Nations Unies A/CN.9/WG.IV/WP.167

Assemblée générale

Distr. limitée
26 janvier 2021
Français
Original : anglais

Commission des Nations Unies pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Soixante et unième session
New York (en ligne), 5-9 avril 2021

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.21-00519 (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 tenus par le Groupe de travail à sa soixantième session (Vienne, 19-23 octobre 2020), dont il est rendu compte dans le document A/CN.9/1045[1].

2. On trouvera un historique des travaux en cours du Groupe de travail IV dans le document A/CN.9/WG.IV/WP.166 (par. 4 à 17).

[1] Dans les notes de bas de page accompagnant le présent projet, le projet de dispositions examiné par le Groupe de travail à sa soixantième session, tel qu'il figure dans le document A/CN.9/WG.IV/WP.162, est appelé la « version précédente ». Le projet fait également référence à d'autres textes de la CNUDCI sur le commerce électronique, à savoir la Loi type de la CNUDCI sur le commerce électronique (« LTCE »), la Loi type de la CNUDCI sur les signatures électroniques (« LTSE »), la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (« CCE ») et la Loi type de la CNUDCI sur les documents transférables électroniques.

Annexe

Projet de dispositions[2] 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 une personne ;

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

c) Par « identification électronique » [« authentification »], dans le cadre des services de gestion de l'identité, on entend un processus utilisé pour obtenir une garantie suffisante du lien unissant une personne à une identité[3] ;

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

e) Par « justificatifs d'identité », on entend les données, ou l'objet matériel sur lequel elles se trouvent, qu'une personne peut présenter à des fins d'identification électronique[4] ;

f) Par « services de gestion de l'identité », on entend des services consistant à gérer le contrôle d'identité ou l'identification électronique de personnes sous forme électronique[5] ;

---

[2] *Forme de l'instrument* : Lors des discussions préliminaires tenues 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.

[3] *Définitions – « identification électronique »* : Le présent projet utilise toujours le terme « identification électronique » plutôt que « authentification », pour répondre aux préoccupations exprimées concernant les significations multiples du terme « authentification » (A/CN.9/1005, par. 13, 84 à 86 et 92). À la soixantième session du Groupe de travail, on a préconisé l'utilisation du terme « authentification » (A/CN.9/1045, par. 134) et le Groupe de travail est convenu de placer entre crochets les définitions des termes « authentification » et « identification électronique » en vue d'un examen ultérieur (ibid., par. 136). Comme la définition du terme « authentification » dans la version précédente n'était utilisée que dans le contexte des services de confiance (comme « un processus utilisé pour attribuer un identifiant à un objet »), c'est le terme « authentification » (et non la définition de ce terme) qui a été placé entre crochets dans le présent projet.

[4] *Définitions – « justificatifs d'identité »* : Le Groupe de travail a examiné cette définition à sa soixantième session (A/CN.9/1045, par. 137). Dans le présent projet, on a modifié celle-ci en remplaçant le membre de phrase « pour permettre l'identification électronique de son identité sous forme électronique » par les mots « à des fins d'identification électronique » afin d'éviter toute redondance. Le Groupe de travail voudra peut-être confirmer cette définition telle qu'elle a été modifiée.

[5] *Définitions – « services de gestion de l'identité »* : Cette définition reflète l'idée selon laquelle la gestion de l'identité comprend deux étapes (ou phases) : le « contrôle d'identité » et l'« identification électronique ». Le Groupe de travail voudra peut-être se demander si la définition des « services de gestion de l'identité » doit faire référence aux fonctions énumérées à l'article 6 a). Dans ce cas, on pourrait ajouter les mots « , y compris les services énumérés à l'article 6 a) » à la fin de la définition.

g) Par « prestataire de services de gestion de l'identité », on entend une personne qui fournit des services de gestion de l'identité[6] ;

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

i) 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'une personne dans un contexte particulier ;

j) 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[7] ;

k) 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[8] ;

l) 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 des systèmes de gestion de l'identité et des services de confiance dans le cadre d'activités commerciales et de services touchant au commerce.

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

a) L'identification d'une personne ;

b) Le recours à un service particulier de gestion de l'identité ; 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 une personne doit être identifiée [ou un service de confiance être utilisé] suivant une procédure définie ou prescrite par la loi[9].

---

[6] *Définitions – « prestataire de services de gestion de l'identité »* : Le Groupe de travail voudra peut-être déterminer s'il convient d'insérer le mot « tout » avant « services de gestion de l'identité », pour préciser que les fonctions énumérées à l'article 6 ne sont peut-être pas toutes pertinentes pour l'ensemble des systèmes de gestion de l'identité et que, par conséquent, un prestataire de services de gestion de l'identité n'exécutera pas nécessairement chacune des fonctions énumérées (A/CN.9/1045, par. 88).

[7] *Définitions – « abonné »* : À la cinquante-neuvième session du Groupe de travail, une préférence a été exprimée en faveur de l'utilisation du terme « abonné » pour désigner la personne à laquelle les services sont fournis (A/CN.9/1005, par. 43 et 96). À sa soixantième session, le Groupe de travail a confirmé qu'il était favorable à la définition du terme « abonné » telle qu'elle figure dans le présent projet (A/CN.9/1045, par. 22). Il a été ajouté que le signataire d'une signature électronique relèverait de cette définition (ibid.), et estimé que tel ne serait pas le cas des « parties utilisatrices » (ibid., par. 18).

[8] *Définitions – « service de confiance »* : Le terme « service de confiance » n'a pas été examiné par le Groupe de travail à sa soixantième session. Conformément aux délibérations qu'il a tenues à sa cinquante-neuvième session, la définition (qui reste inchangée par rapport à la version précédente) associe une définition « abstraite » autonome, qui met l'accent sur la véracité et l'authenticité des données sous-jacentes, à une liste non exhaustive des services de confiance couverts par le projet d'instrument (A/CN.9/1005, par. 18).

[9] *Préservation des lois exigeant une procédure particulière* : L'article 2-3 s'applique pour limiter le recours à la gestion de l'identité. Le Groupe de travail souhaitera peut-être déterminer s'il convient de l'étendre pour limiter le recours aux services de confiance et, dans l'affirmative, s'il convient d'insérer le texte entre crochets. Une approche différente a été adoptée dans la Loi type de la CNUDCI sur le commerce électronique et la Loi type de la CNUDCI sur les signatures électroniques, qui limitent le recours aux services de confiance dans le champ d'application (par

4. Rien dans le présent [instrument], en dehors de ce qui y est disposé, n'a d'incidence sur l'application aux services de gestion de l'identité ou aux services de confiance de toute [règle de droit applicable, y compris de toute][10] loi applicable à la protection et à la confidentialité des données[11].

Article 3. Caractère volontaire de l'utilisation de services de gestion de l'identité et de services de confiance[12]

1. Aucune disposition du présent [instrument] n'oblige une personne à utiliser un service de gestion de l'identité ou 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.

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][13].

---

exemple, les signatures électroniques) en incitant les États adoptants à préciser des exclusions particulières (y compris en renvoyant à des lois particulières) : voir article 7-3 de la Loi type de la CNUDCI sur le commerce électronique et article premier de la Loi type de la CNUDCI sur les signatures électroniques (avec notes d'accompagnement).

[10] *Préservation des autres lois nationales* : L'article 2-4 a été rédigé avant que le Groupe de travail n'examine la forme de l'instrument. Celui-ci souhaitera peut-être déterminer si, au cas où le projet de dispositions prendrait la forme d'une loi type (voir note de bas de page 2), les mots entre crochets peuvent être supprimés. Les textes de la CNUDCI partent du principe que les dispositions d'une loi type seront incorporées dans la législation interne de l'État adoptant, à laquelle s'appliqueront les règles existantes de l'État concerné relatives aux conflits de lois. Si les lois types de la CNUDCI peuvent expressément préserver certaines lois (par exemple, l'article 1-2 de la Loi type de la CNUDCI sur les documents transférables électroniques), elles ne préservent pas l'application de « toute » autre loi en dehors de la loi type concernée. En outre, la référence à la loi « applicable » peut être comprise, à tort, comme une référence à la loi applicable en vertu des règles pertinentes du droit international privé. Voir également la note de bas de page 19 pour ce qui est de la relation entre l'article 2-4 et l'article 7.

[11] *Préservation des lois sur la protection et la confidentialité des données* : À la soixantième session du Groupe de travail, il a été dit que l'article 2-4 devrait faire référence à la « protection et à la confidentialité des données » (plutôt qu'« au respect de la vie privée et à la protection des données ») pour reconnaître que la disposition concernait la « confidentialité des données » et non le respect de la vie privée dans d'autres contextes. Le Groupe de travail souhaitera peut-être confirmer cette référence, telle qu'elle figure dans le présent projet.

[12] *Caractère volontaire de l'utilisation de services de gestion de l'identité et de services de confiance* : L'article 3 reste inchangé par rapport à la version précédente (voir A/CN.9/1045, par. 80). Il est fondé sur l'article 8-2 de la Convention sur les communications électroniques (CCE), qui traite du caractère volontaire de l'utilisation et de l'acceptation des communications électroniques. Le Groupe de travail est convenu que la disposition devrait protéger tant l'abonné que la partie utilisatrice contre l'imposition de toute obligation supplémentaire d'utiliser des services de gestion de l'identité ou des services de confiance (A/CN.9/1005, par. 116). Conformément à l'article 8-2 de la CCE, le Groupe de travail pourrait envisager d'ajouter les mots « ou à accepter » après le mot « utiliser ». Il pourrait également envisager de remplacer les mots « un service de gestion de l'identité ou un service de confiance » par « l'identification électronique ou un service de confiance ».

[13] *Principes généraux* : L'article 4-2 fait pendant à l'article 5-2 de la CCE. Le Groupe de travail voudra peut-être se demander si le texte entre crochets peut être supprimé. À sa cinquante-neuvième session, il a été expliqué qu'il était utile de faire référence à l'interprétation conformément à la loi applicable pour le cas où l'instrument prendrait la forme d'une convention (A/CN.9/1005, par. 117 ; voir précisions dans le document A/CN.9/527, par. 124). Aucune des lois types de la CNUDCI sur le commerce électronique ne contient cette référence supplémentaire.

Chapitre II. Gestion de l'identité

Article 5. Reconnaissance juridique de la gestion de l'identité[14]

Sous réserve de l'article 2, paragraphe 3, l'identification électronique d'une personne n'est pas privée de ses effets juridiques, de sa validité, de sa force exécutoire ou de sa recevabilité comme preuve au seul motif que :

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

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

Article 6. Obligations incombant aux prestataires de services de gestion de l'identité[15]

Le prestataire de services de gestion de l'identité est tenu [au minimum][16] :

a) D'avoir en place des règles de fonctionnement, des procédures et des pratiques adaptées à l'objectif et à la conception[17] du système de gestion de l'identité pour répondre [au minimum][18] aux exigences s'agissant :

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

a. De collecter et d'enregistrer les attributs ;

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

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

Comme indiqué ci-dessus (note 10), les textes de la CNUDCI partent du principe que les dispositions d'une loi type seront incorporées dans la législation interne de l'État adoptant, à laquelle s'appliqueront les règles générales d'interprétation de l'État concerné.

[14] *Reconnaissance juridique de la gestion de l'identité – généralités* : L'article 5 a été modifié pour tenir compte des décisions prises par le Groupe de travail à sa soixantième session (A/CN.9/1045, par. 84).

[15] *Obligations incombant aux prestataires de services de gestion de l'identité* : L'article 6 a été modifié pour tenir compte des décisions prises par le Groupe de travail à sa soixantième session (A/CN.9/1045, par. 95). Lors de cette session, il avait été expliqué que, dans le cas des systèmes privés de gestion de l'identité, les fonctions énumérées seraient généralement régies par des règles contractuelles. Il a été noté que les fonctions énumérées à l'article 6 ne seraient pas toutes pertinentes pour l'ensemble des prestataires de services de gestion de l'identité (par exemple, les systèmes de gestion de l'identité multipartites). Il a également été fait remarquer que l'article 6 devait garantir que le prestataire de services reste responsable pour l'intégralité des services de gestion de l'identité fournis à l'abonné (c'est-à-dire toutes les fonctions énumérées à l'article 6), et que cet article n'empêchait pas le prestataire de services d'externaliser une fonction ou de répartir les risques entre ses sous-traitants (ibid., par. 90 et 91).

[16] Les mots « au minimum » ont été insérés pour indiquer que les fonctions énumérées représentent les « obligations fondamentales » des prestataires de services de gestion de l'identité, qui peuvent être complétées par des obligations contractuelles en vertu des règles de fonctionnement (voir A/CN.9/WG.IV/WP.160). Le Groupe de travail souhaitera peut-être confirmer qu'ils ont aussi pour effet de ne laisser aucune place à des dérogations contractuelles.

[17] À la soixantième session du Groupe de travail, il a été expliqué que les mots « adaptées à l'objectif et à la conception » avaient pour but de conférer une certaine souplesse dans la conception des systèmes de gestion de l'identité (A/CN.9/1045, par. 90). Le Groupe de travail souhaitera peut-être déterminer s'il serait plus approprié de se référer à la « structure » d'un système de gestion de l'identité (plutôt qu'à sa « conception »).

[18] Les mots « au minimum » ont été insérés à l'article 6 a) pour donner suite aux délibérations tenues par le Groupe de travail à sa soixantième session, et visent à répondre à la crainte, déjà exprimée dans la note de bas de page 15, que la formulation du nouvel alinéa a) ne permette à un prestataire de services de décliner sa responsabilité pour ce qui est des fonctions liées au service de gestion de l'identité qui sont exercées par un sous-traitant (par exemple une entité distincte dans un système multipartite du secteur privé) (voir A/CN.9/1045, par. 90). Le Groupe de travail souhaitera peut-être déterminer si les mots « au minimum » figurant dans le chapeau de l'article 6 répondent déjà à cette préoccupation, et si ces mots peuvent par conséquent être supprimés de l'alinéa a) de l'article 6.

ii) D'actualiser les attributs ;

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

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

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

c. De renouveler et de remplacer les justificatifs ;

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

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

b. De gérer les mécanismes d'identification électronique ;

b) D'agir conformément aux règles de fonctionnement, aux procédures et aux pratiques ;

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

d) D'assurer un accès raisonnable aux règles de fonctionnement, aux procédures et aux pratiques ; et

e) De mettre à disposition des moyens raisonnables pour permettre à l'abonné d'adresser une notification conformément à l'article 8.

Article 7. Obligations incombant aux prestataires de services de gestion de l'identité en cas de violation des données[19]

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, le prestataire de services de gestion de l'identité 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 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[20, 21].

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

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

---

[19] *Obligations incombant aux prestataires de services de gestion de l'identité en cas de violation des données* : Le Groupe de travail souhaitera peut-être confirmer que l'article 7 établit une norme minimale à laquelle les règles de fonctionnement du système de gestion de l'identité ou tout autre arrangement contractuel ne peuvent déroger, compte tenu de l'opinion ayant prévalu en son sein selon laquelle l'article 14-2, établissait une telle norme minimale (A/CN.9/1045, par. 19). Il souhaitera peut-être aussi clarifier, à la lumière de la disposition de l'article 2-4 selon laquelle, « en dehors de ce qui y est disposé », l'instrument n'a pas d'incidence sur les lois relatives à la protection et à la confidentialité des données, la relation entre l'article 7 et ces lois (concernant l'avis selon lequel l'article 7 ne s'appliquerait effectivement que dans les États et entités ne disposant pas de telles lois, voir A/CN.9/1045, par. 97 et 98).

[20] *Références à la « loi applicable »* : Conformément aux autres lois types de la CNUDCI sur le commerce électronique, le présent projet fait référence à « la loi » plutôt qu'à « la loi applicable ».

[21] *Rôle des autres lois régissant le traitement des atteintes à la sécurité des données* : À la soixantième session du Groupe de travail, il a été indiqué que plusieurs des mesures énumérées à l'article 7 pourraient relever des lois sur la protection et la confidentialité des données, et que toutes les mesures visées, et pas seulement la notification, devraient être prises conformément à la loi applicable (A/CN.9/1045, par. 99). Le Groupe de travail souhaitera peut-être déterminer s'il convient de supprimer les mots « conformément à la loi », à l'alinéa c) du paragraphe 1 de l'article 7 et, conformément à l'approche décrite dans la note de bas de page 20, d'insérer les mots « , conformément à la loi » à la fin du chapeau du paragraphe 1 de l'article 7.

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

Article 8. Obligations incombant aux abonnés[22]

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

a) Il sait que ses justificatifs d'identité ont été [ou pourraient avoir été] compromis ; ou

[b) Il estime, au regard de circonstances connues de lui, qu'il y a un risque important que ses justificatifs d'identité aient été compromis.][23]

Article 9. Identification d'une personne au moyen de la gestion de l'identité[24]

1. Sous réserve de l'article 2, paragraphe 3, lorsqu'une règle de droit exige ou permet l'identification d'une personne [à une fin particulière], cette règle est satisfaite dans le cas des services de gestion de l'identité si une méthode fiable est employée pour l'identification électronique de cette personne [à cette fin][25].

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.

---

[22] *Obligations incombant aux abonnés* : L'article 8 a été modifié pour tenir compte des décisions prises par le Groupe de travail à sa soixantième session (A/CN.9/1045, par. 105). Par ailleurs, on a modifié le chapeau pour souligner que cette disposition traitait avant tout de la notification, plutôt que de moyens de notification particuliers. Par conséquent, on a reformulé le membre de phrase « utilise les moyens mis à disposition par le prestataire de services de gestion de l'identité conformément à l'article 6, ou utilise autrement des moyens raisonnables pour aviser celui-ci ».

[23] *Obligations incombant aux abonnés – connaissance de la compromission de justificatifs* : L'alinéa b) vise les cas dans lesquels l'abonné est présumé savoir que ses justificatifs ont été compromis.

[24] *Reconnaissance juridique de la gestion de l'identité – généralités* : L'article 9 a été modifié pour tenir compte des décisions prises par le Groupe de travail à sa soixantième session (A/CN.9/1045, par. 117). À cette session, il a été expliqué que l'article 9 visait à fournir une règle d'équivalence fonctionnelle pour l'identification dans les cas où la loi exigeait l'identification mais ne précisait pas de procédure d'identification, ou lorsque les parties étaient d'accord pour s'identifier. Il a également été expliqué que la règle d'équivalence fonctionnelle compléterait, conformément aux principes établis dans les textes de la CNUDCI, la règle relative à la reconnaissance juridique énoncée à l'article 5. Il a été ajouté que l'instrument n'avait pas d'incidence sur les exigences d'identification selon une procédure particulière, comme le prévoyait l'article 2-3. Enfin, il a été dit que la règle ne fonctionnait que lorsqu'il existait un équivalent hors ligne, puisque son but était d'établir des exigences d'équivalence entre l'identification hors ligne et en ligne (ibid., par. 106). S'il n'existe pas d'équivalent hors ligne, l'article 5 reste pertinent en garantissant que l'identification électronique n'est pas privée de la reconnaissance juridique au seul motif qu'elle est effectuée par des moyens électroniques (par exemple, par l'échange de messages de données).

[25] *Reconnaissance juridique de la gestion de l'identité – équivalent hors ligne* : L'inclusion des mots entre crochets relatifs à la finalité vise à répondre à une préoccupation soulevée à la soixantième session concernant la vérification d'attributs suffisants (A/CN.9/1045, par. 110 et 111). Il a été expliqué que, sans corrélation entre les attributs requis pour satisfaire à une exigence d'identification hors ligne et les attributs contenus dans les justificatifs d'identité utilisés pour l'identification électronique, l'article 9 ne permettrait pas d'établir de règle d'équivalence fonctionnelle. Il a été ajouté que le critère de fiabilité ne permettait pas de remédier à ce problème car il portait sur les processus de gestion des justificatifs d'identité plutôt que sur les attributs contenus dans ces justificatifs (ibid., par. 113). À la soixantième session, on s'est interrogé sur la nécessité d'inclure les mots entre crochets (ibid., par. 116). Le raisonnement qui sous-tendait ce point de vue était le suivant : si l'identification électronique implique de relier une personne à une « identité », et si l'« identité » est définie comme un ensemble d'attributs permettant à la personne « d'être identifiée de manière unique dans un contexte particulier », le contexte dans lequel s'applique l'exigence d'identification hors ligne, y compris sa finalité, détermine déjà les attributs requis pour l'identification électronique.

3. Le paragraphe 2 ne limite pas la capacité d'une personne :

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.

Article 10. Exigences pour déterminer la fiabilité des [services] [systèmes] de gestion de l'identité[26]

1. Pour déterminer la fiabilité de la méthode aux fins de l'article 9, toutes les circonstances pertinentes sont prises en considération, notamment[27] :

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 de fonctionnement, des politiques et des pratiques du prestataire de services de gestion de l'identité aux normes et procédures internationales reconnues qui sont pertinentes pour la fourniture de tels services, notamment [au cadre relatif aux niveaux de garantie] [aux niveaux de garantie ou aux cadres similaires fournissant des lignes directrices pour désigner le degré de confiance dans les méthodes et les processus utilisés par les systèmes de gestion de l'identité][28], en particulier aux règles relatives à :

i) La gouvernance ;

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

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

iv) La conservation des documents ;

v) Les installations et le personnel ;

vi) Les contrôles techniques ; et

vii) Le contrôle et l'audit ;

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

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

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

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 ; ou

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

---

[26] *Exigences pour déterminer la fiabilité – titre* : Le titre de l'article 10 a été modifié pour tenir compte des délibérations du Groupe de travail à sa soixantième session (A/CN.9/1045, par. 124).

[27] *Facteurs pertinents pour déterminer la fiabilité* : L'article 10 a été modifié pour tenir compte des décisions prises par le Groupe de travail à sa soixantième session (A/CN.9/1045, par. 118 et 120).

[28] *Niveaux de garantie* : Le membre de phrase « aux niveaux de garantie ou aux cadres similaires fournissant des lignes directrices pour désigner le degré de confiance dans les méthodes et les processus utilisés par les systèmes de gestion de l'identité » vise à englober les différentes formes sous lesquelles ces cadres peuvent être formulés. Le terme « niveau de garantie » est défini dans le document A/CN.9/WG.IV/WP.150. Le Groupe de travail voudra peut-être confirmer si ce membre de phrase convient pour décrire le concept de « cadre relatif aux niveaux de garantie ».

Article 11. Désignation des systèmes de gestion de l'identité fiables[29]

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 [services] 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 [service] de gestion de l'identité [30] ; et

b) De publier une liste des systèmes [services] de gestion de l'identité désignés, en mentionnant notamment les coordonnées du prestataire de services de gestion de l'identité[, ou d'informer le public par d'autres moyens][31].

3. Toute désignation arrêtée en vertu du paragraphe 1 doit être conforme aux normes et procédures internationales reconnues d'exécution du processus de désignation, notamment aux cadres relatifs aux niveaux de garantie.

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

a) Du lieu où le système [service] de gestion de l'identité est exploité ; ou

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

Article 12. Responsabilité des prestataires de services de gestion de l'identité[32]

Option A pour l'article 12[33]

La responsabilité du prestataire de services de gestion de l'identité est déterminée conformément à la loi.

---

[29] *Désignation des systèmes de gestion de l'identité fiables* : L'article 11 établit un mécanisme pour la détermination *ex ante* des systèmes de gestion de l'identité fiables. Il a été modifié pour tenir compte des décisions prises par le Groupe de travail à sa soixantième session (A/CN.9/1045, par. 125, 126 et 129).

[30] *« Systèmes » ou « services »* : Comme convenu par le Groupe de travail à sa soixantième session, on a inséré le mot « service » (au singulier) à côté du mot « système », car les fournisseurs de services de gestion de l'identité offrent des services, et non des systèmes, de gestion de l'identité à leurs abonnés. Toutefois, on a noté que la notion de système de gestion de l'identité englobait celle de service de gestion de l'identité et que la désignation devait renvoyer à cette notion plus large (A/CN.9/1045, par. 126). Le Groupe de travail souhaitera peut-être préciser s'il convient de faire référence aux « services de gestion de l'identité » (au pluriel), étant donné que c'est là le terme défini à l'article 1 f).

[31] *Notification des systèmes de gestion de l'identité désignés* : À sa soixantième session, le Groupe de travail a décidé de mettre entre crochets les mots « ou d'informer le public par d'autres moyens », en vue d'un examen ultérieur. Ils visent à englober des moyens d'information du public autres que la publication de listes. À la soixantième session, plusieurs délégations ont insisté sur le fait que, s'il était possible d'utiliser d'autres moyens, il était essentiel de conserver l'obligation de publier une liste des systèmes de gestion de l'identité désignés (A/CN.9/1045, par. 128). Si ces mots sont conservés, le Groupe de travail souhaitera peut-être envisager de les insérer à l'article 23-2 b).

[32] *Responsabilité des prestataires de services de gestion de l'identité* : L'article 12 a été modifié pour faire pendant aux options présentées à l'article 24 (A/CN.9/1045, par. 131).

[33] Voir note de bas de page 53.

Option B pour l'article 12[34]

1. Sans préjudice de la responsabilité qui lui incombe en cas de manquement à d'autres obligations prévues par la loi, le prestataire de services de gestion de l'identité est responsable du dommage causé intentionnellement ou par négligence à toute personne en raison d'un manquement aux obligations qui lui incombent en vertu [du présent instrument].

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

3. Nonobstant les dispositions du paragraphe 1, le prestataire de services de gestion de l'identité n'est pas responsable 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 limites 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 limites à l'abonné conformément à la loi.

Chapitre III. Services de confiance

Article 13. Reconnaissance juridique des services de confiance[35]

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

a) Il se présente sous forme électronique ; ou

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

Article 14. Obligations incombant aux prestataires de services de confiance

1. Le prestataire de services de confiance[36] :

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

b) Rend ces politiques et pratiques facilement accessibles aux abonnés et aux tiers; et

c) Fournit et met à la disposition du public les moyens que l'abonné devrait utiliser pour satisfaire à l'obligation de notifier toute atteinte à la sécurité conformément à l'article 15[37].

---

[34] Voir note de bas de page 54.

[35] *Reconnaissance juridique des services de confiance – généralités* : L'article 13 a été modifié pour tenir compte des décisions prises par le Groupe de travail à sa soixantième session (A/CN.9/1045, par. 16).

[36] *Obligations incombant aux prestataires de services de confiance – respect des politiques et pratiques* : L'article 14-1 a été modifié pour tenir compte des décisions prises par le Groupe de travail à sa soixantième session (A/CN.9/1045, par. 18 et 21).

[37] *Obligations incombant aux prestataires de services de confiance – obligation de mettre à disposition des moyens de notification* : Le Groupe de travail souhaitera peut-être déterminer si l'obligation visée à l'article 14-1 c) doit être de même nature que celle visée à l'article 6 d), et, dans l'affirmative, s'il convient d'aligner la formulation des deux obligations.

2. En cas d'atteinte à la sécurité ou de perte d'intégrité ayant une incidence importante[38] sur un service de confiance, le prestataire de ce service est tenu[39] :

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

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

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

Article 15. Obligations incombant aux abonnés[40]

L'abonné[41] informe le prestataire de services de confiance si :

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

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

Article 16. Signatures électroniques[42]

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 employée pour :

a) Identifier la personne ; et

b) Indiquer la volonté de cette personne concernant l'information contenue 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 23 est utilisée.

3. Le paragraphe 2 ne limite pas la capacité d'une personne :

a) D'établir par tout autre moyen, aux fins du paragraphe 1, la fiabilité d'une méthode au regard de l'article 22 ; ou

---

[38] À sa soixantième session, le Groupe de travail a été invité à fournir des orientations sur la signification de l'expression « incidence importante ». À cet égard, il voudra peut-être noter que l'article 19-2 du règlement eIDAS (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) exige des prestataires de services de confiance qu'ils notifient « toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ». Plusieurs facteurs peuvent contribuer à l'évaluation de cette incidence. Des formulaires dédiés de notification en application du règlement aident à évaluer l'incidence en précisant la durée de l'atteinte, le type de données et le pourcentage d'abonnés concernés, ainsi que d'autres informations pertinentes. Des lignes directrices techniques pour la notification d'incidents en application de l'article 19 du règlement eIDAS, ainsi qu'un rapport annuel sur ces incidents de sécurité, sont disponibles auprès de l'Agence de l'Union européenne pour la cybersécurité.

[39] Selon l'opinion qui avait prévalu au sein du Groupe de travail à sa soixantième session, l'article 14-2 établissait une norme minimale d'application obligatoire et il n'y avait donc pas de possibilité de dérogation contractuelle (A/CN.9/1045, par. 19). Voir également la note 19.

[40] *Obligations incombant aux abonnés – généralités* : Le Groupe de travail souhaitera peut-être envisager de modifier l'article 15 pour l'aligner sur l'article 8, en prenant note de la proposition énoncée dans la note de bas de page 37.

[41] *Obligations incombant aux abonnés – définition de l'« abonné »* : À sa cinquante-neuvième session, le Groupe de travail est convenu que l'instrument ne devrait pas imposer d'obligations aux parties utilisatrices (A/CN.9/1005, par. 38 à 40, 95 et 96). Comme indiqué dans la note de bas de page 7, il a été expliqué à la soixantième session que le signataire d'une signature électronique entrerait dans la définition du terme « abonné » (A/CN/9/1045, par. 22).

[42] *Signatures électroniques* : À sa soixantième session, le Groupe de travail est convenu de conserver le texte de l'article 16 tel qu'il figurait dans la version précédente en vue de l'examiner plus avant (A/CN.9/1045, par. 34).

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

Article 17. Cachets électroniques

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

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

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

2. Une méthode est présumée fiable aux fins du paragraphe 1 si un cachet électronique désigné conformément à l'article 23 est utilisé.

3. Le paragraphe 2 ne limite pas la capacité d'une personne :

a) D'établir par tout autre moyen, aux fins du paragraphe 1, la fiabilité d'une méthode au regard de l'article 22 ; ou

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

Article 18. Horodatages électroniques

1. Lorsqu'une règle de droit exige ou permet que certains documents, documents d'archives, 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 employée pour :

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

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

2. Une méthode est présumée fiable aux fins du paragraphe 1 si un horodatage électronique désigné conformément à l'article 23 est utilisé.

3. Le paragraphe 2 ne limite pas la capacité d'une personne :

a) D'établir par tout autre moyen, aux fins du paragraphe 1, la fiabilité d'une méthode au regard de l'article 22 ; ou

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

Article 19. Archivage électronique[43]

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

a) L'information contenue dans ce message est accessible pour être consultée ultérieurement ; et

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

[43] *Archivage électronique* : L'article 19 a été modifié pour tenir compte des décisions prises par le Groupe de travail à sa soixantième session (A/CN.9/1045, par. 39). Celui-ci était notamment convenu que le terme « message de données » englobait des données qui n'étaient ni transmises ni reçues (A/CN.9/1045, par. 41).

ii) Conserver le message de données dans le format sous lequel il a été créé, transmis ou reçu, ou dans un autre format dont il peut être démontré qu'il permet de détecter toute altération du message 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, du stockage et de l'affichage ;

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.

2. Une méthode est présumée fiable aux fins du paragraphe 1 b) si un [service] d'archivage électronique désigné conformément à l'article 23 est utilisé.

3. Le paragraphe 2 ne limite pas la capacité d'une personne :

a) D'établir par tout autre moyen, aux fins du paragraphe 1, la fiabilité d'une méthode au regard de l'article 22 ; ou

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

Article 20. [Services d']envoi recommandé électronique[44]

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

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

b) Indiquer la date et l'heure auxquelles le message de données a été envoyé;

c) Assurer l'intégrité du message de données ; et

d) Identifier l'expéditeur et le destinataire.

2. Une méthode est présumée fiable aux fins du paragraphe 1 si un [service] d'envoi recommandé électronique désigné conformément à l'article 23 est utilisé.

3. Le paragraphe 2 ne limite pas la capacité d'une personne :

a) D'établir par tout autre moyen, aux fins du paragraphe 1, la fiabilité d'une méthode au regard de l'article 22 ; ou

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

[44] *Envoi recommandé – fonctions* : L'article 20 a été modifié pour tenir compte de la décision prise par le Groupe de travail à sa soixantième session d'exiger expressément que le service d'envoi électronique assure l'intégrité du message de données et identifie l'expéditeur et le destinataire (A/CN.9/1045, par. 44).

Article 21. Authentification de site Internet[45]

1. Lorsqu'une règle de droit exige ou permet l'authentification d'un site Internet, cette règle est satisfaite si une méthode fiable est employée pour identifier la personne qui détient le nom de domaine[46] du site Internet et pour associer celle-ci audit site[47].

2. Une méthode est présumée fiable aux fins du paragraphe 1 si une authentification de site Internet désignée conformément à l'article 23 est utilisée.

3. Le paragraphe 2 ne limite pas la capacité d'une personne :

a) D'établir par tout autre moyen, aux fins du paragraphe 1, la fiabilité d'une méthode au regard de l'article 22 ; ou

b) D'apporter des preuves de la non-fiabilité d'une authentification de site Internet désignée.

Article 22. Exigences pour déterminer la fiabilité des services de confiance[48]

1. Pour déterminer la fiabilité de la méthode aux fins des articles 16 à 21, toutes les circonstances pertinentes sont prises en considération, notamment :

a) Toute règle, politique ou pratique de fonctionnement du prestataire de services de confiance, y compris tout plan visant à assurer la continuité en cas de cessation des activités ;

b) Toute norme ou procédure internationale reconnue qui est applicable et pertinente pour la fourniture de services de confiance ;

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 ;

---

[45] *Authentification de site Internet – généralités* : L'article 21 a été modifié pour tenir compte des décisions prises par le Groupe de travail à sa soixantième session (A/CN.9/1045, par. 48).

[46] *Authentification de site Internet – personne qui détient le nom de domaine* : L'expression « personne qui détient le 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 le cas où elle le fait afin de satisfaire à une règle de droit qui « exige » une telle authentification. Dans ces circonstances, la partie agirait donc en vertu d'une règle de droit qui « permet » cette authentification.

[47] *Authentification de site Internet – fonctions* : À sa cinquante-neuvième session, le Groupe de travail est convenu que la fonction essentielle de l'authentification d'un 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). À sa soixantième session, il a été indiqué que l'authentification de site Internet comprenait deux éléments : l'identification de la personne détenant le nom de domaine et l'association de cette personne au site en question. Par conséquent, l'objet du service de confiance était la fiabilité du site Internet et non l'identité du propriétaire. Il a été souligné que l'authentification de sites Internet visait à identifier des personnes, et non des objets (A/CN.9/1045, par. 47). À cette session, il a également été indiqué que toute discussion relative aux objets dans le cadre du projet d'instrument devrait se limiter à leur traçabilité jusqu'à une personne (ibid., par. 49). L'article 21 est la seule disposition qui traite d'objets.

[48] *Exigences pour déterminer la fiabilité* : L'article 22 (article 23 de la version précédente) a été modifié pour tenir compte des décisions prises par le Groupe de travail à sa soixantième session (A/CN.9/1045, par. 56, 57 et 61). Le niveau de fiabilité de la méthode utilisée peut varier selon la fonction recherchée avec ladite méthode.

h) La fonction pour laquelle le service de confiance est utilisé[49] ; et

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

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

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 23. Désignation de services de confiance fiables[50]

1. [*Toute personne, tout organe ou toute autorité, de droit public ou privé, indiqué[e] par l'État ou entité adoptant[e] comme compétent[e] en la matière*] peut désigner les services de confiance qui sont fiables aux fins des articles 16 à 21.

[1 *bis*. Une méthode est présumée fiable aux fins des articles 16 à 21 si un service de confiance désigné conformément au paragraphe 1 est utilisé.

1 *ter*. Le paragraphe 2 ne limite pas la capacité d'une personne :

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

b) D'apporter des preuves de la non-fiabilité d'un service de confiance désigné.][51]

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

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

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

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

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

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

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

---

[49] L'article 22-1 h) reflète la décision prise par le Groupe de travail à sa soixantième session (voir A/CN.9/1045, par. 56). Celui-ci souhaitera peut-être noter que ce facteur diffère de celui énoncé à l'article 10-1 d).

[50] *Désignation de services de confiance fiables – généralités* : L'article 23 (article 24 de la version précédente) a été modifié pour tenir compte des décisions prises par le Groupe de travail à sa soixantième session (A/CN.9/1045, par. 61). Il établit un mécanisme permettant la détermination *ex ante* de services de confiance fiables. Il a été expliqué lors des discussions tenues à sa cinquante-neuvième session que la désignation ne s'appliquait pas à des types génériques de services de confiance ni à l'ensemble des services de confiance offerts par un prestataire de services de confiance particulier, mais à un service de confiance particulier fourni par un prestataire de services donné (A/CN.9/1005, par. 69).

[51] *Désignation de services de confiance fiables – effets* : Le Groupe de travail voudra peut-être déterminer s'il convient d'insérer les paragraphes 1 *bis* et 1 *ter* à l'article 23 et, par conséquent, de supprimer les paragraphes 2 et 3 correspondants des articles 16, 17, 18, 19, 20 et 21. De même, il voudra peut-être se demander si les paragraphes 2 et 3 de l'article 9 devraient être déplacés à l'article 11.

Article 24. Responsabilité des prestataires de services de confiance[52]

Option A[53]

[La responsabilité du prestataire de services de confiance est déterminée conformément à la loi.]

Option B[54]

1. Sans préjudice de la responsabilité qui lui incombe en cas de manquement à d'autres obligations prévues par la loi, le prestataire de services de confiance est responsable du dommage causé intentionnellement ou par négligence à toute personne en raison d'un manquement aux obligations qui lui incombent en vertu [du présent instrument].

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

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

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

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

Chapitre IV. Aspects internationaux

Article 25. Reconnaissance internationale des [systèmes][services] de gestion de l'identité et des services de confiance

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

2. Pour déterminer si [des justificatifs d'identité] [un système de gestion de l'identité] [des services de gestion de l'identité] ou un service de confiance offrent

---

[52] *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. À sa soixantième session, il a examiné plusieurs options proposées par le Secrétariat. L'article 24 a été modifié pour tenir compte des décisions prises à cette session (A/CN.9/1045, par. 66).

[53] L'option A adopte une approche minimaliste en reconnaissant que la responsabilité du prestataire de services de confiance, y compris toute limitation de celle-ci, doit être déterminée conformément à la loi applicable en dehors de l'instrument. Le Groupe de travail voudra peut-être se demander s'il convient de conserver cette disposition 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 découlerait des principes généraux de droit.

[54] L'option B adopte une approche similaire à celle utilisée à l'article 13 du règlement eIDAS. Le paragraphe 1 énonce un principe général de responsabilité en cas de manquement, intentionnel ou par négligence, à l'une quelconque des obligations découlant de l'instrument. La norme de négligence envisagée est ordinaire, c'est-à-dire ni légère ni grave. La négligence légère et la négligence grave sont des notions juridiques dont le contenu peut différer selon le système juridique et qui n'existent peut-être pas dans tous les systèmes juridiques. Le paragraphe 2 fait référence au droit interne pour des questions connexes telles que les éléments constitutifs de la négligence, la charge de la preuve et d'autres questions relatives à la preuve, et des questions telles que la faute contributive et la responsabilité pour fait d'autrui. Le paragraphe 3 établit les conditions de limitation de la responsabilité.

[un niveau de fiabilité substantiellement équivalent] [le même niveau de fiabilité], il est tenu compte [des normes internationalement reconnues][55].

[3. L'équivalence est présumée si une personne, un organe ou une autorité indiqué[e] par [*l'État ou entité adoptant[e]*] conformément aux articles 11 et 23 a déterminé l'équivalence aux fins du présent paragraphe.][56]

Article 26. Coopération

[*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 de systèmes de gestion de l'identité et de services de confiance étrangers, qu'elle soit accordée unilatéralement ou d'un commun accord ;

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

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

---

[55] *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 (A/CN.9/1005, par. 120). Le présent projet fait pendant à l'article 12-2 de la LTSE, qui exige une équivalence « substantielle ». Une autre option proposée dans la version précédente prévoyait une équivalence exacte (c'est-à-dire que le service étranger devait offrir « le même niveau de fiabilité »). Ces délibérations ont été poursuivies à la soixantième session (A/CN.9/1045, par. 69).

[56] *Reconnaissance internationale – présomption d'équivalence* : Le paragraphe 3 vise à relier l'article 25 aux articles 11 et 23 (voir A/CN.9/1045, par. 71), notamment en ce qui concerne la désignation *ex ante*. Le Groupe de travail souhaitera peut-être examiner les cas dans lesquels une autorité de désignation se prévaudrait du paragraphe 3 plutôt que de désigner le système de gestion de l'identité ou le service de confiance étranger, compte tenu notamment des articles 11-4 et 23-4. En outre, il voudra peut-être déterminer si une nouvelle disposition devrait être ajoutée à l'article 25 afin d'habiliter l'autorité de désignation à décider qu'un système de gestion de l'identité ou un service de confiance désigné par une autorité étrangère sera traité dans l'État adoptant comme un système de gestion de l'identité ou un service de confiance désigné en vertu des articles 11-1 et 23-1 respectivement.