

[7] *Définitions – « mécanismes d'identification électronique »* : Le Groupe de travail voudra peut-être examiner s'il convient d'insérer la définition suivante dans le projet d'instrument : « Par "mécanismes d'identification électronique", dans le cadre des services de gestion de l'identité, on entend les mécanismes au moyen desquels les sujets utilisent des justificatifs d'identité pour s'identifier. » La définition s'inspire du paragraphe 3 c) de l'article 8 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, abrogeant la directive 1999/93/CE (« règlement eIDAS »). Ce faisant, le Groupe de travail voudra peut-être garder à l'esprit les définitions des termes « identification électronique » et « justificatifs d'identité ». L'expression « mécanismes d'identification électronique » est employée uniquement à l'article 6.

[8] *Définitions – « identité »* : Cette définition s'inspire du document A/CN.9/WG.IV/WP.150, par. 31. À la cinquante-neuvième session du Groupe de travail, il a été généralement admis qu'il fallait inclure dans la définition une exigence d'« unicité » (voir A/CN.9/1005, par. 108).

[9] *Définitions – « justificatifs d'identité »* : Cette définition s'inspire du document A/CN.9/WG.IV/WP.150, par. 21. L'expression est largement synonyme de « moyen d'identification électronique » tel que défini à l'article 3, par. 2, du règlement eIDAS. La définition comprend des éléments de celle qui figure à l'article 59.1-550 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). À la cinquante-neuvième session du Groupe de travail, il a été noté que les justificatifs d'identité électroniques pouvaient être utilisés hors ligne, et il a donc été proposé que la définition fasse plutôt référence aux justificatifs d'identité se présentant « sous forme électronique » (plutôt

g) Par « services de gestion de l'identité », on entend des services consistant à gérer le contrôle d'identité ou l'identification électronique de [sujets][personnes] sous forme électronique[10] ;

h) Par « prestataire de services de gestion de l'identité » on entend une personne qui fournit des services de gestion de l'identité[11] ;

i) Par « système de gestion de l'identité », on entend un ensemble de fonctions et de fonctionnalités permettant de gérer le contrôle de l'identité ou l'identification électronique de [sujets][personnes] sous forme électronique[12] ;

j) Par « contrôle d'identité », on entend le processus consistant à réunir, à vérifier et à valider suffisamment d'attributs pour établir et confirmer l'identité d'[un sujet][une personne] dans un contexte particulier[13] ;

k) Par « sujet » on entend une personne [ou un objet][14] ;

---

que « dans un environnement en ligne »). Le Groupe de travail est convenu de modifier la définition en conséquence (A/CN.9/1005, par. 110).

[10] *Définitions – « services de gestion de l'identité »* : Cette définition s'inspire du document A/CN.9/WG.IV/WP.150, par. 35, option a). Elle renvoie à l'idée selon laquelle la gestion de l'identité comprend deux étapes (ou phases) : le « contrôle d'identité » et l'« identification électronique » (précédemment désignés par les termes « identification » et « authentification », A/CN.9/1005, par. 84). On s'était inquiété précédemment de ce que l'identité soit définie par une référence cumulée à ces étapes (A/CN.9/965, par. 91). Compte tenu de cette préoccupation, la définition mentionne « le contrôle d'identité *ou* l'identification électronique », étant entendu que le terme « ou » est ici inclusif (A/CN.9/1005, par. 109). La référence à la « forme électronique » fait suite à ce dont le Groupe de travail est convenu concernant la définition des « justificatifs identité » (voir note de bas de page 9). Le terme « identification » a été remplacé par « contrôle d'identité » pour tenir compte du changement de terminologie (voir note de bas de page 13).

[11] *Définitions – « prestataire de services de gestion de l'identité »* : Cette définition tient compte de ce dont le Groupe de travail est convenu à sa cinquante-neuvième session (A/CN.9/1005, par. 111).

[12] *Définitions – « système de gestion de l'identité »* : À la cinquante-neuvième session du Groupe de travail, on s'est demandé s'il était bien nécessaire, dès lors que le projet faisait référence aux « services de gestion de l'identité », de parler de « systèmes de gestion de l'identité ». Toutefois, il a été souligné que, dans plusieurs dispositions du projet d'instrument, il était plus approprié de mentionner les « systèmes de gestion de l'identité », notamment à l'article 5 sur la non-discrimination (A/CN.9/1005, par. 86 et 112) et à l'article 11 sur la détermination *ex ante* de la fiabilité (A/CN.9/1005, par. 104). En conséquence, le Groupe de travail a décidé de conserver une définition du système de gestion de l'identité (A/CN.9/1005, par. 112). La définition actuelle du terme reflète la décision du Groupe de travail de faire référence aux « fonctions et fonctionnalités », conformément à la terminologie de l'UIT, dont la recommandation UIT-T X.1252 définit la gestion d'identité comme un « ensemble de fonctions et de fonctionnalités » utilisées i) pour garantir les informations d'identité ; ii) pour garantir l'identité d'une entité ; iii) pour permettre des applications commerciales et de sécurité.

[13] *Définitions – « contrôle d'identité »* : Comme indiqué au paragraphe 2 ci-dessus, le présent projet utilise l'expression « contrôle d'identité » au lieu d'« identification » pour répondre aux préoccupations concernant les multiples significations de ce dernier terme (cf. A/CN.9/WG.IV/WP.150, par. 29).

À la cinquante-neuvième session du Groupe de travail, il a été souligné que la définition de l'« identification » incluait l'étape (ou la phase) d'inscription par les prestataires de services de gestion de l'identité, mais excluait l'étape (ou la phase) d'authentification, qui est désignée dans le présent projet comme l'étape (ou la phase) d'identification électronique (A/CN.9/1005, par. 84). L'« inscription » peut être définie comme le processus par lequel les prestataires de services de gestion de l'identité « vérifient les déclarations d'identité d'un sujet avant de lui délivrer un justificatif » (A/CN.9/WG.IV/WP.150, par. 26).

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

[14] *Définitions – « sujet »* : L'emploi des termes « sujet » et « personne » a été révisé pour en assurer la cohérence dans l'ensemble du projet de dispositions. Le terme « sujet » est utilisé uniquement dans le cadre de la gestion de l'identité.

Les mots « ou un objet » peuvent être supprimés si le Groupe de travail convient de limiter les dispositions relatives à la gestion de l'identité aux personnes physiques et morales. Dans ce cas, le Groupe de travail pourrait envisager de supprimer la définition du terme « sujet » et de remplacer ce terme par le mot « personne » dans l'ensemble du projet d'instrument.

l) 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[15] ;

m) Par « service de confiance », on entend un service électronique qui garantit certaines qualités d'un message de données et comprend les signatures électroniques, les cachets électroniques, les horodatages électroniques, l'authentification de site Internet, l'archivage électronique et les services d'envoi recommandé électroniques[16] ;

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

Article 2. Champ d'application

1. Le présent [instrument] s'applique à l'utilisation et à la reconnaissance internationale de systèmes de gestion de l'identité et de services de confiance dans le cadre d'activités commerciales et de services touchant au commerce[17, 18].

2. Aucune disposition du présent [instrument] n'exige :

a) L'identification d'une personne[19] ;

b) Le recours à un service de gestion de l'identité particulier ; ou

c) Le recours à un service de confiance particulier.

3. Aucune disposition du présent [instrument] n'a d'incidence sur une exigence légale selon laquelle un [sujet][une personne] doit être identifié[e] suivant une procédure définie ou prescrite par la loi.

---

[15] *Définitions – « abonné »* : Le terme « abonné » est employé aux articles 8 et 15, qui imposent des obligations aux abonnés en cas d'atteinte à la sécurité ou de compromission des services. À la cinquante-neuvième session du Groupe de travail, il a été noté que le terme « utilisateur » n'était pas clair car il pouvait désigner à la fois : a) la personne à laquelle les services étaient fournis (par exemple, la personne identifiée) et avec laquelle le prestataire de services entretenait une relation contractuelle, et b) la partie s'étant fiée aux services avec laquelle le prestataire de services n'entretenait pas de relation contractuelle (voir A/CN.9/1005, par. 28, 39 et 95). Une préférence a été exprimée en faveur de l'utilisation du terme « abonné » pour désigner la personne à laquelle les services étaient fournis (A/CN.9/1005, par. 43 et 96).

[16] *Définitions – « services de confiance »* : L'expression « services de confiance » est tirée du règlement eIDAS, où elle est définie comme « un service électronique normalement fourni contre rémunération » consistant en l'un des différents services décrits au chapitre III du règlement. En soi, le règlement eIDAS ne donne pas de définition autonome des « services de confiance ». Le projet précédent tentait d'établir une telle définition en parlant d'« un service électronique qui offre un certain niveau de fiabilité en ce qui concerne la qualité des données ». À la cinquante-neuvième session du Groupe de travail, il a été indiqué qu'une telle définition ne fournissait pas d'orientations adéquates et qu'il convenait de suivre l'approche adoptée dans le règlement eIDAS. Dans le même temps, il a été noté qu'en fournissant une définition plus « abstraite », on pourrait mieux prendre en compte les évolutions futures. Il a aussi été noté que les services de confiance concernaient plus la véracité et l'authenticité des données que leur fiabilité. La définition actuelle tient compte de la décision du Groupe de travail d'inclure une liste non exhaustive de services de confiance (A/CN.9/1005, par. 18).

[17] *Champ d'application – utilisation des systèmes de gestion de l'identité et des services de confiance à l'échelle tant interne qu'internationale* : À sa cinquante-deuxième session, la Commission a noté que le Groupe de travail devrait s'attacher à élaborer un instrument qui pourrait s'appliquer à l'utilisation des systèmes de gestion de l'identité et des services de confiance à l'échelle tant interne qu'internationale (A/74/17, par. 172).

[18] *Champ d'application – services touchant au commerce* : À sa cinquante-neuvième session, le Groupe de travail est convenu qu'il suffisait de renvoyer aux « services touchant au commerce » pour englober les opérations effectuées avec certaines autorités publiques intervenant dans le domaine du commerce, notamment les guichets uniques pour les opérations douanières, et qu'il n'était donc pas nécessaire d'employer le mot « publics » pour qualifier l'expression (A/CN.9/1005, par. 115).

[19] Le Groupe de travail voudra peut-être examiner le rapport entre cette disposition et l'article 3-1.

4. Sous réserve de ce que prévoient ses dispositions, rien, dans le présent [instrument], n'a d'incidence sur l'application aux services de gestion de l'identité ou aux services de confiance des règles de droit applicables, y compris celles applicables au respect de la vie privée et à la protection des données[20].

Article 3. Caractère volontaire de l'utilisation de services de gestion de l'identité et de services de confiance[21]

1. Aucune disposition du présent [instrument] n'exige d'une personne qu'elle utilise un service de gestion de l'identité ou recoure à un service de confiance 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 du présent [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 dans le commerce international[22].

2. Les questions concernant les matières régies par le présent [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[23].

---

[20] La référence au respect de la vie privée et à la protection des données reflète l'importance que le Groupe de travail attache à ces questions, bien qu'il soit entendu qu'elles sortent du cadre de son mandat (A/CN.9/965, par. 125).

[21] *Caractère volontaire de l'utilisation de services de gestion de l'identité et de services de confiance* : L'article 3 se fonde sur l'article 8-2 de la CCE. Le libellé a été révisé pour tenir compte des décisions prises par le Groupe de travail à sa cinquante-neuvième session (voir A/CN.9/1005, par. 116). Dans sa forme actuelle, la disposition empêche l'imposition de toute nouvelle obligation non seulement à l'abonné, mais aussi au prestataire de services et à la partie s'étant fiée aux services. Le principe du caractère volontaire de l'utilisation a déjà été examiné par le Groupe de travail à sa cinquante-septième session (A/CN.9/965, par. 110), où un lien a été établi avec le principe de l'autonomie des parties.

[22] *Interprétation uniforme* : Les textes de la CNUDCI contiennent généralement une disposition établissant une obligation d'interprétation uniforme. À sa cinquante-neuvième session, le Groupe de travail est convenu de préciser que la référence à la bonne foi s'entendait de la bonne foi « dans le commerce international » (A/CN.9/1005, par. 118). Dans sa forme actuelle, l'article 4-1 fait pendant à l'article 5-1 de la CCE.

[23] *Principes généraux* : À sa cinquante-neuvième session, le Groupe de travail est convenu de ne pas énumérer certains des principes généraux sur lesquels se fonde l'instrument, à savoir la non-discrimination à l'égard de l'utilisation de moyens électroniques, la neutralité technologique et l'équivalence fonctionnelle (A/CN.9/1005, par. 118). Dans sa forme actuelle, l'article 4-2 fait pendant à l'article 5-2 de la CCE.

Chapitre II. Gestion de l'identité

Article 5. Reconnaissance juridique de la gestion de l'identité[24]

Les effets juridiques, la validité, la force exécutoire ou l'admissibilité comme preuve de l'identification électronique d'[un sujet][une personne][25] ne sont pas refusés au seul motif que :

a) Le contrôle d'identité et l'identification électronique se font sous forme électronique[26] ; ou

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

Article 6. Obligations incombant aux prestataires de services de gestion de l'identité[27]

Les prestataires de services de gestion de l'identité sont tenus [au minimum] :

a) D'inscrire les [sujets][personnes], en ayant notamment soin :

i) De collecter et d'enregistrer les attributs, selon qu'il convient pour le service de gestion de l'identité ;

ii) De contrôler et de vérifier l'identité ; et

iii) D'attacher les justificatifs d'identité [au sujet][à la personne] ;

b) D'actualiser les attributs ;

c) De gérer les justificatifs d'identité conformément aux règles qui régissent les systèmes de gestion de l'identité, en ayant notamment soin :

i) D'émettre, de délivrer et d'activer les justificatifs ;

---

[24] *Reconnaissance juridique de la gestion de l'identité – généralités :* L'article 5-1 se fonde sur des dispositions similaires dans les textes existants de la CNUDCI relatifs au commerce électronique, comme l'article 5 de la LTCE, l'article 8-1 de la CCE et l'article 7-1 de la Loi type de la CNUDCI sur les documents transférables électroniques (publication des Nations Unies, numéro de vente : E.17.V.5). Il permet juridiquement l'utilisation de services de gestion de l'identité et s'applique indépendamment de l'existence ou non d'un équivalent hors ligne (cf. art. 9). La référence à l'« admissibilité comme preuve » s'inspire de l'article 9 de la LTCE. Le paragraphe 1 b) étend la disposition de non-discrimination à la discrimination entre les déterminations *ex ante* et *ex post* de la fiabilité. Il traite uniquement du refus d'effets juridiques en cas de recours à un système de gestion de l'identité non désigné, et n'a donc pas d'incidence sur l'article 9-2, qui accorde des effets juridiques *plus importants* à la détermination *ex ante* de la fiabilité sous la forme d'une présomption réfutable de fiabilité.

[25] *Reconnaissance juridique de la gestion de l'identité – non-discrimination* : À sa cinquante-neuvième session, le Groupe de travail est convenu que l'objectif de non-discrimination tel qu'il est présenté dans le chapeau de l'article 5-1 (c'est-à-dire la chose protégée par la disposition de non-discrimination) devrait être « la vérification d'identité » (A/CN.9/1005, par. 86) et que, dans ce contexte, « vérification » était synonyme d'« authentification » (A/CN.9/1005, par. 85). Compte tenu de l'approche décrite au paragraphe 2, l'expression « identification électronique » est désormais utilisée.

[26] *Reconnaissance juridique de la gestion de l'identité – motifs de discrimination interdits* : À sa cinquante-neuvième session, le Groupe de travail est convenu que le motif de discrimination interdit énoncé au paragraphe 1 a) devrait être le fait que « l'identification et la vérification » se présentent sous une forme électronique (voir A/CN.9/1005, par. 86). Compte tenu de l'approche décrite au paragraphe 2, et conformément à la définition des « services de gestion de l'identité » figurant à l'article premier, les expressions « contrôle d'identité » et « identification électronique » sont désormais utilisées.

[27] *Obligations incombant aux prestataires de services de gestion de l'identité* : Les obligations prévues à l'article 6 ont été élaborées en consultation avec des experts à la suite d'une demande formulée par le Groupe de travail à sa cinquante-huitième session (A/CN.9/971, par. 67). La disposition a été révisée pour tenir compte de la décision prise par le Groupe de travail à sa cinquante-neuvième session de modifier l'alinéa a) i) pour donner effet au principe de minimisation des données (A/CN.9/1005, par. 93).

ii) De suspendre, de révoquer et de réactiver les justificatifs ; et

iii) De renouveler et de remplacer les justificatifs ;

d) De gérer l'identification électronique des [sujets][personnes], en ayant notamment soin :

i) De gérer les facteurs d'identification électronique ; et

ii) De gérer les mécanismes d'identification électronique ;

e) De garantir la disponibilité en ligne et le bon fonctionnement des systèmes de gestion de l'identité ; et

f) D'assurer un accès raisonnable aux règles qui régissent les systèmes de gestion de l'identité.

Article 7. Obligations incombant aux prestataires de services de gestion de l'identité en cas de violation des données[28]

1. En cas d'atteinte à la sécurité ou de perte d'intégrité ayant une incidence importante sur un système de gestion de l'identité, notamment sur les attributs qui y sont gérés, les prestataires de services de gestion de l'identité sont tenus :

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 ;

c) De notifier l'atteinte ou la perte conformément à la loi applicable.

2. Si [un sujet][une personne] leur notifie une atteinte à la sécurité ou une perte d'intégrité, les prestataires de services de gestion de l'identité sont tenus :

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[29]

L'abonné informe le prestataire de services de gestion de l'identité si :

a) Il sait que les justificatifs d'identité ou les mécanismes d'identification électronique du système de gestion de l'identité concerné ont été compromis ; ou

b) Des circonstances dont il a connaissance engendrent un risque important que les justificatifs d'identité ou les mécanismes d'identification électronique aient été compromis.

---

[28] *Obligations incombant aux prestataires de services de gestion de l'identité en cas de violation des données* : L'article 7 a été révisé pour tenir compte des décisions prises par le Groupe de travail à sa cinquante-neuvième session (A/CN.9/1005, par. 94 et par. 32 à 36). En particulier, le Groupe de travail est convenu que les obligations incombant aux prestataires de services de gestion de l'identité en cas de violation des données devraient être formulées sur le modèle des obligations incombant aux prestataires de services de confiance en cas de violation des données, qui sont énoncées à l'article 14-2. Pour un examen plus approfondi de la portée de ces obligations, voir les notes de bas de page 43 et 44.

[29] *Obligations incombant aux abonnés* : L'article 8 a été révisé pour tenir compte des décisions prises par le Groupe de travail à sa cinquante-neuvième session (A/CN.9/1005, par. 96 et par. 37 à 43). En particulier, le Groupe de travail est convenu que les obligations incombant aux abonnés aux services de gestion de l'identité devraient être alignées sur celles incombant aux abonnés aux services de confiance, qui sont énoncées à l'article 14. Pour un examen plus approfondi de la portée de ces obligations, voir les notes de bas de page 45 et 46.

Article 9. Identification d'[un sujet][une personne] au moyen de la gestion de l'identité[30]

Option A

1. Lorsqu'une règle de droit exige ou permet l'identification d'[un sujet][une personne], cette règle est satisfaite dans le cas de la gestion de l'identité si une méthode fiable est employée pour l'identification électronique de [ce sujet][cette personne][31].

Option B

1. Un sujet peut être identifié au moyen de services de gestion de l'identité si une méthode fiable est employée pour l'identification électronique de [ce sujet][cette personne][32].

2. Une méthode est présumée fiable aux fins du paragraphe 1 si un système de gestion de l'identité désigné conformément à l'article 11 est utilisé.

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

a) D'établir par tout autre moyen, aux fins du paragraphe 1, la fiabilité d'une méthode au regard de l'article 10 ; ou

b) D'apporter des preuves de la non-fiabilité d'un système de gestion de l'identité désigné[33].

Article 10. Facteurs pertinents pour déterminer la fiabilité

1. Pour déterminer la fiabilité de la méthode aux fins de l'article 9, 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 qui régissent l'exploitation du système de gestion de l'identité aux normes et procédures internationales reconnues, notamment au cadre relatif aux niveaux de garantie, une attention particulière étant accordée aux règles qui régissent :

---

[30] *Reconnaissance juridique de la gestion de l'identité – généralités* : Cette disposition vise à assurer une reconnaissance juridique en ce qui concerne l'utilisation de la gestion de l'identité à des fins d'identification. Deux options sont soumises à l'examen du Groupe de travail. L'option A de l'article 9 a été révisée pour tenir compte des décisions prises par le Groupe de travail à sa cinquante-neuvième session (A/CN.9/1005, par. 98, 99 et 101). Lors de cette session, il a été noté que l'article 9 s'appliquerait normalement lorsque les parties étaient convenues d'utiliser un service de gestion de l'identité pour s'identifier mutuellement (A/CN.9/1005, par. 97). En vertu de l'article 2-2 b), l'article 9 ne se substitue pas à une exigence légale prévue par la loi applicable selon laquelle un sujet doit être identifié suivant une procédure définie ou prescrite.

[31] *Reconnaissance juridique de la gestion de l'identité – équivalent hors ligne* : L'option A de l'article 9 conserve l'approche de l'équivalence fonctionnelle des projets antérieurs. Il a été noté précédemment qu'une disposition fondée sur l'équivalence fonctionnelle supposait la désignation d'un équivalent hors ligne (A/CN.9/965, par. 66). À sa cinquante-neuvième session, le Groupe de travail est convenu que l'équivalent hors ligne était l'« identification d'un sujet », dont il fait mention dans le titre de l'article.

[32] *Reconnaissance juridique de la gestion de l'identité* : L'option B de l'article 9 vise à affirmer la légalité du recours à l'identification électronique sans appliquer une approche d'équivalence fonctionnelle. Le Groupe de travail voudra peut-être garder à l'esprit l'article 5 lorsqu'il examinera cette option.

[33] *Présomption de fiabilité* : À sa cinquante-neuvième session, le Groupe de travail est convenu que l'article 9 devrait être remanié sur le modèle des dispositions équivalentes énonçant les exigences applicables en matière de services de confiance (c'est-à-dire, les articles 16 à 22) (A/CN.9/1005, par. 99). En conséquence, on a inséré les paragraphes 2 et 3 qui se fondent sur les paragraphes 2 et 3 de l'article 16 et remplacent effectivement les paragraphes 4 et 5 de l'article 11 du projet précédent.

i) La gouvernance ;

ii) La publication d'avis et l'information des 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 système de gestion de l'identité ; et

d) Tout accord entre les parties.

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

a) Du lieu où le système de gestion de l'identité est exploité ; ni

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

Article 11. Désignation des systèmes de gestion de l'identité fiables[34]

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 systèmes de gestion de l'identité qui sont fiables aux fins de l'article 9.

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 système de gestion de l'identité ; et

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

3. Toute désignation arrêtée en vertu du paragraphe 1 doit être conforme aux normes et procédures internationales reconnues de détermination de la fiabilité des systèmes de gestion de l'identité, notamment aux cadres relatifs aux niveaux de garantie.

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

a) Du lieu où le système de gestion de l'identité est exploité ; ni

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

[34] *Désignation des systèmes de gestion de l'identité fiables :* L'article 11 établit un mécanisme pour la détermination *ex ante* des systèmes d'identification fiables. Il a été révisé pour tenir compte des décisions prises par le Groupe de travail à sa cinquante-neuvième session (A/CN.9/1005, par. 102) et a donc été reformulé sur le modèle de la disposition correspondante du chapitre II qui traite de la détermination *ex ante* des services de confiance fiables (art. 24). Pour un examen plus approfondi des différents éléments de cette disposition, voir les notes de bas de page 63 et 64.

Article 12. Responsabilité des prestataires de services de gestion de l'identité[35]

Option A

[La responsabilité des prestataires de services de gestion de l'identité est déterminée conformément à la loi applicable.][36]

Option B

Un prestataire de services de gestion de l'identité assume les conséquences juridiques de tout manquement aux obligations qui lui incombent en vertu [du présent instrument].

Option C

1. Les prestataires de services de gestion de l'identité sont tenus responsables des dommages causés intentionnellement ou par négligence à quiconque en raison de manquements aux obligations qui leur incombent [en vertu du présent instrument][37].

2. Le paragraphe 1 s'applique conformément aux règles prévues par la loi applicable en matière de responsabilité.

3. Nonobstant les dispositions du paragraphe 1, les prestataires de services de gestion de l'identité ne sont pas tenus responsables envers l'abonné des dommages découlant de l'utilisation d'un système de gestion de l'identité dans la mesure où :

a) Cette utilisation dépasse 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 ; et

b) Le prestataire de services de gestion de l'identité a notifié ces limitations à l'abonné conformément à la loi applicable.

Chapitre III. Services de confiance[38]

Article 13. Reconnaissance juridique des services de confiance[39]

Les [qualités d'un message de données garanties][40] [données qui sont échangées, vérifiées ou authentifiées] par l'utilisation ou à l'aide d'un service de confiance ne

---

[35] *Responsabilité des prestataires de services de gestion de l'identité* : À sa cinquante-neuvième session, le Groupe de travail a décidé de ne pas inclure de disposition « refuge » exonérant de responsabilité les prestataires de services de gestion de l'identité sous certaines conditions (A/CN.9/1005, par. 104). Pour le reste, le Groupe de travail est convenu de réexaminer la responsabilité des prestataires de services de gestion de l'identité conjointement avec la responsabilité des prestataires de services de confiance (A/CN.9/1005, par. 106). En conséquence, l'article 12 a été révisé pour faire pendant aux options présentées à l'article 25. Trois options sont soumises à l'examen du Groupe de travail.

[36] Le Groupe de travail voudra peut-être se demander si cette disposition devrait être conservée dans le cas où le projet d'instrument prendrait la forme d'une loi type ou si elle serait superflue, dès lors que son effet juridique serait produit en vertu de principes juridiques généraux.

[37] Cette disposition se fonde sur le projet de libellé dont le Groupe de travail est convenu à sa cinquante-huitième session (A/CN.9/971, par. 101). Ce projet a été modifié afin de préciser la cause des dommages pour lesquels la responsabilité est imposée.

[38] Le chapitre relatif aux services de confiance comporte une disposition générale sur la reconnaissance juridique des services de confiance (art. 13) ; une norme de fiabilité générale assortie d'une clause de non-discrimination géographique destinée à faciliter la reconnaissance internationale (art. 23) ; un mécanisme de désignation *ex ante* des services de confiance fiables (art. 24) ; une disposition sur la responsabilité (art. 25) ; et une liste de services de confiance (art. 16 à 22).

[39] *Reconnaissance juridique des services de confiance – généralités* : L'article 13 a été révisé pour tenir compte des décisions prises par le Groupe de travail à sa cinquante-neuvième session (A/CN.9/1005, par. 26).

[40] La formulation « Les qualités d'un message de données garanties » est proposée pour aligner

sont pas privées de leurs effets juridiques, de leur validité ou de leur force exécutoire, ou leur admissibilité comme preuve[41] n'est pas refusée au seul motif que :

a) Elles se présentent sous forme électronique ; ou

b) Elles ne sont pas associées à un service de confiance désigné conformément à l'article 24.

Article 14. Obligations incombant aux prestataires de services de confiance

1. Le prestataire de services de confiance[42] :

a) Agit en conformité avec les déclarations qu'il fait concernant ses politiques et pratiques ; et

b) Rend ces politiques et pratiques facilement accessibles aux abonnés.

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 :

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[43] ;

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

c) De notifier l'atteinte ou la perte conformément à la loi applicable[44].

---

davantage l'article 13 sur la définition des « services de confiance ».

[41] Il est proposé d'insérer les mots « ou de leur admissibilité comme preuve » de façon à aligner cette disposition sur l'article 5.

[42] *Obligations incombant aux prestataires de services de confiance – respect des politiques et pratiques* : L'article 14-1 a été révisé pour tenir compte des décisions prises par le Groupe de travail à sa cinquante-neuvième session (A/CN.9/1005, par. 31 et 73). En ce qui concerne le paragraphe 1 b), le Groupe de travail s'est accordé sur le texte suivant : « [C]es politiques et pratiques sont rendues facilement accessibles aux abonnés », qui a été refondu dans le présent projet pour préciser qu'il s'agit d'une obligation imposée au prestataire de services. Le Groupe de travail voudra peut-être examiner si l'obligation devrait être alignée sur celle faite aux prestataires de services de gestion de l'identité, à l'alinéa f) de l'article 6, « [D]'assurer un accès raisonnable aux règles qui régissent les systèmes de gestion de l'identité ».

[43] *Obligations incombant aux prestataires de services de confiance – mettre fin à l'atteinte à la sécurité* : L'article 14-2 a) du projet précédent imposait l'obligation de suspendre les services de confiance touchés par une atteinte à la sécurité jusqu'à ce qu'il ait été « mis fin » à l'atteinte, ou bien jusqu'à ce qu'un nouveau certificat ou équivalent ait été délivré (voir également A/CN.9/WG.IV/WP.154, par. 47). Estimant que d'autres mesures que la suspension totale pourraient être appropriées, le Groupe de travail est convenu à sa cinquante-neuvième session que le prestataire de services de confiance devrait plutôt être tenu de « prendre toutes les mesures raisonnables » (A/CN.9/1005, par. 33). L'article 14-2 a) du présent projet tient compte de cette décision et précise que les mesures doivent viser à mettre fin à l'atteinte. Le Groupe de travail voudra peut-être examiner si la référence au fait de « mettre fin » à l'atteinte reflète l'objectif souhaité des mesures à prendre par le prestataire de services de confiance pour remédier à une atteinte à la sécurité.

[44] *Obligations incombant aux prestataires de services de confiance – notification de l'atteinte à la sécurité* : L'article 14-3 du projet précédent imposait une obligation de notification au prestataire de services de confiance, qui précisait a) à qui et b) dans quel délai cette notification devait être faite. À sa cinquante-neuvième session, le Groupe de travail est convenu que l'instrument devrait renvoyer à la loi applicable à ces questions (A/CN.9/1005, par. 36).

Article 15. Obligations incombant aux abonnés

L'abonné informe le prestataire de services de confiance si [45]:

a) Il sait que le service de confiance a été compromis d'une manière qui en affecte la fiabilité [46]; ou

b) Des circonstances dont il a connaissance engendrent un risque important que le service de confiance ait été compromis.

Article 16. Signatures électroniques

1. Lorsqu'une règle de droit exige ou permet la signature d'une personne, cette règle est satisfaite dans le cas d'un message de données si une méthode fiable est utilisée pour :

a) Identifier la personne ;

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

2. Une méthode est présumée fiable aux fins du paragraphe 1 si une signature électronique désignée conformément à l'article 24 est utilisée.

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

a) D'établir par tout autre moyen, aux fins du paragraphe 1, la fiabilité d'une méthode au regard de l'article 23 ; ou

b) D'apporter des preuves de la non-fiabilité d'une signature électronique désignée[47].

Article 17. Cachets électroniques

1. Lorsqu'une règle de droit exige ou permet qu'une personne morale[48] appose un cachet, cette règle est satisfaite dans le cas d'un message de données si une méthode fiable est utilisée pour :

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

b) Détecter toute altération du message de données après le moment de l'apposition, en dehors de l'ajout de tout endossement et de toute modification

---

[45] *Obligations incombant aux abonnés – généralités* : À sa cinquante-neuvième session, le Groupe de travail est convenu que l'instrument ne devrait pas imposer d'obligations aux parties s'étant fiées aux services (A/CN.9/1005, par. 38 à 40, 95 et 96).

[46] *Obligations incombant aux abonnés – déclenchement* : Alors que l'obligation imposée aux prestataires de services de confiance à l'article 14-2 est déclenchée en cas « d'atteinte à la sécurité ou de perte d'intégrité », l'obligation imposée aux abonnés à l'article 15 est déclenchée par le fait que le service de confiance a été « compromis ». À la cinquante-neuvième session du Groupe de travail, il a été proposé que l'article 15 porte sur la fiabilité des services de confiance (A/CN.9/1005, par. 37). L'ajout des mots « d'une manière qui en affecte la fiabilité » dans le présent projet tient compte de cette proposition. Une formulation similaire figure à l'article 10, paragraphe 1, du règlement eIDAS.

[47] *Signatures électroniques – présomption de fiabilité* : À sa cinquante-neuvième session, le Groupe de travail est convenu que les services de confiance qui sont réputés fiables sur la base d'une approche *ex ante* (c'est-à-dire conformément à l'article 24) devraient bénéficier d'effets juridiques plus importants sous la forme d'une présomption réfutable de fiabilité (A/CN.9/1005, par. 12). Il est aussi convenu que cette présomption devrait figurer dans chaque disposition énonçant les exigences applicables en matière de services de confiance (c'est-à-dire les articles 16 à 22) (A/CN.9/1005, par. 51). Les articles 16-2 et 16-3 tiennent compte de cette décision et remplacent respectivement les articles 24-4 et 24-5, du projet précédent. L'article 16-3 fait pendant à l'article 6-4 de la Loi type sur les signatures électroniques (LTSE) (publication des Nations Unies, numéro de vente : F.02.V.8).

[48] *Cachets électroniques – limitation aux personnes morales* : À sa cinquante-neuvième session, le Groupe de travail est convenu que les cachets électroniques n'étaient créés que par des personnes morales et que, par conséquent, l'article 17 du précédent projet (art. 18 du présent projet) devrait s'en tenir aux abonnés qui sont des personnes morales (A/CN.9/1005, par. 52 et 54).

intervenant dans le cours normal de la communication, de la conservation et de l'exposition[49].

2. Une méthode est présumée fiable aux fins du paragraphe 1 si un cachet électronique désigné conformément à l'article 24 est utilisé.

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

a) D'établir par tout autre moyen, aux fins du paragraphe 1, la fiabilité d'une méthode au regard de l'article 23 ; ou

b) D'apporter des preuves de la non-fiabilité d'un cachet électronique désigné[50].

Article 18. Horodatages électroniques

1. Lorsqu'une règle de droit exige ou permet que certains documents, documents d'activité ou certaines informations ou données soient accompagnés d'une indication de date et d'heure, cette règle est satisfaite dans le cas d'un message de données si une méthode fiable est utilisée 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[51].

2. Une méthode est présumée fiable aux fins du paragraphe 1 si un horodatage électronique désigné conformément à l'article 24 est utilisé.

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

a) D'établir par tout autre moyen, aux fins du paragraphe 1, la fiabilité d'une méthode au regard de l'article 23 ; ou

b) D'apporter des preuves de la non-fiabilité d'un horodatage électronique désigné[52].

Article 19. Archivage électronique

1. Lorsqu'une règle de droit exige ou permet que certains documents, documents d'activité ou certaines informations soient conservés, cette règle est satisfaite dans le cas de l'archivage d'un message de données[53], si :

a) L'information que contient ce message est accessible pour être consultée ultérieurement ; et

---

[49] *Cachets électroniques – fonction* : À sa cinquante-neuvième session, le Groupe de travail est convenu que la fonction d'un cachet électronique était de garantir l'origine et l'intégrité des données auxquelles il était associé (A/CN.9/1005, par. 52 et 54). L'assurance de l'origine est prévue à l'alinéa a), tandis que celle de l'intégrité est prévue à l'alinéa b). Il a été estimé que l'assurance de l'origine remplissait la même fonction que l'identification de la personne morale créant le cachet (A/CN.9/1005, par. 52), auquel cas il était concevable que l'origine des données puisse être garantie par l'utilisation d'une signature électronique. La mention prévoyant, à l'alinéa b), « l'ajout de tout endossement et de toute modification intervenant dans le cours normal de la communication, de la conservation et de l'exposition » tient compte de ce dont est convenu le Groupe de travail (A/CN.9/1005, par. 56 à 58).

[50] *Cachets électroniques – présomption de fiabilité* : Voir note de bas de page 47.

[51] *Horodatages électroniques – généralités* : L'article 18 a été révisé pour tenir compte des décisions prises par le Groupe de travail à sa cinquante-neuvième session (A/CN.9/1005, par. 55).

[52] *Horodatages électroniques – présomption de fiabilité* : Voir note de bas de page 47.

[53] *Services d'archivage électronique – généralités* : Le projet précédent faisait référence à l'archivage électronique en précisant « si ce sont des messages de données qui sont conservés ». Dans un souci d'alignement sur la formulation d'autres dispositions relatives aux services de confiance et sur le reste du paragraphe 1, ainsi que sur la formulation utilisée par le Groupe de travail à sa cinquante-neuvième session (A/CN.9/1005, par. 59), le présent projet mentionne « l'archivage d'un message de données ».

b) Une méthode fiable est utilisée pour :

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

ii) Détecter toute altération du message de données après cette date et cette heure, en dehors de l'ajout de tout endossement et de toute modification intervenant dans le cours normal de la communication, de la conservation et de l'exposition[54].

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, sont conservées si elles existent[55].

2. Une méthode est présumée fiable aux fins du paragraphe 1 b) si un service d'archivage électronique désigné conformément à l'article 24 est utilisé.

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

a) D'établir par tout autre moyen, aux fins du paragraphe 1, la fiabilité d'une méthode au regard de l'article 23 ; ou

b) D'apporter des preuves de la non-fiabilité d'un service d'archivage électronique désigné[56].

Article 20. Services d'envoi recommandé électroniques

1. Lorsqu'une règle de droit exige ou permet que certains documents, documents d'activité ou certaines informations soient envoyés par courrier recommandé ou au moyen d'un service similaire[57], cette règle est satisfaite dans le cas d'un message de données si une méthode fiable est utilisée pour :

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

b) Indiquer la date et l'heure auxquelles le message de données a été envoyé[58].

2. Une méthode est présumée fiable aux fins du paragraphe 1 si un service d'envoi recommandé électronique désigné conformément à l'article 24 est utilisé.

---

[54] *Services d'archivage électronique – fonction* : À sa cinquante-neuvième session, le Groupe de travail est convenu qu'une fonction essentielle de l'archivage électronique était de garantir l'intégrité des données (A/CN.9/1005, par. 59). Conformément à la décision prise par le Groupe de travail, l'alinéa b) ii) a été reformulé pour tenir compte des critères d'évaluation de l'intégrité définis à l'article 17-1 b).

[55] 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 la LTCE, art. 10-2).

[56] *Services d'archivage électronique – présomption de fiabilité* : Voir note de bas de page 47.

[57] *Services d'envoi recommandé électroniques – équivalent hors ligne* : Le projet précédent faisait référence à une règle de droit exigeant ou permettant « la preuve de l'expédition et de la réception » d'un document, etc. À la cinquante-neuvième session du Groupe de travail, il a été estimé que l'on pourrait obtenir une formulation plus appropriée en mettant l'accent sur l'équivalence fonctionnelle entre les services de courrier recommandé et les services d'envoi recommandé électroniques. En conséquence, le chapeau de l'article 20-1 a été révisé pour faire référence à une règle de droit exigeant que le document, etc., soit envoyé « par courrier recommandé ou au moyen d'un service similaire ».

[58] *Services d'envoi électroniques – fonction* : À sa cinquante-neuvième session, le Groupe de travail est convenu que la fonction essentielle d'un service d'envoi électronique était de fournir l'assurance « de l'heure à laquelle le message de données était reçu pour envoi par le service d'envoi recommandé électronique et de l'heure à laquelle ce message était envoyé au destinataire par ce système » (A/CN.9/1005, par. 64). L'article 20-1 du présent projet a été reformulé en conséquence, bien que la disposition fasse référence à une « indication » de temps, conformément à la terminologie utilisée à l'article 18- 1. Le Groupe de travail voudra peut-être examiner si cette disposition devrait exiger expressément que le service d'envoi électronique garantisse l'intégrité du message de données, confirme sa réception et son envoi et identifie l'expéditeur et/ou le destinataire. On peut avancer que ces fonctions sont déjà visées par les alinéas a) et b).

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

a) D'établir par tout autre moyen, aux fins du paragraphe 1, la fiabilité d'une méthode au regard de l'article 23 ; ou

b) D'apporter des preuves de la non-fiabilité d'un service d'envoi recommandé électronique désigné[59].

Article 21. Authentification de site Internet

Lorsqu'une règle de droit exige ou permet l'authentification d'un site Internet, cette règle est satisfaite si une méthode fiable est utilisée pour identifier la personne qui détient le nom de domaine du site Internet et pour associer celle-ci audit site[60].

Article 22. Authentification d'objet

Lorsqu'une règle de droit exige ou permet l'authentification d'un objet, cette règle est satisfaite si une méthode fiable est employée à cet effet[61].

Article 23. Norme de fiabilité pour les services de confiance[62]

1. Pour déterminer la fiabilité de la méthode aux fins des articles 16 à 22, toutes les circonstances pertinentes sont prises en considération, notamment :

a) Toute règle de fonctionnement applicable au service de confiance, y compris toute interruption prévue d'activité visant à assurer la continuité ;

b) Toutes normes et procédures internationales reconnues qui sont applicables ;

c) Toute norme sectorielle applicable ;

d) La sûreté du matériel et des logiciels ;

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

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

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

h) Toute convention en la matière.

2. Une méthode est jugée fiable s'il est démontré dans les faits qu'elle a rempli les fonctions associées au service de confiance considéré.

---

[59] *Services d'envoi électronique – présomption de fiabilité* : Voir note de bas de page 47.

[60] *Authentification de site Internet – fonction* : À sa cinquante-neuvième session, le Groupe de travail est convenu que la fonction essentielle de l'authentification de site Internet était de relier ledit site à la personne à laquelle le nom de domaine avait été attribué ou concédé sous licence (A/CN.9/1005, par. 66). Dans le présent projet, l'expression « détenteur du nom de domaine » est utilisée pour désigner les personnes auxquelles le droit d'utiliser le nom de domaine a été attribué ou concédé sous licence par un bureau d'enregistrement de noms de domaine. Jusqu'à présent, le Groupe de travail s'est concentré sur les circonstances dans lesquelles une partie (par exemple, le propriétaire du site Internet) accepte d'authentifier un site, plutôt que sur celles dans lesquelles elle le fait afin de satisfaire à une règle de droit qui « exige » une telle authentification. Dans ces conditions, la partie agirait en vertu d'une règle de droit qui « permet » cette authentification.

[61] *Authentification d'objet – fonction* : Le Groupe de travail voudra peut-être se demander s'il y a lieu d'insérer un article 23 pour faire référence à tous les cas d'identification d'objets matériels et numériques. Ce faisant, il voudra peut-être examiner la définition proposée pour le terme « authentification » et la révision proposée pour la définition du terme « objet » afin d'exclure les objets du champ d'application des dispositions relatives à la gestion de l'identité.

[62] *Norme de fiabilité* : L'article 23 a été révisé pour tenir compte des décisions prises par le Groupe de travail à sa cinquante-neuvième session (A/CN.9/1005, par. 67 et 68).

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

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

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

Article 24. Désignation de services de confiance fiables[63]

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 fiables aux fins des articles 16 à 22.

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 23, pour désigner un système de confiance ; et

b) De publier une liste des systèmes de confiance désignés, en mentionnant notamment les coordonnées des prestataires de services de confiance[64].

3. Toute désignation arrêtée en vertu du paragraphe 1 doit être conforme aux normes et procédures internationales reconnues de détermination de la fiabilité des services de confiance, notamment aux cadres relatifs aux niveaux de fiabilité.

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

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

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

---

[63] *Désignation de services de confiance fiables – généralités* : L'article 24 établit un mécanisme pour la détermination *ex ante* de services de confiance fiables. Les paragraphes 1 et 4 (par. 3 du projet précédent) ont été révisés pour tenir compte de la décision prise par le Groupe de travail à sa cinquante-neuvième session selon laquelle la désignation devrait avoir pour objet les services de confiance et non les méthodes utilisées par ceux-ci (A/CN.9/1005, par. 69). Il a été expliqué à cette occasion que la désignation ne s'appliquait pas à des types génériques de services de confiance ou à l'ensemble des services de confiance offerts par un prestataire de services de confiance particulier, mais à un service de confiance déterminé fourni par un prestataire de services donné.

[64] *Désignation de services de confiance fiables – obligations de l'autorité de désignation* : Un nouveau paragraphe 2 a été inséré pour tenir compte de la décision prise par le Groupe de travail à sa cinquante-neuvième session d'imposer deux nouvelles obligations à l'autorité de désignation (A/CN.9/1005, par. 73). Le paragraphe 2 a) vise à assurer un certain degré de cohérence entre les services de confiance qui sont désignés comme fiables selon une approche *ex ante* et ceux qui satisfont à la norme de fiabilité énoncée à l'article 23 selon une approche *ex post*. Le paragraphe 2 b) vise à promouvoir la transparence et à informer les abonnés potentiels du service de confiance concerné (A/CN.9/1005, par. 70).

Article 25. Responsabilité des prestataires de services de confiance[65]

Option A

[La responsabilité des prestataires de services de confiance est déterminée conformément à la loi applicable.][66]

Option B

Un prestataire de services de confiance assume les conséquences juridiques de tout manquement aux obligations qui lui incombent en vertu du [présent instrument].

Option C

1. Les prestataires de services de confiance sont tenus responsables des dommages causés intentionnellement ou par négligence à quiconque en raison de manquements aux obligations qui leur incombent [en vertu du présent instrument].

2. Le paragraphe 1 s'applique conformément aux règles prévues par la loi applicable en matière de responsabilité.

3. Nonobstant les dispositions du paragraphe 1, les prestataires de services de confiance ne sont pas tenus responsables envers l'abonné des dommages découlant de l'utilisation d'un service de confiance dans la mesure où :

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

b) Le prestataire de services de confiance a notifié ces limitations à l'abonné conformément à la loi applicable.

---

[65] *Responsabilité des prestataires de services de confiance* : À sa cinquante-neuvième session, le Groupe de travail s'est largement prononcé en faveur du maintien d'une disposition sur la responsabilité, afin d'assurer la sécurité juridique. Plusieurs propositions ont été avancées. Le Groupe de travail a demandé au Secrétariat de reformuler l'article 25 en tenant compte de ces propositions, en vue d'un examen ultérieur. L'article 25 du présent projet a été refondu en conséquence. L'option A adopte l'approche minimaliste en rappelant que la responsabilité du prestataire de services de confiance, y compris toute limitation de celle-ci, doit être déterminée en fonction de la loi applicable. L'option B adopte l'approche suivie à l'article 9-2 de la LTSE. Tout en conservant les limitations de responsabilité prévues par la loi applicable, elle précise qu'un manquement du prestataire de services de confiance aux obligations énoncées dans le projet d'instrument entraînera certaines conséquences juridiques. L'option C est celle qui donne le plus d'orientations en s'appuyant sur l'article 25 du projet précédent. Elle comprend un nouveau paragraphe 2, fondé sur l'article 11, paragraphe 4, du règlement eIDAS. Le paragraphe 3 a été révisé pour tenir compte des décisions du Groupe de travail (A/CN.9/1005, par. 76).

[66] Le Groupe de travail voudra peut-être se demander si cette disposition devrait être conservée dans le cas où le projet d'instrument prendrait la forme d'une loi type ou si elle serait superflue, dès lors que son effet juridique serait produit en vertu de principes juridiques généraux.

Chapitre IV. Aspects internationaux

Article 26. Reconnaissance internationale de la gestion de l'identité et des services de confiance[67]

1. Un système de gestion de l'identité exploité ou un service de confiance fourni en dehors de [*l'État adoptant*] a les mêmes effets juridiques dans [*l'État adoptant*] qu'un système de gestion de l'identité exploité ou un service de confiance fourni dans [*l'État adoptant*] à condition qu'il offre un niveau de fiabilité substantiellement équivalent[68].

2. 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].

Article 27. Coopération[69]

[*Toute personne, tout organe ou toute autorité, de droit public ou privé, indiqué[e] par l'État adoptant comme compétent[e] en la matière*] [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 reconnaissance des effets juridiques des systèmes de gestion de l'identité et des services de confiance étrangers, qu'elle soit accordée unilatéralement ou d'un commun accord ;

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

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

---

[67] *Reconnaissance internationale – généralités* : L'article 26 s'inspire de l'article 12-2 de la LTSE. Cette disposition a pour objet « de définir le critère général pour la reconnaissance transfrontière des certificats, faute de quoi les prestataires de services de certification seraient astreints à la lourde obligation d'obtenir des licences dans un grand nombre de pays » (voir *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, deuxième partie, par. 153). L'article 26 vise à donner des orientations pour la mise en œuvre d'autres dispositions du projet d'instrument relatives à la reconnaissance internationale, à savoir : L'article 10-2 (origine géographique non pertinente aux fins de la détermination de la fiabilité des méthodes de gestion de l'identité) ; l'article 11-4 (origine géographique non pertinente aux fins de la désignation de méthodes de gestion de l'identité fiables) ; l'article 23-3 (origine géographique non pertinente aux fins de la détermination de la fiabilité des services de confiance) et l'article 24-4 (origine géographique non pertinente aux fins de la désignation de services de confiance fiables). Les articles 10-2, 11-4, 23-3 et 24-4 sont fondés sur l'article 12-1 de la LTSE, qui établit une règle générale de non-discrimination pour la détermination de l'efficacité juridique d'un certificat ou d'une signature électronique (voir *Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation 2001*, deuxième partie, paragraphe 152). Pour faciliter ces délibérations, le Groupe de travail voudra peut-être revoir son examen de l'interaction entre les articles 12-1 et 12-2 de la LTSE, dont il est rendu compte dans le document A/CN.9/483, par. 28 à 36.

[68] *Reconnaissance internationale – niveau d'équivalence* : À la cinquième-neuvième session du Groupe de travail, différents points de vue ont été exprimés quant au niveau d'équivalence requis pour que des effets juridiques se produisent à l'échelle internationale. Le présent projet fait pendant à l'article 12-2 de la LTSE, qui exige une équivalence « substantielle ». Une autre option proposée dans le projet précédent consistait dans une équivalence exacte (c'est-à-dire que le service étranger devait offrir « le même niveau de fiabilité »).

[69] *Coopération internationale* : L'article 27 a été révisé pour tenir compte des décisions prises par le Groupe de travail à sa cinquante-neuvième session (A/CN.9/1005, par. 122).