Nations Unies A/CN.9/WG.IV/WP.154

Assemblée générale

Distr. limitée
12 septembre 2018
Français
Original : anglais

Commission des Nations Unies pour le droit commercial international
Groupe de travail IV (commerce électronique)
Cinquante-septième session
Vienne, 19-23 novembre 2018

Questions juridiques liées à la gestion de l'identité et aux services de confiance

Note du Secrétariat

Table des matières

V.18-05927 (F)

I. Introduction

1. La présente note donne un aperçu de quelques aspects de certains des thèmes recensés par le Groupe de travail dans le cadre de l'examen des questions juridiques liées à la gestion de l'identité et aux services de confiance (A/CN.9/936, par. 58), afin de faciliter la poursuite des débats. En particulier, elle vise à mettre en lumière les questions clefs et à proposer des solutions possibles, sans pour autant limiter la possibilité d'examiner d'autres sujets ou d'aborder certains sujets conjointement, le cas échéant. Le document de travail A/CN.9/WG.IV/WP.153 illustre certains aspects d'autres sujets recensés par le Groupe de travail dans le cadre de l'examen des questions juridiques liées à la gestion de l'identité et aux services de confiance.

2. Les paragraphes 6 à 17 du document de travail A/CN.9/WG.IV/WP.152 fournissent des informations relatives aux travaux du Groupe de travail sur les questions juridiques liées à la gestion de l'identité et aux services de confiance. On trouvera une liste d'autres documents pertinents au paragraphe 18 du document de travail A/CN.9/WG.IV/WP.152.

II. Questions pertinentes pour des travaux futurs sur les aspects juridiques de la gestion de l'identité et des services de confiance

A. Certification des prestataires de dispositifs de gestion de l'identité et de services de confiance

3. La certification, y compris l'autocertification, l'accréditation et les audits indépendants peuvent grandement contribuer à instaurer la confiance des utilisateurs envers les prestataires de dispositifs de gestion de l'identité et de services de confiance. Le type de service en jeu, le coût et le niveau de garantie requis peuvent influer sur le choix de la forme de certification la plus appropriée.

4. Le Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (règlement eIDAS) prévoit un système global de contrôle et de certification des services de confiance. Conformément à l'article 17 du règlement, les États membres désignent un organe chargé d'activités de contrôle régulières à l'égard des prestataires de services de confiance qualifiés et d'activités de contrôle ponctuelles à l'égard d'autres prestataires de services de confiance. L'article 17-4 fournit une liste des tâches spécifiques dont l'organe de contrôle doit s'acquitter.

5. Il convient de noter que, dans le cadre du règlement eIDAS, l'existence d'un organe de contrôle est nécessaire pour qu'un prestataire de services de confiance puisse être considéré comme qualifié. En particulier, selon l'article 20, les prestataires de services de confiance qualifiés font l'objet, au moins tous les 24 mois, d'un audit effectué par un organisme d'évaluation de la conformité. Le rapport d'évaluation de la conformité est transmis à l'organe de contrôle. Le non-respect des demandes de l'organe de contrôle peut entraîner le retrait du statut qualifié au prestataire de services de confiance ou à l'un quelconque de ses services.

6. Par ailleurs, en vertu du règlement eIDAS, seuls les prestataires de services de confiance qualifiés peuvent offrir des services de confiance qualifiés qui sont associés à certains effets juridiques (comme les présomptions). Par exemple, conformément à l'article 25-2, l'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite. En résumé, l'existence d'un organe de contrôle permet d'offrir des services de confiance qualifiés associés à des effets juridiques.

7. En ce qui concerne les services de confiance, les alinéas e) et f) de l'article 10 de la Loi type de la CNUDCI sur les signatures électroniques font référence à

l'existence de l'accréditation, des audits et de l'autocertification en tant que facteur pouvant s'avérer pertinent pour évaluer la fiabilité des systèmes utilisés par le prestataire de services de certification. Par conséquent, selon cette approche, l'existence d'un organe de contrôle et de systèmes d'accréditation est facultative et l'appréciation de leur existence est discrétionnaire.

8. Dans les modèles de reconnaissance juridique mutuelle qui utilisent des listes de confiance (voir A/CN.9/WG.IV/WP.153, par. 61 à 73 et 76 à 79), la certification (y compris l'autocertification) est un élément nécessaire pour évaluer les dispositifs de gestion de l'identité en fonction des résultats. Il peut être nécessaire de prédéfinir un ensemble de profils à utiliser pour l'évaluation.

9. Le Groupe de travail voudra peut-être se demander si l'existence de la certification, y compris l'autocertification, de l'accréditation et des audits indépendants devrait être associée à certains effets juridiques et, dans l'affirmative, lesquels, ou si ces éléments devraient plutôt être recensés comme potentiellement pertinents pour évaluer la fiabilité, la confiance ou d'autres qualités des prestataires de services de confiance et de gestion d'identité. Lors de ses délibérations, il voudra peut-être aussi indiquer si le recours à la certification, y compris l'autocertification, à l'accréditation et à des audits indépendants, devrait être obligatoire ou facultatif.

B. Niveaux de garantie

1. Gestion de l'identité

10. Le niveau de garantie est une mesure de la fiabilité d'une revendication d'identité qui se fonde sur les processus utilisés. Différentes entités publiques et privées proposent des définitions différentes des niveaux de garantie, qui sont régulièrement mises à jour en fonction de l'évolution des technologies et des processus opérationnels. Compte tenu de l'adoption du principe de neutralité technologique, seuls les niveaux de garantie formulés de manière technologiquement neutre sont pris en considération.

11. L'organisme nord-américain National Institute of Standards and Technology a identifié trois niveaux de garantie liée à l'identité, à savoir : un niveau de garantie de l'identité (pour « identity assurance level »), un niveau de garantie de l'authentifiant (pour « authenticator assurance level ») et un niveau de garantie de la fédération (pour « federation assurance level »)[1]. Le niveau de garantie de l'identité renvoie au processus de vérification de l'identité, le niveau de garantie de l'authentifiant renvoie au processus d'authentification et le niveau de garantie de la fédération renvoie au protocole de revendication mis en œuvre dans un environnement fédéré pour communiquer des informations concernant l'authentification et les attributs (le cas échéant) à une partie se fiant à la signature ou au certificat, appelée aussi « partie utilisatrice » (pour « relying party »).

12. Plus précisément, le niveau de garantie de l'identité renvoie à la robustesse du processus de vérification de l'identité permettant de déterminer avec confiance l'identité d'une personne ; le niveau de garantie de l'authentifiant renvoie à la robustesse du processus d'authentification lui-même et au lien entre un authentifiant et l'identifiant spécifique d'un individu ; et le niveau de garantie de la fédération renvoie à la robustesse du protocole d'assertion mis en œuvre par la fédération pour communiquer des informations concernant l'authentification et les attributs à une partie utilisatrice lorsqu'une architecture fédérée de l'identité est utilisée[2].

13. Chaque niveau de garantie de l'identité a son propre degré de robustesse associé à certaines exigences. Par exemple, au niveau de garantie de l'identité 1, les attributs,

---

[1] Publication spéciale 800-63-3 du National Institute of Standards and Technology, *Digital Identity Guidelines*, juin 2017, chap. 2. Disponible à l'adresse https://doi.org/10.6028/NIST.SP.800-63-3.

[2] National Institute of Standards and Technology, *Digital Identity Guidelines*, cit., chap. 5-2.

s'il y en a, sont autorevendiqués ou devraient être traités comme tels. Au niveau de garantie de l'identité 2, une vérification d'identité à distance ou en personne est requise. Le niveau de garantie de l'identité 2 exige que les attributs d'identification aient été vérifiés en personne ou à distance en utilisant, au minimum, des procédures spécifiques. Au niveau de garantie de l'identité 3, une vérification de l'identité en personne est requise et les attributs d'identification doivent être vérifiés par le représentant autorisé d'un fournisseur de services de certification qui examinera des documents physiques conformément à des procédures précises.

14. L'article 8 du règlement eIDAS établit trois niveaux de garantie des schémas d'identification électronique, à savoir faible, substantiel et élevé, ainsi que les critères correspondants. En particulier, le niveau de garantie faible accorde un degré limité de fiabilité à l'identité revendiquée ou prétendue d'une personne ; le niveau de garantie substantiel accorde un degré substantiel de fiabilité à l'identité revendiquée ou prétendue d'une personne ; et le niveau de garantie élevé accorde un niveau de fiabilité à l'identité revendiquée ou prétendue d'une personne plus élevé que le niveau de garantie substantiel.

15. Un règlement d'exécution du règlement eIDAS [3] établit des spécifications techniques et procédures minimales à mettre en œuvre pour déterminer la fiabilité et la qualité des quatre aspects suivants : inscription, gestion des moyens d'identification électronique, authentification, et gestion et organisation des prestataires de schémas d'identification électronique dans un contexte transfrontalier. Ces spécifications techniques et procédures sont décrites d'une manière technologiquement neutre.

16. Compte tenu de ce qui précède, le Groupe de travail voudra peut-être examiner la question de savoir si la notion de niveau de garantie devrait être utilisée pour satisfaire aux exigences juridiques ou pour déterminer les effets juridiques. Dans l'affirmative, il souhaitera peut-être aussi examiner, en particulier, la relation entre, d'une part, les niveaux de garantie et, d'autre part, les exigences et mécanismes en matière de reconnaissance juridique. Il voudra peut-être également se demander s'il devrait examiner les caractéristiques des niveaux de garantie et, le cas échéant, dans quelle mesure.

2. Services de confiance

17. Il est essentiel de se demander si la notion de niveau de garantie devrait s'appliquer également aux services de confiance. Un certain nombre de lois nationales portant sur les signatures électroniques reconnaissent en effet deux niveaux de ces signatures. Le premier englobe toutes les formes de signatures électroniques. Le second associe certaines conséquences juridiques, telles que la présomption d'origine et d'intégrité, aux signatures électroniques qui satisfont à certaines exigences. On peut dès lors considérer que cette approche introduit différents niveaux de garantie en ce qui concerne les signatures électroniques.

18. S'agissant des services de confiance, l'article 24-1 du règlement eIDAS fournit une illustration de l'utilisation de niveaux de garantie dans le cadre de la satisfaction d'une exigence en matière d'identification en vue de la délivrance d'un certificat qualifié. Plus précisément, pour satisfaire à l'exigence selon laquelle un prestataire de services de confiance qualifié doit vérifier l'identité de la personne à laquelle il délivre un certificat qualifié, le règlement eIDAS autorise la réalisation de cette vérification à distance à l'aide d'un moyen d'identification électronique doté d'un niveau de garantie « substantiel » ou « élevé ».

---

[3] Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique.

19. Le Groupe de travail voudra peut-être se demander si la notion de niveaux de garantie devrait s'appliquer aux services de confiance et, dans l'affirmative, de quelle manière.

C. Responsabilité

20. Le régime de responsabilité applicable peut avoir une incidence importante sur la promotion de l'utilisation de systèmes de gestion de l'identité et de services de confiance à des fins à la fois commerciales et non commerciales. À cet égard, il convient de noter que, s'il existe généralement des voies de recours en cas d'identification fautive dans les transactions commerciales, il se peut qu'aucune responsabilité ne soit liée à l'attribution fautive de l'identité de base dans les documents papier si le droit national n'attribue pas la responsabilité de ce service aux entités publiques.

21. Le Groupe de travail a déjà recensé certaines questions pertinentes pour ses débats sur la responsabilité des parties intervenant dans des systèmes de gestion de l'identité ou dans des services de confiance, à savoir : les entités qui devraient être tenues responsables (émetteurs, prestataires ou autres parties), en tenant compte des régimes spéciaux de responsabilité applicables aux entités publiques ; la possibilité de limiter la responsabilité des parties qui respecteraient les exigences préétablies ; les mécanismes statutaires de limitation de la responsabilité tels que la dispense ou l'inversion de la charge de la preuve ; et les limitations contractuelles de la responsabilité (A/CN.9/936, par. 85).

22. Dans certains cas, il peut être difficile d'établir quelle entité est responsable, par exemple en ce qui concerne les données d'attributs de confiance fournies par un service de confiance dans le cadre de l'utilisation de la technologie du registre distribué pour l'horodatage (A/CN.9/936, par. 86). Dans d'autres cas, un mécanisme fondé sur l'assurance peut être utilisé pour les transactions commerciales, en vertu duquel l'utilisation abusive du système d'identification électronique ou du service de confiance peut entraîner une indemnisation par l'assureur. Un autre mécanisme prévoit le déblocage automatisé d'indemnités préétablies ou des pénalités déterminées si certaines conditions sont remplies.

1. Gestion de l'identité

23. L'article 9 du règlement eIDAS impose de soumettre, au moment de la notification d'un schéma d'identification électronique, des informations sur le régime de responsabilité applicable à l'émetteur des moyens d'identification électronique et à la partie gérant la procédure d'authentification.

24. Conformément à l'article 11 du règlement eIDAS, l'État membre notifiant est responsable du dommage causé en raison d'un manquement aux obligations qui lui incombent de veiller à ce que les données d'identification personnelle représentant de manière univoque la personne en question soient attribuées à la bonne personne, et de garantir la disponibilité en ligne des informations d'authentification utilisées pour confirmer les données d'identification de la personne. L'article 11 attribue également à la partie qui émet des moyens d'identification électronique la responsabilité du dommage résultant de l'incapacité à attribuer un moyen d'identification électronique à la personne représentée de manière univoque par ses données d'identification. Enfin, il attribue au gestionnaire de la procédure d'authentification la responsabilité du dommage résultant de l'incapacité à assurer le bon fonctionnement du schéma d'authentification en ligne utilisé pour confirmer les données d'identification de la personne.

25. L'article 11 du règlement eIDAS ne s'applique qu'aux transactions transfrontalières et exige que le dommage soit causé intentionnellement ou par négligence. Il s'applique conformément aux dispositions nationales en ce qui concerne des questions telles que la définition du dommage et la répartition de la

charge de la preuve, et sans préjudice de la responsabilité supplémentaire découlant du droit national des parties impliquées dans les transactions où les systèmes de gestion de l'identité sont utilisés.

26. En résumé, conformément au règlement eIDAS, les parties intervenant dans le cadre d'un système d'identification électronique sont responsables du dommage causé par tout manquement aux obligations définies qui leur incombent, si ce dommage est causé intentionnellement ou par négligence, pour autant que la transaction soit transfrontalière, et sans préjudice d'une responsabilité supplémentaire découlant du droit national.

27. L'article 281 de la loi 2017-20 du Bénin indique que les gestionnaires de systèmes d'identification électronique sont responsables des dommages causés intentionnellement ou par leur négligence à tout utilisateur de ces systèmes.

28. En vertu de l'article 1-552 de la *Virginia Electronic Identity Management Act* (loi de l'État de Virginie sur la gestion de l'identité électronique), les opérateurs de cadres de confiance en matière d'identité et les fournisseurs de dispositifs d'identité ne sont pas responsables si le justificatif d'identité est fourni ou si l'attribut d'identité ou la marque de confiance sont attribués conformément aux normes en matière de gestion d'identité approuvées par le Secrétaire à la technologie du Commonwealth de Virginia, à tout accord contractuel, et à tous règlements et politiques écrits du cadre de confiance en matière d'identité dont le fournisseur est membre. Selon l'article 1-550, une marque de confiance est « un cachet officiel, un élément d'authentification, une certification, une licence ou un logo lisible par machine qui peut être fourni par un opérateur de cadre de confiance en matière d'identité à un fournisseur de dispositifs d'identité certifié dans son cadre de confiance en matière d'identité pour indiquer que ce fournisseur respecte les règles et politiques écrites du cadre concerné ».

29. En résumé, la *Virginia Electronic Identity Management Act* exonère de toute responsabilité les opérateurs de cadres de l'identité et les fournisseurs de dispositifs d'identité qui respectent les normes établies par un organisme public, les représentations conventionnelles et les règlements en matière de fédération. Le respect des spécifications et des normes minimales établies par le Commonwealth de Virginie est contrôlé par le recours à des autorités de certification tierces indépendantes qui réalisent des examens de conformité objectifs, cohérents et vérifiables, fondés sur des critères de certification clairement définis[4]. L'exonération ne s'applique pas si l'opérateur du cadre de l'identité ou le fournisseur de dispositifs d'identité a fait preuve de négligence grave dans le cadre d'un acte ou d'une omission ou s'il s'est rendu coupable d'inconduite volontaire.

30. L'article 1-555 de la *Virginia Electronic Identity Management Act* prévoit qu'aucune de ses dispositions ou aucun acte ou omission connexe de la part d'une entité publique lié à la gestion de l'identité ne saurait être interprété comme une levée de l'immunité souveraine de cette entité publique.

31. Le Groupe de travail souhaitera peut-être examiner quelles entités devraient être tenues responsables, en vertu de quel régime de responsabilité et si un régime spécial de responsabilité devrait être mis en place pour les entités publiques.

32. Lors de l'examen du régime de responsabilité, le Groupe de travail souhaitera peut-être se pencher sur les points suivants : a) la possibilité de limiter la responsabilité des parties qui remplissent des exigences prédéterminées, par exemple par l'exonération ou le renversement de la charge de la preuve ; b) la question de savoir si différents niveaux de garantie devraient être associés à différents régimes de responsabilité ; c) la possibilité de limiter la responsabilité par contrat ; et

[4] Commonwealth of Virginia Identity Management Standards Advisory Council, *Guidance Document 5: Certification of Identity Trust Framework Operators* (projet), art. 7 : Certification des opérateurs de cadres de confiance en matière d'identité.

d) l'éventuelle mise en place de l'obligation de fournir des métadonnées décrivant le régime de responsabilité, notamment toute limitation qui existerait.

2. Services de confiance

33. Conformément à l'article 13 du règlement eIDAS, les prestataires de services de confiance sont responsables des dommages causés intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations prévues par le règlement. Autrement dit, la responsabilité des prestataires qui se conforment aux obligations prévues par le Règlement n'est pas engagée.

34. En outre, l'article 13 introduit une présomption réfragable d'intention ou de négligence de la part d'un prestataire de services de confiance qualifié, alors que la charge de prouver l'intention ou la négligence d'un prestataire non qualifié incombe à la personne qui invoque les dommages. Cette disposition vise à renforcer la confiance des utilisateurs à l'égard des prestataires qualifiés puisque, en cas de dommage, la demande de réparation est facilitée par la présomption. Enfin, l'article 13 prévoit la possibilité que les prestataires de services de confiance limitent leur responsabilité, à condition que les clients soient dûment informés au préalable de ces limitations et que celles-ci puissent être reconnues par des tiers.

35. La Loi type de la CNUDCI sur les signatures électroniques comporte des dispositions traitant de la responsabilité liée au comportement du signataire (art. 8), du prestataire de services de certification (art. 9) et de la partie se fiant à la signature ou au certificat (art. 11). Ces dispositions précisent les obligations de chaque entité intervenant dans le cycle de vie de la signature électronique. La loi prévoit la possibilité que les prestataires de services de certification limitent la portée ou l'étendue de leur responsabilité.

D. Mécanismes de coopération institutionnelle

36. Certains mécanismes de coopération institutionnelle, privé ou public, pourraient contribuer à atteindre la reconnaissance juridique mutuelle et l'interopérabilité des systèmes de gestion de l'identité et des services de confiance.

37. L'article 12 du règlement eIDAS fournit un exemple de mécanisme de coopération institutionnelle en indiquant que les États membres devraient coopérer en ce qui concerne l'interopérabilité et la sécurité des schémas d'identification électronique. La coopération peut consister en des échanges d'informations, d'expériences et de bonnes pratiques, notamment en ce qui concerne les exigences techniques et les niveaux de garantie, l'évaluation par les pairs des schémas d'identification électronique et l'examen des évolutions pertinentes.

38. Un des actes d'exécution du règlement eIDAS [5] fournit des détails supplémentaires sur l'échange d'informations et l'évaluation par les pairs, notamment en indiquant que l'État membre fournit les informations demandées sauf si leur divulgation risque de porter atteinte à la sécurité publique ou nationale, ou à des secrets commerciaux, professionnels ou industriels. Il établit également un réseau de coopération pour faciliter la conduite des activités de coopération. Il convient de noter que, si l'examen par les pairs d'un schéma d'identification électronique susceptible d'être notifié est volontaire, dans la pratique, les résultats peuvent largement contribuer à voir si le dispositif répond aux normes établies et l'évaluation constitue donc une étape importante du mécanisme de notification qui est au cœur de la structure institutionnelle du règlement eIDAS.

39. On peut envisager un autre type de coopération entre systèmes de gestion de l'identité par le biais de la fédération de tels systèmes. Selon ce modèle, les informations relatives à l'identité vérifiées au sein d'un système de gestion de

[5] Décision d'exécution (UE) 2015/296 de la Commission du 24 février 2015 établissant les modalités de coopération entre les États membres en matière d'identification électronique.

l'identité sont mises à la disposition d'un certain nombre de parties (qui en ont besoin pour diverses raisons) au sein d'un système différent, de manière convenue et contrôlée (voir aussi A/CN.9/WG.IV/WP.153, par. 47). Les systèmes fédérés assurent l'interopérabilité entre leurs participants en utilisant un cadre technique et juridique commun défini par un ensemble de règles systémiques. La fédération peut donc contribuer à l'augmentation du nombre d'utilisateurs et d'applications, et aider à modérer les coûts liés à la gestion de l'identité. Bien que le socle des systèmes fédérés soit généralement contractuel, des dispositions législatives peuvent contribuer à promouvoir ce mécanisme (voir, par exemple, l'utilisation de marques de confiance dans la *Virginia Electronic Identity Management Act* au paragraphe 28 ci-dessus).

E. Transparence

40. Le Groupe de travail a établi la pertinence du principe de transparence en vue de débats futurs sur la gestion de l'identité et les services de confiance (A/CN.9/936, par. 8). Ce faisant, il a mis en relief les deux tâches suivantes liées à ce principe : l'obligation de faire connaître les systèmes de gestion d'identité et les services de confiance qui sont proposés et de donner des informations concernant leur qualité, et l'obligation de notification des atteintes à la sécurité.

41. En ce qui concerne les services offerts et leur qualité, il convient de noter que les prestataires de dispositifs de gestion d'identité et de services de confiance participant à des systèmes fédérés ou obtenant d'une autre manière la certification de leurs services doivent fournir une quantité importante d'informations. Des obligations minimales de divulgation peuvent être établies pour d'autres fournisseurs. Par exemple, l'article 9-1 de la Loi type de la CNUDCI sur les signatures électroniques contient une liste d'informations que le prestataire de services de certification doit fournir à la partie utilisatrice.

42. S'agissant de l'obligation de notifier les atteintes à la sécurité, il a été noté qu'il y avait des éléments communs, mais également de grandes différences, entre les notifications d'atteinte à la sécurité et celles de violation des données. Il a été ajouté qu'il existait des exemples utiles de mécanismes allant au-delà de la simple notification en cas d'atteinte à la sécurité (A/CN.9/936, par. 89). Des considérations supplémentaires pouvaient avoir trait à l'utilisation éventuelle du renseignement sur les cybermenaces pour atténuer les risques.

43. L'article 10 du règlement eIDAS impose aux États membres l'obligation de faire connaître les atteintes ou les altérations qui affectent la fiabilité de l'authentification transfrontalière du schéma d'identification électronique. Tout État membre concerné doit également suspendre ou révoquer immédiatement l'authentification ou les éléments altérés.

44. L'article 19-2 du règlement eIDAS prévoit une obligation similaire pour les prestataires de services de confiance, qui doivent notifier à l'organe de contrôle et, le cas échéant, à d'autres organismes concernés, tels que l'autorité chargée de la protection des données, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées. La notification doit être faite dans les meilleurs délais et, en tout état de cause, dans les 24 heures suivant la prise de connaissance de l'infraction ou de la perte.

45. L'article 8-1 b) de la Loi type de la CNUDCI sur les signatures électroniques prévoit un mécanisme de notification facultatif que le signataire peut utiliser si les données de création de signature ont été compromises ou s'il existe un risque important qu'elles aient pu l'être.

46. Une éventuelle disposition sur l'obligation de notifier les atteintes à la sécurité pourrait se lire comme suit :

> Les prestataires de services de confiance et les fournisseurs de dispositifs d'identité doivent, dans les meilleurs délais [et en tout état de cause dans les ... jours après en avoir eu connaissance], notifier [à l'autorité de contrôle] [à leurs clients affectés et aux parties utilisatrices] toute atteinte à la sécurité ou perte d'intégrité ayant une incidence [importante] sur les services, justificatifs d'identité ou processus d'authentification fournis ou sur les données à caractère personnel qui y sont conservées.
>
> En cas d'atteinte à la sécurité ou perte d'intégrité importante, les prestataires de services de confiance et les fournisseurs de dispositifs d'identité suspendent la fourniture des services concernés [jusqu'à...].
>
> Les utilisateurs de services de confiance et de dispositifs d'identité informent le prestataire de services si les justificatifs d'identité, les processus d'authentification ou les données de création de services de confiance ont été compromis, ou si certaines circonstances connues de l'utilisateur font naître un risque important que les justificatifs d'identité, les processus d'authentification ou les données de création de services de confiance puissent avoir été compromis.

47. Le projet de disposition comporte des éléments facultatifs (entre crochets), qui visent à prévoir un délai dans lequel la notification doit être effectuée, à identifier les parties à notifier et à établir le niveau d'incidence sur les services, les justificatifs d'identité ou les données à caractère personnel qui déclenche l'obligation de notification. Il est également possible d'établir l'obligation de suspendre le dispositif de gestion de l'identité et les services de confiance soit jusqu'à ce que l'atteinte ou la perte soit contenue soit jusqu'à ce qu'un nouveau processus de certification (ou un processus similaire) soit mis en place.

F. Conservation des données

48. Le Groupe de travail a déjà souligné l'importance de l'harmonisation et de l'interopérabilité des régimes de conservation des données pour le commerce international (A/CN.9/936, par. 91). Ce faisant, il a mis en évidence au moins deux aspects potentiellement intéressants. Le premier concerne la protection des données, et le second est lié à leur stockage et à leur archivage.

49. La protection des données est un sujet à même de soulever des questions particulièrement complexes. Le Groupe de travail voudra peut-être confirmer que, conformément au principe général selon lequel les textes de la CNUDCI sur le commerce électronique n'affectent pas les dispositions de fond (voir A/CN.9/WG.IV/WP.153, par. 48), les lois sur la protection des données et les sujets connexes, notamment la protection de la vie privée, devraient rester pleinement applicables. Il voudra peut-être aussi se demander si des précisions ou des éclaircissements supplémentaires seraient utiles.

50. Il est possible de stocker et d'archiver des documents en mettant en œuvre des moyens électroniques, comme l'indique déjà l'article 10 de la Loi type de la CNUDCI sur le commerce électronique, qui établit les conditions de l'équivalence fonctionnelle entre les messages de données et les documents papier en matière de conservation. Les obligations de conservation des documents proviennent du droit matériel et sont liées au temps nécessaire à la prescription des différentes actions.

51. La prestation de services de stockage et d'archivage des données peut faire l'objet d'un service de confiance spécialisé (voir ci-dessous, par. 64 et 65). Dans le cadre de l'interopérabilité des services de confiance, le Groupe de travail souhaitera peut-être examiner les questions relatives à la portabilité des archives électroniques.

G. Encadrement des prestataires de services

52. Si le Groupe de travail estime qu'il convient d'aborder les dispositifs de gestion de l'identité et les systèmes de services de confiance plutôt que les opérations connexes (voir A/CN.9/WG.IV/WP.153, par. 57 à 59), la création d'un organe de contrôle pourra être utile, voire s'imposer, pour instaurer la confiance à l'égard des prestataires de services et des services fournis. Toutefois, la mise en place d'un tel organe a des répercussions administratives et financières. Certains mécanismes de substitution ou complémentaires (comme la certification par des tiers) peuvent aider à atteindre les objectifs visés par le contrôle des prestataires de services, tout en réduisant les coûts associés.

53. Conformément à la législation des états du Vermont et de la Virginie, le contrôle des prestataires de dispositifs de gestion de l'identité relève d'organismes publics. De même, selon l'article 97 de la loi 2017-07 du Togo, le contrôle des prestataires de services de confiance relève de l'autorité nationale chargée de la certification. Conformément à l'article 283 de la loi 2017-20 du Bénin, les entités délivrant les moyens d'identification électronique sont désignées par une autorité publique. L'existence d'un mécanisme de contrôle de la gestion et de la fourniture de services liés à l'identité est également implicite dans le système de notification établi par le règlement eIDAS.

54. En ce qui concerne les prestataires de services de confiance, diverses lois confèrent à un organe de contrôle le pouvoir d'accorder un statut qualifié ou lui donnent un droit de regard sur la manière dont ce statut est accordé par des tiers. Le règlement eIDAS exige quant à lui la désignation par les États membres d'un organe national de contrôle compétent à l'égard des prestataires de services de confiance.

55. Adoptant le principe de neutralité, la Loi type de la CNUDCI sur les signatures électroniques contient une référence facultative à l'existence d'organes de contrôle, puisque l'incorporation de dispositions impératives sur l'existence d'organes de contrôle peut se comprendre comme empêchant l'adoption d'un modèle de marché fondé sur l'autoréglementation des services de confiance.

H. Questions propres aux services de confiance

56. Les travaux sur les questions juridiques relatives aux services de confiance sont étroitement liés à ceux portant sur la gestion de l'identité. En conséquence, les commentaires relatifs aux services de confiance dans le contexte du principe de l'équivalence fonctionnelle (A/CN.9/WG.IV/WP.153, par. 36 et 37), de la reconnaissance juridique (A/CN.9/WG.IV/WP.153, par. 93 à 98), des niveaux de garantie (par. 17 à 19 ci-dessus) et de la responsabilité (par. 33 à 35 ci-dessus) ont été faits en relation avec l'examen des mêmes questions en ce qui concerne la gestion de l'identité.

57. Toutefois, le traitement juridique des services de confiance peut également poser des défis particuliers. Fondamentalement, les services de confiance diffèrent tous les uns des autres et, par conséquent, chacun soulève un ensemble différent de questions à examiner. Se pose par ailleurs la question de savoir si le traitement juridique des services de confiance doit prendre en compte une liste non exhaustive de tels services fondée sur une définition commune, ou plutôt fournir des règles communes applicables à tous les services de confiance et des règles spécifiques applicables à chacun d'entre eux.

58. En outre, on pourrait éventuellement renvoyer aux dispositions en matière d'équivalence fonctionnelle pour décrire les tâches liées à l'utilisation de chaque service de confiance, d'une manière analogue aux dispositions de la CNUDCI sur les signatures électroniques et la conservation des documents (voir A/CN.9/WG.IV/WP.153, par. 36). L'existence d'un important corpus législatif

traitant des signatures électroniques[6] et l'expérience acquise dans l'application de ces lois peuvent contribuer à l'examen de cette proposition.

59. Le règlement eIDAS offre un exemple de législation complète sur les services de confiance. Il contient des dispositions générales notamment sur la responsabilité et la charge de la preuve (art. 13 ; voir ci-dessus, par. 23 à 26), le contrôle (art. 17 ; voir ci-dessus, par. 53) et les exigences de sécurité (art. 19 ; voir ci-dessus, par. 44, sur l'obligation de notification des atteintes à la sécurité ou des pertes de données).

60. Le règlement eIDAS contient une section spécifique applicable à tous les services de confiance qualifiés. Ces derniers sont aisément trouvables car ils figurent dans une liste de confiance tenue par les États membres de l'Union européenne. À cet égard, le Groupe de travail voudra peut-être se demander s'il faudrait établir une distinction entre les différents services de confiance en se fondant sur le niveau de garantie à associer à chacun d'entre eux et, dans ce cas, quel mécanisme institutionnel devrait servir à distinguer ces services.

61. Le règlement eIDAS comporte également des dispositions spécifiques portant sur les services de confiance suivants : signatures électroniques ; cachets électroniques ; horodatages électroniques ; services d'envoi recommandé électronique et authentification de site internet[7]. Chaque service de confiance peut être fourni sous forme qualifiée. Les signatures et les cachets électroniques peuvent aussi être fournis sous forme avancée.

62. La loi 045-2009/AN du Burkina Faso comporte une section sur les dispositions applicables à tous les prestataires de services de confiance, ainsi que des dispositions sur la procédure d'accréditation permettant d'obtenir le statut de prestataire qualifié. On y trouve également des dispositions spécifiques pour les certificats électroniques qualifiés, l'archivage électronique, l'horodatage électronique et les services d'envoi recommandé électronique. La loi comprend par ailleurs un chapitre entièrement consacré aux signatures électroniques.

63. La loi 2017-20 du Bénin comporte une section générale applicable à tous les prestataires de services de confiance et des dispositions particulières concernant les services de confiance suivants : signatures électroniques ; cachets électroniques ; horodatages électroniques et archivage électronique.

64. La loi 2017-20 du Bénin précise, à l'article 301, que « [l]'archivage électronique garantit l'authenticité et l'intégrité des documents, données et informations conservés par ce moyen ». Elle contient également une disposition sur l'équivalence fonctionnelle similaire à l'article 10 de la Loi type de la CNUDCI sur le commerce électronique.

65. L'article 302 de la loi 2017-20 du Bénin indique par ailleurs que l'archivage électronique vise à conserver des données, documents et informations en vue d'une utilisation ultérieure, et que les données concernées doivent être structurées, indexées et conservées sur des formats appropriés à la conservation et à la migration (voir aussi ci-dessus, par. 51). L'accès devrait être possible indépendamment de l'évolution des technologies. La disposition s'applique aussi bien aux documents émis sous forme électronique qu'aux documents papier ultérieurement numérisés.

66. La loi 2017-07 du Togo comporte également une section sur les dispositions applicables à tous les prestataires de services de confiance, notamment les procédures permettant d'obtenir le statut de prestataire de services de confiance qualifié. On y trouve aussi des dispositions particulières portant sur les certificats électroniques, l'archivage électronique, les horodatages électroniques et les services d'envoi

---

[6] Le système de suivi mondial du cyberdroit (Global Cyberlaw Tracker) de la CNUCED indique que 145 États, soit 78 % du total, ont adopté des lois sur les transactions électroniques, qui comportent généralement des dispositions sur les signatures électroniques.

[7] Ces services de confiance sont définis dans le document A/CN.9/WG.IV/WP.150.

recommandé électronique. La loi comprend par ailleurs un chapitre entièrement consacré aux signatures électroniques.

67. La loi 2017-07 du Togo est complétée par le décret 2018-062/PR qui établit de surcroît des obligations à remplir par tous les prestataires de services de confiance. Ces obligations portent sur la sécurité et la confidentialité des données, la responsabilité, les ressources financières, l'accessibilité, la protection des données, la transparence et la gestion des risques. En outre, le décret comporte des dispositions concernant chacun des services de confiance recensés dans la loi 2017-07.

68. On citera au nombre des autres services de confiance qui ont été identifiés mais n'ont pas encore fait l'objet d'un traitement législatif spécifique, les comptes séquestre électroniques et les preuves de présence électronique. Ce dernier service a été examiné en lien avec les testaments électroniques[8].

69. Le Groupe de travail voudra peut-être se demander s'il conviendrait ou non d'utiliser les mêmes mécanismes pour le traitement juridique des dispositifs de gestion d'identité et des services de confiance. En outre, il souhaitera peut-être s'interroger quant à savoir si le traitement juridique des services de confiance devrait envisager une liste ouverte de tels services se fondant sur une définition commune de la notion de « service de confiance », ou plutôt prévoir des règles communes applicables à tous les services de confiance et des règles spécifiques applicables à chacun d'entre eux. En particulier, il voudra peut-être voir s'il faudrait élaborer des règles d'équivalence fonctionnelle pour chaque service de confiance et s'il conviendrait également de renvoyer à des niveaux de garantie dans le contexte des services de confiance.

[8] Voir par exemple l'article 8 du projet de Electronic Wills Act en cours d'élaboration par la National Conference of Commissioners on Uniform State Laws.