Nations Unies A/CN.9/1113

Assemblée générale

Distr. générale
30 mai 2022
Français
Original : anglais/français

Commission des Nations Unies pour le droit commercial international
Cinquante-cinquième session
New York, 27 juin-15 juillet2022

Commented [Start1]: <<ODS JOB NO>>N2203488F<<ODS JOB NO>>
<<ODS DOC SYMBOL1>>A/CN.9/1113<<ODS DOC SYMBOL1>>
<<ODS DOC SYMBOL2>><<ODS DOC SYMBOL2>>

Projet de loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance

Compilation des commentaires reçus de gouvernements et d'organisations internationales

Table des matières

		Page
I.	Introduction	2
II.	Compilation des commentaires	2
A.	Banque mondiale	2
B.	Allemagne, Autriche, Belgique, France, Pologne, Tchéquie, Union européenne, Union internationale du notariat et Conseil des notariats de l'Union européenne	7
C.	International and Comparative Law Research Center	15
D.	Ordre des avocats de Paris	17
E.	Banque asiatique de développement	17

V.22-03488 (F) 230622 240622
2203488

Merci de recycler

I. Introduction

1. À sa quarante-neuvième session, en 2016, la Commission était saisie d'une note du secrétariat portant sur les questions juridiques liées à la gestion de l'identité et aux services de confiance (A/CN.9/891), qui résumait les débats tenus pendant le colloque de la CNUDCI organisé sur ce thème à Vienne, les 21 et 22 avril 2016. Elle est convenue que les questions de la gestion de l'identité et des services de confiance devaient rester inscrites au programme du Groupe de travail IV (Commerce électronique) (A/71/17, par. 228). Ce dernier a donc entrepris l'examen de ce sujet à sa cinquante-quatrième session (Vienne, 31 octobre-4 novembre 2016).

2. À sa cinquante-quatrième session, en 2021, la Commission s'est déclarée satisfaite des progrès réalisés par le Groupe de travail IV dans les travaux qu'il menait au sujet des questions juridiques liées à la gestion de l'identité et aux services de confiance, et l'a encouragé à achever ceux-ci et à les lui soumettre pour examen à sa cinquante-cinquième session, en 2022.

3. À sa soixante-deuxième session (Vienne, 22-26 novembre 2021), le Groupe de travail IV a achevé sa troisième lecture du projet de dispositions sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance et de la note explicative qui l'accompagne. À cette session, il a prié le secrétariat de réviser le projet de dispositions et le projet de note explicative en tenant compte de ses délibérations et décisions et de communiquer le texte ainsi modifié à la Commission, sous la forme d'une loi type, afin qu'elle l'examine à sa cinquante-cinquième session, en 2022. Le secrétariat a également été prié de communiquer le texte révisé à tous les gouvernements et aux organisations internationales compétentes, afin qu'ils fassent part de leurs observations, et de compiler les observations reçues en vue de leur examen par la Commission (A/CN.9/1087, par. 11).

4. Les textes révisés du projet de loi type et du projet de note explicative ont été regroupés et transmis à la Commission (A/CN.9/1112). Par une note verbale datée du 21 avril 2022, le Secrétariat a transmis ceux-ci aux États et aux organisations internationales invitées, afin qu'ils puissent formuler des observations.

5. On trouvera dans le présent document les commentaires reçus par le Secrétariat au sujet du projet de loi type et du projet de note explicative. Ceux-ci sont reproduits tels qu'ils ont été reçus par le Secrétariat, avec quelques modifications de forme. Les commentaires qui lui parviendront après la publication du présent document seront publiés sous forme d'additifs, dans l'ordre dans lequel ils auront été reçus.

II. Compilation des commentaires

A. Banque mondiale

[Original : anglais]
[21 avril 2022]

1. Pour donner suite à la demande du Groupe de travail, la Banque mondiale a le plaisir de lui présenter les observations suivantes sur le projet de loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance (A/CN.9/1112), et plus particulièrement sur le projet de note explicative (annexe II), à l'occasion de la soixante-troisième session tenue par le Groupe de travail IV à New York (session hybride en présentiel et en ligne) du 4 au 8 mars 2022. Les références contenues dans ces commentaires renvoient aux paragraphes de la note explicative.

2. La Banque mondiale estime que ces ajouts sont conformes aux discussions tenues et aux décisions prises par le Groupe de travail, qu'ils appuient. Ces précisions n'ont pas pour but de relancer les discussions sur des questions qui ont déjà été

tranchées, mais plutôt de contribuer à une lecture plus cohérente de la Loi type, et donc à son adoption.

3. Les observations sont divisées en deux parties : la première **(1)** présente la partie pertinente du texte de la note explicative telle quelle, en proposant des ajouts qui figurent entre crochets et sont soulignés (c'est-à-dire que le texte proposé serait indiqué comme suit : « [par exemple] ») et en réinsérant des parties de texte supprimées précédemment, qui figurent entre crochets et sont en italique (c'est-à-dire que le texte proposé serait indiqué comme suit : « [*par exemple*] ») ; et la seconde **(2)** motive chacune des propositions, dans l'ordre dans lequel elles apparaissent dans la note :

1. Texte actuel de la note explicative avec les ajouts proposés :

47. L'identification est le processus qui consiste à distinguer [de manière unique] une personne sur la base d'informations la concernant [dans un contexte particulier] (à savoir des attributs), qui peuvent être recueillies ou observées. Elle consiste à vérifier que les attributs recueillis ou observés correspondent à une « identité » préalablement établie pour la personne identifiée. Ainsi, l'identification a souvent lieu lorsqu'une personne invoque une identité particulière et présente des attributs en vue de sa vérification. [*L'identification est particulièrement importante pour instaurer la confiance dans les opérations en ligne*[1]. *Elle consiste essentiellement à vérifier que les attributs recueillis ou observés correspondent à une « identité » préalablement établie pour la personne identifiée*] [(on parle de « confirmation d'identité » lorsqu'il s'agit d'établir l'identité unique d'une personne ; et d'« identification électronique », ou d'« authentification » dans certains pays, lorsqu'il s'agit de vérifier a posteriori des justificatifs attestant de cette identité dans une opération particulière).]

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

a) La première étape de la gestion de l'identité consiste à recueillir les attributs qui peuvent constituer l'« identité fondamentale » de la personne (c'est-à-dire les attributs [de base] qui sont généralement enregistrés par des organismes publics dans les registres et statistiques de l'état civil [ou les systèmes d'identification fondamentale] lorsqu'il s'agit de personnes physiques et dans les registres des sociétés et des entreprises lorsqu'il s'agit de personnes morales). Ces attributs peuvent être présentés sous la forme de justificatifs délivrés [ou reconnus] par les administrations publiques (par exemple, un certificat d'enregistrement) et vérifiés auprès de l'organisme émetteur. [La mesure dans laquelle le justificatif peut être reconnu est déterminée sur la base d'un examen de l'objet pour lequel celui-ci a été émis.] Ce processus, qui peut être exécuté [soit par des moyens électroniques soit] « hors ligne » [,] à l'aide de justificatifs matériels présentés en personne, aboutit à la délivrance de justificatifs à la personne ;

2. Raisons expliquant les différents ajouts qu'il est proposé d'apporter à la note explicative :

2.1 Premièrement, l'ajout proposé (au paragraphe 47) des mots « de manière unique » et « dans un contexte particulier » traduit le principe, déjà accepté par le Groupe de travail, selon lequel la nature du justificatif d'identité reflète le caractère unique de la personne dans un contexte donné. Si certains justificatifs d'identité peuvent être utilisés et acceptés de manière relativement générale, les justificatifs

[1] Banque mondiale. 2021. *Rapport sur le développement dans le monde 2021 : Des données au service d'une vie meilleure*. Washington, Banque mondiale. https://www.worldbank.org/en/publication/wdr2021.

d'identité ne permettent pas nécessairement tous d'identifier efficacement ou valablement une personne dans un autre contexte – de fait, nombre d'entre eux ne sont pas destinés à être utilisés à grande échelle. Cette logique est reflétée et mise en évidence dans les travaux du Groupe de travail et du secrétariat, et a été acceptée par le Groupe de travail, une fois incorporée dans le texte de la Loi type, qui définit l'« *identité* », à l'article 1 d), comme « *un ensemble d'attributs qui permet à une personne d'être identifiée de manière unique dans un contexte particulier* » (*le soulignement est de l'auteur*). Par conséquent, les termes proposés – « de manière unique » et « dans un contexte particulier » – devraient également être inclus dans la note explicative, afin d'assurer la cohérence entre la Loi type et la note.

2.2 Deuxièmement, au paragraphe 47, la Banque mondiale demande que la phrase faisant référence à l'instauration de la confiance soit rétablie. La phrase en question – « *L'identification est particulièrement importante pour instaurer la confiance dans les opérations en ligne* » – est importante pour permettre une compréhension globale et plus vaste des motivations qui sous-tendent la Loi type, et est nécessaire pour mettre en évidence les objectifs que l'identification électronique (par opposition aux services de confiance) est censée poursuivre. Comme l'indique le titre de la Loi type, la confiance dans les opérations en ligne est au cœur de la question, et le renforcement de la confiance est un élément clef et un objectif des travaux en général. Toutefois, en raison de la structure double (quoique parallèle) de la Loi type, il est nécessaire de rappeler expressément l'importance de l'établissement de la confiance dans le contexte de la gestion de l'identité (par opposition à la partie concernant les services de confiance). La phrase en question reflète les discussions tenues par le Groupe de travail tout au long de ses sessions au sujet de la « fiabilité ». La Banque mondiale, entre autres, a soulevé cette question lors de plusieurs sessions du Groupe de travail, et a renvoyé ce dernier à son principal rapport sur la question, à savoir le *Rapport sur le développement dans le monde 2021 : Des données au service d'une vie meilleure*[2]. La Banque mondiale souhaiterait également l'introduction d'une note de bas de page faisant référence à ce rapport à la fin de cette phrase. Comme elle est une institution spécialisée des Nations Unies, il ne serait en effet pas inapproprié de mentionner un tel produit, et cela correspondrait aux références faites, ailleurs dans la note, aux produits élaborés par des organismes des Nations Unies – la note de bas de page 1 de la note par exemple fait référence à un rapport de la CNUCED.

2.3 Troisièmement, au paragraphe 47, la Banque mondiale souhaiterait que la phrase qui suit immédiatement celle évoquée au paragraphe 2.2 ci-dessus soit tout d'abord rétablie, puis complétée comme suit : « *Elle consiste essentiellement à vérifier que les attributs recueillis ou observés correspondent à une « identité » préalablement établie pour la personne identifiée* (on parle de « confirmation d'identité » lorsqu'il s'agit d'établir l'identité unique d'une personne ; et d'« identification électronique », ou d'« authentification » dans certains pays, lorsqu'il s'agit de vérifier a posteriori des justificatifs attestant de cette identité dans une opération particulière) ». La Banque mondiale estime qu'il est important de rétablir ainsi cette phrase et de la compléter car cela permettrait, premièrement, d'éviter toute confusion possible et, deuxièmement, de combler les lacunes entre les différentes notions d'« identité ». Sur ce point, et avant d'expliquer la logique qui sous-tend cette proposition, la Banque mondiale souhaite renouveler son soutien à la décision prise par le Groupe de travail d'utiliser le terme « identification électronique » plutôt qu'« authentification » dans la Loi type pour décrire la seconde phase du processus de gestion de l'identité, et souligner que la Loi type représente une étape importante dans la réalisation des objectifs de développement durable[3]. La délégation de la Banque mondiale avait toutefois cru comprendre qu'à l'issue des longues discussions tenues sur ce sujet lors des sessions précédentes, le Groupe de travail avait décidé de mentionner l'utilisation du terme « authentification » dans la

[2] Ibid.
[3] Cible 16.9 de l'objectif de développement durable n° 16. https://sdgs.un.org/fr/goals/goal16.

note explicative afin de garantir la clarté d'utilisation du terme « identification électronique ».

La Banque mondiale se fonde sur sa vaste expérience accumulée dans le domaine du financement de projets d'identification numérique dans divers pays pour formuler cette proposition, car dans ce cadre, le terme « identification », indépendamment du qualificatif employé, peut être interprété comme renvoyant à quelque chose d'autre, ou du moins de plus limité, que le sens que lui donne la Loi type. Comme on l'a noté au cours des délibérations du Groupe de travail, tout a une signification culturelle et, quelle que soit la définition d'un terme, il convient de respecter cette signification culturelle sous-jacente. Par exemple, les interprétations faites dans la langue française et dans les systèmes administratifs qui suivent cette tradition donnent un sens juridique solide à la notion d'« identité » et, par extension, de processus d'« identification ». Ces interprétations multidimensionnelles sont fondamentalement de nature relationnelle, avec des attributs obligatoires utilisés pour définir l'identité, notamment la date et le lieu de naissance, la filiation et la profession, entre autres. Il découle de cette conception qu'une personne n'est pas identifiée à partir de rien mais plutôt que, pour être « identifiée » et avoir une « identité », elle doit être reliée à certains de ses attributs. La Loi type, cependant, admet de nombreux cas où plusieurs de ces attributs associés ne sont ni nécessaires, ni même nécessairement justifiés. En effet, dans de nombreux cas d'échanges commerciaux électroniques, seuls des attributs limités et fondamentaux sont souvent requis pour identifier une personne. Par conséquent, c'est précisément pour des raisons d'interprétation dans de tels contextes – c'est-à-dire dans les cas où le terme « identification » a un certain sens culturel et juridique plus solide et plus établi, et qu'il risque implicitement de conduire les lecteurs issus de tels contextes à lui donner un sens différent de celui visé par la Loi type – que la Banque mondiale propose cette formule supplémentaire.

La Banque mondiale estime qu'il est essentiel d'apporter ces précisions sur l'« authentification » dans la note explicative, afin d'éviter toute confusion. En effet, elle a pris conscience de ce risque dans le cadre des opérations menées dans différents pays.

2.4 Quatrièmement, comme c'est le cas du point évoqué au paragraphe 2.1 ci-dessus, l'insertion proposée (au paragraphe 48) de la formule « pour une transaction déterminée (c'est-à-dire l'identification électronique) » vise à réaffirmer que la présentation et la vérification des justificatifs d'identité par des moyens électroniques sont spécifiques au contexte, et ont pour objet l'identification électronique (c'est-à-dire la seconde étape du processus d'identification).

2.5 Cinquièmement, l'ajout proposé (au paragraphe 48 a)) des mots « de base » comme qualificatif des attributs, et de la formule « ou les systèmes d'identification fondamentale » en complément des « registres et statistiques de l'état civil » – est un prolongement de la logique présentée au paragraphe 2.3 ci-dessus. Ces ajouts sont conformes au langage et à l'approche adoptés par le Groupe de travail, y compris le langage utilisé par le Secrétariat dans ses documents, et celui qui a été convenu au niveau international et est dûment observé par les organismes des Nations Unies. Nous les abordons l'un après l'autre :

2.5.1 Premièrement, l'ajout des mots « de base » est important, car ceux-ci constituent un qualificatif essentiel qui précise ce que la note explicative dit déjà, mais que l'on pourrait facilement interpréter de manière erronée. La note explicative parle déjà de « recueillir les attributs qui peuvent constituer l'"identité fondamentale" de la personne ». L'identité fondamentale ne requiert pas davantage que des attributs de base pour être fondamentale.

2.5.2 Deuxièmement, l'insertion des mots « ou les systèmes d'identification fondamentale » est impérative pour permettre une adoption large et réussie de la Loi type. Comme indiqué au paragraphe 2.5.1 ci-dessus, la note explicative parle déjà d'« identité fondamentale », et le Groupe de travail et le Secrétariat ont utilisé ce terme à plusieurs reprises dans leurs délibérations

et discussions, en l'opposant aux justificatifs d'identité « transactionnelle » ou « fonctionnelle »[4]. Si l'on peut considérer que la question de l'identification fondamentale sortirait du cadre du travail, cela ne signifie pas qu'il faille renoncer à utiliser une terminologie spécifique bien acceptée, ou à y recourir, lorsque cette terminologie est appropriée[5]. Telle qu'elle est actuellement rédigée, la note laisse entendre, à tort, que les registres et statistiques de l'état civil sont la seule source de création de l'identité fondamentale. Étant donné que la notion d'« identité fondamentale » est déjà utilisée dans le texte, ainsi que dans les rapports établis par le Secrétariat et qu'elle a été acceptée par le Groupe de travail, l'ajout proposé des mots « ou les systèmes d'identification fondamentale » permet de lever une ambiguïté, tout en respectant les interprétations du Groupe de travail.

2.6 Sixièmement, et là encore, il s'agit d'une proposition découlant de l'expérience accumulée par la Banque mondiale dans le cadre d'opérations menées dans différents pays, l'ajout proposé (au paragraphe 48 a)) des mots « ou reconnus » à côté de la référence existante aux « justificatifs délivrés par les administrations publiques » est important car il se peut que le justificatif ne soit pas délivré par une administration publique. En effet, il arrive assez fréquemment que les gouvernements délèguent au secteur privé la tâche d'élaborer et de délivrer des justificatifs d'identité. Dans ce contexte, la formule proposée est jugée essentielle à la cohérence globale et à l'applicabilité de la Loi type et considérée comme un ajout important à la note explicative.

2.7 Septièmement, l'ajout proposé (au paragraphe 48 a)) de la phrase « La mesure dans laquelle le justificatif peut être reconnu est déterminée sur la base d'un examen de l'objet pour lequel celui-ci a été émis » vise à établir un lien avec la logique du point soulevé au paragraphe 2.4 ci-dessus, selon laquelle la présentation et la vérification des justificatifs d'identité par des moyens électroniques sont interprétées comme étant spécifiques au contexte.

2.8 Huitièmement, l'ajout proposé (au paragraphe 48 a)) de « soit par des moyens électroniques soit » est lui aussi destiné à compléter la formule existante dans la note explicative, à savoir les mots « hors ligne ». Cet ajout est important dans le cas des justificatifs d'identité matériels présentés en personne, pour lesquels une certaine forme de vérification hors ligne – par exemple à travers une inspection visuelle – peut être complétée par une certaine forme de vérification électronique, par exemple à travers la connexion à un système dorsal, ou à travers le scannage d'un élément du justificatif physique, comme un code QR, qui n'est pas nécessairement relié à un système dorsal mais est susceptible de lire le code QR (sécurisé) pour rechercher une signature numérique. Il peut donc y avoir des contextes dans lesquels un moyen électronique de vérification est appliqué à un justificatif d'identité matériel, cas de figure qui n'est pas pleinement ou adéquatement pris en compte dans la formule « hors ligne » utilisée pour qualifier le processus. L'ajout de la formule proposée est jugé important pour permettre une lecture cohérente et complète de la Loi type.

2.9 Enfin, sur le plan rédactionnel, la Banque mondiale propose que les éventuelles références restantes au « respect de la vie privée et à la protection des

[4] Voir notamment le document A/CN.9/WG.IV/WP.153 (où il est dit que « La détermination primaire de l'identité, ou identité fondamentale, correspond à l'attribution de l'identité dans le contexte d'origine de l'entité et au moment de son origine » (par. 8), et que « Dans certains cas, [l'identification] peut reposer sur l'utilisation d'un processus de justification et d'authentification de l'identité qui établit l'identité sur la base de justificatifs de l'identité fondamentale. Par conséquent, la reconnaissance juridique de l'identité fondamentale entre pays et entre systèmes de gestion de l'identité pourrait se révéler utile, voire nécessaire. »). Voir également les documents A/CN.9/WG.IV/WP.158 et A/CN.9/WG.IV/WP.163.

[5] Voir par exemple la note de bas de page 7 du document A/CN.9/WG.IV/WP.153 (où il est dit que « Lorsqu'il examinera la définition du terme "identité", le Groupe de travail voudra peut-être se demander s'il est nécessaire de poser l'exigence de l'unicité aux fins de ses travaux étant donné que : a) l'unicité est un attribut de l'identité fondamentale, et b) l'identité fondamentale est actuellement exclue du champ de ses travaux »).

données » soient modifiées pour renvoyer à « la protection et à la confidentialité des données », car cela permettrait de replacer la « confidentialité » dans le contexte de la « protection des données », plutôt que d'évoquer le droit fondamental à la vie privée, bien plus large. Cette formule a déjà été retenue dans le texte de la Loi type, comme le Secrétariat l'a confirmé lors de cette dernière session.

La délégation de la Banque mondiale estime que ces ajouts amélioreront la cohérence et la clarté de la note explicative, et qu'ils découlent naturellement du langage et de la logique adoptés par le Groupe de travail, y compris le langage utilisé par le Secrétariat dans ses documents. S'il n'est pas possible de faire une lecture complète, claire et cohérente de la Loi type, appuyée par la note explicative, on risque de limiter considérablement la mesure dans laquelle la Loi type sera appliquée et adoptée.

B. Allemagne, Autriche, Belgique, France, Pologne, Tchéquie, Union européenne, Union internationale du notariat et Conseil des notariats de l'Union européenne

[Original : anglais]
[25 mai 2022]

I. Contexte et problématique

1. À sa soixante-troisième session, le Groupe de travail a examiné les dernières questions en suspens concernant le projet de loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance. Nous pensons avoir trouvé un consensus sur la plupart de ces questions lors de cette session.

2. Néanmoins, nos délégations souhaitent attirer l'attention de toutes les délégations auprès de la CNUDCI sur les articles 9 et 10 relatifs à la gestion de l'identité, ainsi que sur les articles 16 à 21 et l'article 22 relatifs aux services de confiance, pour lesquels **aucun consensus n'a été atteint au sein du Groupe de travail**. Il existe actuellement deux positions divergentes sur ces articles.

3. Dans ce contexte, le **document** A/CN.9/1112 transmis par le secrétariat à la Commission à des fins d'examen à sa cinquante-cinquième session **ne reflète pas les délibérations tenues ni les décisions prises par le Groupe de travail au cours des dernières sessions**. Plus particulièrement, il ne présente qu'une seule position, au sujet de laquelle nous avons exprimé nos réserves à plusieurs reprises lors des dernières sessions. Nous regrettons également que la position en question ne figure pas du moins entre crochets – pratique usuelle dans les négociations internationales – malgré le fait que le Groupe de travail n'ait pas pris de décision au sujet de ces articles.

4. Par les présents commentaires, nous souhaitons rappeler la problématique (point II), expliquer notre position sur le principe de fiabilité de la méthode (III), et préciser les modifications que nous demandons dans le projet de loi type et la note explicative (point IV).

II. Contexte

5. Comme on peut le lire dans le rapport de la soixante et unième session (document A/CN.9/1051), il y a eu des discussions (par. 45 à 51) au sujet des articles 16 à 21 et de l'article 22 (articles relatifs aux services de confiance, qui font pendant aux articles 9 et 10 relatifs à la gestion de l'identité). On peut surtout y lire **qu'il y avait alors deux positions différentes et que le Groupe de travail n'a pas pris de décision sur ces articles étant donné qu'aucun consensus n'avait été atteint**.

6. Nos délégations ont donc été très surprises de voir, dans le document établi par le secrétariat en vue de la soixante-deuxième session, en novembre 2021 (document A/CN.9/WG.IV/WP.170), que les articles 9, 10, 16 à 21 et 22 avaient été modifiés par

celui-ci. Le secrétariat avait en effet uniquement inséré l'une des propositions, sans la mettre entre crochets, ce qui avait été suggéré par quelques autres délégations (bien qu'aucun consensus n'ait été atteint), comme si le Groupe de travail était parvenu à un accord, et sans tenir compte d'autres positions, notamment celle de nos délégations. Comme on peut le constater dans le rapport sur les travaux de cette soixante-deuxième session (document A/CN.9/1087), nos délégations ont contesté la formulation adoptée dans les articles 9 et 10 (voir par. 38 à 46, et en particulier par. 39 et 40 du rapport) et le Groupe de travail n'est parvenu à aucun consensus ni aucune décision au cours de cette soixante-deuxième session. Dans ce contexte, nous avons été extrêmement surpris d'entendre une délégation dire ce qui suit lors de la soixante-troisième session, la dernière en date : « *Il a été ajouté qu'à la soixante-deuxième session, il n'avait pas été estimé que l'article 10 présentait un déséquilibre, et que le Groupe de travail devait bien réfléchir avant de réexaminer des questions à un stade aussi avancé des délibérations.* » (document A/CN.9/1093). Nous avons également été **surpris de constater que le document** A/CN.9/1112 **établi par le secrétariat ne tenait pas compte des deux points de vue divergents** exprimés lors de la soixante-deuxième session du Groupe de travail.

7. Nos délégations ont répété avec insistance notre position lors de la soixante-troisième session du Groupe de travail. Nous avons également fait une déclaration commune au cours de cette session pour regretter cette situation et demander au secrétariat de refléter les deux positions dans le texte qui serait transmis à la Commission pour la session de juillet, malheureusement en vain.

8. Dans ce contexte, nous avons également proposé de modifier une partie du projet de synthèse couvrant la soixante-troisième session du Groupe de travail, dans un souci de transparence et afin de refléter plus exactement les interventions de nos délégations. La délégation des États-Unis d'Amérique s'est opposée à ces changements, sans aucune justification. Encore une fois, nous regrettons les objections soulevées par cette délégation et contestons également cette façon de procéder, raison pour laquelle le document A/CN.9/1093 ne constitue pas le rapport du Groupe de travail mais uniquement un résumé de la Présidente et du Rapporteur sur les travaux de la soixante-troisième session du Groupe de travail IV (Commerce électronique).

III. Principe de fiabilité de la méthode

9. Le fait que l'identification (ou les fonctions liées aux services de confiance) soit uniquement utile si elle est fiable constitue un élément central du projet, et est en principe admis par toutes les délégations (voir la version actuelle de la note explicative, par. 143).

10. Le texte actuel (document A/CN.9/1112) ne préserve toutefois plus ce principe.

11. Tout d'abord, l'article 9 ne prévoit plus que l'exigence d'identification est satisfaite si une méthode **fiable** est utilisée, ce qui le prive de son contenu essentiel et le rend redondant. Nous pouvons faire les mêmes remarques pour les articles 16 à 21.

12. Deuxièmement, l'article 10-1 b), dans sa version actuelle, remet en question le principe de fiabilité.

13. L'article 10-1 b) permet l'identification avec une méthode qui a « *démontré dans les faits qu'elle a rempli la fonction décrite à l'article 9* ». Contrairement à la méthode visée à l'article 10-1 a), une méthode qui a uniquement « *démontré dans les faits qu'elle a rempli la fonction décrite à l'article 9* » n'est pas nécessairement fiable (voir par. 143 de la version actuelle de la note explicative). L'article 10-1 b) est donc contraire au consensus auquel le Groupe de travail était parvenu, selon lequel toutes les méthodes visées à l'article 9 doivent être fiables. En introduisant une identification de fait (art. 10-1 b)) comme alternative à l'identification par une méthode fiable (art. 10-1 a)), on contourne le principe fondamental de la fiabilité.

14. D'autres délégations ont fait valoir que l'introduction de l'article 10-1 b) permettrait d'éviter des procédures judiciaires inutiles. Toutefois, en cas de doute, le

seul moyen de déterminer si une méthode a « *démontré dans les faits qu'elle a rempli la fonction décrite à l'article 9* » consiste à laisser à un tribunal le soin de trancher cette question. La clause dite « de sauvegarde » contenue à l'article 10-1 b) ne permet donc pas adéquatement de prévenir les procédures judiciaires.

15. Nous reconnaissons toutefois que le fait qu'une méthode ait rempli son objectif peut être important. En guise de compromis, nous suggérons donc de déplacer le contenu de l'article 10-1 b) à l'article 10-2 f). De cette façon, son contenu pourra être pris en compte avec toutes les autres circonstances pertinentes.

16. Cette proposition est également neutre du point de vue du système :

- L'article 10-2 décrit les circonstances qui peuvent être prises en considération pour déterminer la fiabilité, si celle-ci est déterminée *ex post* ;
- L'article 10-4, quant à lui, dispose qu'une méthode désignée *ex ante* est toujours présumée fiable ;
- L'article 10-1 est neutre par rapport au système et indique simplement qu'il n'existe pas de niveau abstrait de fiabilité, et que l'identification doit uniquement « *être suffisamment fiable* », concept sur lequel le Groupe de travail s'est toujours entendu.

17. Nous pouvons faire les mêmes remarques, *mutatis mutandis*, pour l'article 22.

IV. Modifications demandées dans le document A/CN.9/1112

18. Pour résumer notre position, il convient de veiller à ce que les textes de la loi type et de la note explicative reflètent deux grands principes :

1. La méthode utilisée pour remplir la fonction doit toujours être « fiable » ;

2. La loi type ne devrait pas laisser entendre que la méthode peut être évaluée autrement que par :

a. Les autorités désignées dans l'État adoptant (approche *ex ante*) ou

b. Un tribunal dans le cadre de l'examen des différents facteurs énumérés à l'article 10-2, en cas de litige (approche *ex post*).

Par ailleurs, les conséquences juridiques particulières (présomption et renversement de la charge de la preuve) devraient uniquement bénéficier à la méthode désignée dans l'approche *ex ante*. Elles ne devraient bénéficier à aucune méthode utilisée dans l'approche *ex post*, et encore moins à une méthode qui a uniquement « démontré dans les faits qu'elle a rempli la fonction », puisque cette méthode n'a pas nécessairement besoin d'être fiable et qu'on ne sait pas très bien qui évaluera ce qui constitue une « démonstration dans les faits ».

19. Les modifications proposées ci-après visent à souligner ces deux principes (les modifications sont soulignées : les ajouts sont indiqués en **caractères gras**, les suppressions en ~~caractères barrés~~).

Annexe I – Projet de loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance

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

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

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

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

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

~~(b) Avoir démontré dans les faits qu'elle a rempli la fonction décrite à l'article 9~~.

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

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

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

i) La gouvernance ;

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

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

iv) La conservation des documents ;

v) Les installations et le personnel ;

vi) Les contrôles techniques ; et

vii) Le contrôle et l'audit ;

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

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

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

f) Avoir démontré dans les faits qu'elle a rempli la fonction décrite à l'article 9 ; et

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

3. (…).

Article 16. Signatures électroniques

Lorsque la loi exige la signature d'une personne, ou prévoit des conséquences en l'absence de signature, cette exigence est satisfaite dans le cas d'un message de données si une méthode **fiable** est utilisée pour :

a) Identifier la personne ; et

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

Article 17. Cachets électroniques

Lorsque la loi exige qu'une personne morale appose un cachet, ou prévoit des conséquences en l'absence de cachet, cette exigence est satisfaite dans le cas d'un message de données si une méthode **fiable** est utilisée pour :

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

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

Article 18. Horodatages électroniques

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

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

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

Article 19. Archivage électronique

Lorsque la loi exige que des documents, documents d'activité ou informations soient conservés, ou prévoit des conséquences en l'absence de leur conservation, cette exigence est satisfaite dans le cas d'un message de données si une méthode **fiable** est utilisée pour :

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

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

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

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

Article 20. Services d'envoi recommandé électroniques

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

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

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

c) Identifier l'expéditeur et le destinataire.

Article 21. Authentification de site Web

Lorsque la loi exige l'authentification du site Web, ou prévoit des conséquences en l'absence d'authentification, cette exigence est satisfaite si une méthode **fiable** est utilisée pour :

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

b) Associer cette personne au site Web.

Article 22. Critères de fiabilité pour les services de confiance

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

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

~~(b) Avoir démontré dans les faits qu'elle a rempli les fonctions décrites dans l'article~~.

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

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

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

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

d) Toute norme sectorielle applicable ;

e) La sûreté du matériel et des logiciels ;

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

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

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

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

j) Avoir démontré dans les faits qu'elle a rempli la fonction décrite dans l'article concerné (articles 16 à 21) ; et

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

3. (…).

Annexe II – Note explicative accompagnant le projet de loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance

57. Cette approche *ex ante* ~~peut~~ fourni**t** plus de clarté et de prévisibilité en ce qui concerne l'effet juridique des services de gestion de l'identité et des services de confiance **grâce aux présomptions et au renversement de la charge de la preuve**, y compris lorsqu'ils sont utilisés à l'échelle internationale. Toutefois, elle présuppose l'existence d'un mécanisme institutionnel, c'est-à-dire d'une entité compétente pour administrer le processus de désignation.

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

que le lieu d'origine, qui devrait déterminer si la reconnaissance juridique doit être accordée.

111. L'alinéa b) précise que le fait que le service de gestion de l'identité ne soit pas un service désigné n'empêche pas sa reconnaissance juridique. En d'autres termes, il accorde une reconnaissance juridique égale aux services de gestion de l'identité qui sont désignés ***ex ante*** et à ceux qui ne le sont pas **(faisant l'objet d'une évaluation *ex post* du juge)**, ce qui garantit la neutralité quant à l'approche choisie pour évaluer la fiabilité. Toutefois, il n'implique pas que tous les services de gestion de l'identité utilisent des méthodes fiables et offrent donc un niveau de garantie suffisant pour l'identification électronique : pour parvenir à ce résultat, la fiabilité de la méthode utilisée doit être évaluée conformément aux articles 10 et 11, selon le cas.

134. La méthode utilisée pour satisfaire à la règle de l'article 9 doit être **fiable et** conforme au paragraphe 1 de l'article 10, c'est-à-dire qu'elle doit être suffisamment fiable au regard de l'objet pour lequel le service de gestion de l'identité est utilisé~~ou avoir démontré dans les faits qu'elle a rempli la fonction pour laquelle elle a été utilisée~~.

138. L'identification électronique peut être utilisée pour satisfaire à l'obligation de vérifier certains attributs de l'identité d'une personne, par exemple l'âge ou le lieu de résidence, comme l'exige l'identification fondée sur des documents physiques. À cet égard, étant donné que la notion d'« identité » est définie par rapport au « contexte », qui détermine à son tour les attributs requis pour l'identification, l'identification effective d'une personne sur la base de l'article 9 comprend la vérification des attributs requis. Les mots « à cette fin » traduisent également la nécessité de vérifier les attributs pertinents. ~~Les dispositions énoncées à l'article 10 relatives à la fiabilité ne traitent pas de la vérification d'attributs particuliers, car elles portent sur les processus de gestion des justificatifs d'identité plutôt que sur les attributs contenus dans ces justificatifs.~~**Les dispositions relatives à la détermination de la fiabilité d'un service de gestion de l'identité énoncées à l'article 10 concernent également la méthode appliquée pour vérifier des attributs particuliers si cette vérification fait partie de l'identification électronique visée.**

~~142. Le paragraphe 1 b) contient une clause visant à empêcher la répudiation du service de gestion de l'identité lorsque celui-ci a effectivement rempli sa fonction. La répudiation se produit lorsqu'un sujet déclare ne pas avoir effectué une action. Pour que le mécanisme prévu au paragraphe 1 b) fonctionne, il faut que la méthode, qu'elle soit fiable ou non, ait effectivement rempli la fonction d'identification, c'est-à-dire qu'elle ait associé la personne qui cherche à s'identifier aux justificatifs d'identité. Cette disposition s'inspire de l'article 9-3 b) ii) de la CCE.~~

143. La Loi type exige ~~de manière générale~~ l'utilisation de méthodes fiables, et le paragraphe 2 f) n'entend pas promouvoir ni valider l'utilisation de méthodes non fiables. **Il reconnaît plutôt le rôle que les outils d'identification ayant fait leurs preuves peuvent jouer dans l'évaluation, par le juge, de la fiabilité d'un service de gestion de l'identité.** ~~Il reconnaît plutôt que, d'un point de vue technique, la fonction (dans le cas de l'article 9, l'identification) et la fiabilité sont deux attributs indépendants, et précise qu'en vertu de la Loi type, l'identification peut être assurée dans les faits ou par l'utilisation d'une méthode fiable. En d'autres termes, l'aboutissement de l'identification dans les faits évite de devoir évaluer la fiabilité de la méthode utilisée.~~

148. Les articles 10 et 11 font référence à la notion de « cadre relatif aux niveaux de garantie » ou à des cadres similaires désignés par d'autres termes. Le cadre relatif aux niveaux de garantie donne des indications aux parties utilisatrices sur le degré de confiance qu'elles peuvent accorder aux processus de contrôle de l'identité et d'identification électronique et les aide à déterminer s'ils sont adéquats à des fins spécifiques. La Loi type ne définit pas de niveaux de garantie ni n'exige la définition ou l'utilisation de tels niveaux. **Néanmoins, la définition des niveaux de garantie pourrait faciliter la reconnaissance internationale.**

187. L'exigence d'une signature papier est satisfaite si une méthode **fiable** est utilisée pour identifier le signataire du message de données et indiquer sa volonté concernant le message de données signé. La référence à la méthode **fiable** utilisée « concernant l'information contenue dans le message de données » s'applique tant à l'identification de la personne qu'à l'indication de sa volonté.

198. L'article 19 traite des services d'archivage électronique, qui assurent la sécurité juridique quant à la validité des documents électroniques conservés. La méthode **fiable** utilisée pour l'archivage électronique apporte une garantie quant à l'intégrité des documents électroniques archivés, ainsi qu'à la date et à l'heure de l'archivage. En outre, les informations archivées doivent être accessibles conformément à l'exigence d'équivalence fonctionnelle avec la notion de « forme écrite » dans l'environnement papier (art. 6-1 de la LTCE).

212. La LTSE et plusieurs lois régionales et nationales sur les signatures électroniques établissent une distinction entre les services de confiance selon qu'ils font l'objet d'une **évaluation *ex ante* ou *ex post* du** niveau de fiabilité qu'ils offrent. Plus précisément, ces lois confèrent des effets juridiques plus importants **(notamment des présomptions et un renversement de la charge de la preuve)** aux signatures électroniques qui **ont prouvé à l'avance qu'elles satisfaisaient** à certaines exigences **(approche *ex ante*)** et qui sont donc réputées offrir un niveau de fiabilité plus élevé **(voir par. 216 ci-dessous)**. En outre, certaines lois peuvent exiger que seules les signatures électroniques offrant un niveau de fiabilité ~~plus~~ élevé puissent être désignées. ~~Cette~~ **La même** approche ~~n'~~a ~~pas~~ été suivie dans la Loi type ~~et~~ **pour** les services de confiance~~peuvent être désignés indépendamment du niveau de fiabilité qu'ils offrent~~.

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

224. **Pour le moment, il** ~~L~~es niveaux de fiabilité définis dans les différents pays peuvent ne pas correspondre exactement. Ce décalage est même probable car il n'existe pas **à l'heure actuelle** de définitions des niveaux spécifiques de fiabilité qui soient reconnues à l'échelle mondiale **(en attendant l'émergence de normes internationales dans ce domaine)**. Pour surmonter les difficultés liées à la reconnaissance internationale qui découlent de ce décalage **temporaire**, **mais également dans l'optique du futur, lorsque des normes internationales auront été élaborées,** l'article 25 fait référence à la notion de « niveau de fiabilité au moins équivalent », qui englobe les niveaux de fiabilité identiques ou supérieurs à celui qui est requis. Cette notion ne doit pas être interprétée comme imposant le respect d'exigences techniques strictes, ce qui pourrait entraîner des obstacles à la reconnaissance mutuelle et, en fin de compte, au commerce, **mais aussi le non-respect du principe de neutralité technologique**.

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

C. International and Comparative Law Research Center

[Original : anglais]
[25 mai 2022]

1. Le International and Comparative Law Research Center (ci-après, l'« **ICLRC** ») fonde les présents commentaires sur le contenu des documents suivants :

- A/CN.9/1093 – Rapport du Groupe de travail IV (Commerce électronique) sur les travaux de sa soixante-troisième session (New York, 4-8 avril 2022) ;
- A/CN.9/1112 – Projet de loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance (ci-après, la « **Loi type** »), y compris la note explicative (ci-après, la « **note explicative** »).

2. Les commentaires contenus dans le présent document reflètent exclusivement le point de vue d'expert de l'ICLRC, qui assiste en tant qu'observateur aux sessions du Groupe de travail IV de la CNUDCI.

I. Contexte régional

3. Depuis plusieurs années, l'ICLRC suit les discussions menées par les experts au sein de l'Union économique eurasiatique (ci-après, « **l'UEE** ») au sujet du commerce électronique et de l'échange de données informatisé. Les économies des membres de l'UEE croissent rapidement grâce à l'émergence des technologies numériques et à leur introduction sur les marchés. Les États membres et l'UEE s'attachent actuellement à identifier une approche efficace et communément reconnue pour supprimer les obstacles aux flux de données électroniques entre les États membres et à établir un régime juridique complet relatif aux transactions numériques et à la reconnaissance internationale des enregistrements de données et des documents électroniques dans l'UEE.

4. Nous pensons que le travail d'expert mené par le Groupe de travail IV de la CNUDCI pourrait offrir des orientations utiles sur la gestion de l'identité et les services de confiance à l'échelle internationale, ainsi que des solutions pratiques bienvenues pour permettre l'élaboration d'un cadre juridique pertinent dans la région eurasiatique.

5. Dans ce contexte, si l'on veut disposer d'un guide véritablement exhaustif, nous pensons que le projet de loi type gagnerait à être retravaillé et à contenir des dispositions supplémentaires concernant l'équivalence, la fiabilité et la fonctionnalité des services de gestion de l'identité et des services de confiance. Les commentaires ci-dessous reflètent l'opinion de l'ICLRC quant aux approches qui pourraient être adoptées et soulignent plusieurs facteurs qui pourraient être pris en compte pour la mise en place d'un cadre international essentiel dans ce domaine.

II. Conditions minimales

6. Selon nous, les approches suivies par l'Union européenne et par le Conseil de l'Europe en matière de protection des données et de services de gestion de l'identité pourraient servir de meilleures pratiques, en raison de leur efficacité et de leur reconnaissance à l'échelle internationale. Celles-ci définissent un certain niveau minimal de protection garantissant aux utilisateurs de différents pays que leurs données sont protégées, quel que soit l'endroit exact – au sein du marché unique numérique – où elles sont traitées. Cette approche fondée sur des « conditions minimales » n'impose pas de charge excessive aux acteurs du marché.

7. Selon le paragraphe 114 de la note explicative, les obligations énoncées dans la Loi type sont décrites de manière technologiquement neutre, car l'application du principe de neutralité technologique dans le contexte de la gestion de l'identité exige que la configuration minimale requise fasse référence aux propriétés du système, et

non à des technologies spécifiques. Cependant, pour une raison qui nous échappe, cette approche des « conditions minimales » n'a apparemment pas été suivie à l'article 10 de la Loi type, qui constitue le mécanisme central de la reconnaissance internationale des services de gestion de l'identité.

8. À notre avis, les exigences énoncées à l'article 10-2 a) et b) de la Loi type peuvent difficilement être considérées comme minimales, et risquent d'accroître l'incertitude pour les acteurs du marché. Il est presque impossible d'imaginer qu'il soit possible de prendre en considération toutes les circonstances pertinentes et de respecter « toutes normes et procédures internationalement reconnues applicables qui sont pertinentes pour la fourniture de services de gestion de l'identité, notamment [le] cadre relatif aux niveaux de garantie ».

9. Pour en venir à ce que nous considérons comme les meilleures pratiques, on pourrait recommander l'utilisation d'un ensemble de principes et (ou) de critères spécifiques qui pourraient servir à évaluer la fiabilité de la méthode d'identification (authentification). Une telle évaluation, qui serait conforme au principe de neutralité technologique et à l'approche des « conditions minimales », renforcerait le degré de certitude pour les acteurs du marché qui introduisent cette méthode d'identification ou ce type de service de gestion de l'identité sur un marché, et assurerait la transparence quant au niveau de protection offert aux utilisateurs de ces services.

III. Présomption de fiabilité

10. Avec l'approche suivie actuellement en ce qui concerne la fiabilité de la méthode, la présomption vaut uniquement pour les méthodes désignées (art. 11), et non pour les méthodes évaluées *ex post* (art. 10). Cette approche peut provoquer des incertitudes sur le marché et empêcher les acteurs du marché d'utiliser des méthodes qui n'ont pas été désignées par les autorités compétentes. Il est à noter qu'aucune exigence de ce type n'existe dans le domaine du commerce électronique en ce qui concerne la preuve d'identité « traditionnelle » utilisée pour la conclusion de contrats sur papier.

11. Afin d'éviter de telles incertitudes et de promouvoir l'ouverture et la compétitivité sur le marché de la gestion de l'identité, l'ICLRC aimerait proposer de revoir l'approche actuellement suivie à l'article 10 de la Loi type et de fonder celui-ci sur la présomption générale de fiabilité pour toutes les méthodes qui sont effectivement utilisées pour l'identification. Cette présomption pourrait être renversée en cas de violation des principes énoncés par la Loi type. Ces principes comprennent la légalité (la méthode n'est pas interdite par la loi applicable), la transparence (le niveau de protection, le processus et les résultats de l'identification sont visibles pour les utilisateurs), la responsabilité (le prestataire de services doit démontrer la fonctionnalité et la durabilité de son service) et la sécurité (le prestataire de services a mis en place un ensemble de mesures de sécurité de l'information qui empêchent tout accès non autorisé au système de gestion de l'identité).

12. En conséquence, l'ICLRC propose de modifier l'article 10 comme suit :

« *Article 10. Présomption de fiabilité des services de gestion de l'identité*

1. Aux fins de l'article 9, la méthode utilisée par le prestataire de services de gestion de l'identité est présumée fiable, à moins qu'[une personne, un organe ou une autorité, de droit public ou privé, indiqué(e) par l'État adoptant comme compétent(e) en la matière] ne prouve qu'elle n'est pas fiable en raison de son caractère illégal, de son manque de transparence ou de l'incapacité du prestataire de services de gestion de l'identité à démontrer la fonctionnalité, la durabilité et la sécurité de la méthode.

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

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

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

IV. Guide pour l'incorporation

13. La Loi type n'est pas accompagnée d'un guide sur la réforme législative qui serait nécessaire pour la mettre en œuvre. Le processus de mise en œuvre, en particulier au niveau international (ou régional), peut s'avérer difficile, alors qu'il faudrait tendre à l'uniformité non seulement dans les textes juridiques mais aussi dans leur application. Nous pensons qu'il serait important de poursuivre le travail des experts dans cette direction et d'assortir la Loi type d'un guide de mise en œuvre.

D. Ordre des avocats de Paris

[Original : français]
[25 mai 2022]

1. Tout d'abord, il faut se féliciter de cette initiative visant à renforcer la sécurité des transactions internationales conclues au moyen de signatures électroniques qui vont grâce à ce projet de texte pouvoir être mutuellement reconnues car reposant sur une base légale. On sait combien en Europe, l'adoption d'une telle réglementation fut difficile entre le premier paquet numérique des années 1999-2000 jusqu'à l'adoption en 2014 du règlement eIDAS (nº 910/2014), entré en vigueur seulement en 2016. Le projet est ambitieux mais plus que nécessaire au niveau international.

2. Soucieux des libertés individuelles, le Barreau de Paris ne peut que se réjouir que dans les articles 2 et 3 du projet de loi, il soit rappelé que le mécanisme de reconnaissance mutuelle d'identité numérique ne peut se faire au détriment de la réglementation sur la protection des données à caractère personnel ni sans le consentement de la personne physique quant à l'usage d'un mécanisme gestionnaire d'identité.

3. On sait que, chaque année, dans un nombre de plus en plus important de juridictions, l'administration de la preuve dans des procédures judiciaires implique l'usage d'outils de type « eDiscovery ». La qualité d'avocat permet, dans les échanges avec ses clients, de bénéficier du secret professionnel (ou « legal privilege ») et ainsi les écarter des débats. Il est suggéré dans le projet de loi que le système gestionnaire d'identité puisse intégrer la qualité d'avocat pour faciliter et renforcer numériquement la protection par le secret professionnel.

4. Enfin, la technologie couverte par le projet de loi repose pour l'essentiel sur la signature électronique classique avec un tiers de confiance. De futurs travaux pourront aussi s'intéresser à la reconnaissance mutuelle de la blockchain (incontournable dans les smart contracts), laquelle fonctionne sur la base d'une communauté en mode horizontal, sans tiers de confiance à proprement parler.

E. Banque asiatique de développement

[Original : anglais]
[26 mai 2022]

1. La Banque asiatique de développement (BAsD) remercie sincèrement le Secrétariat et le Groupe de travail IV de la CNUDCI de l'avoir invitée à examiner et à commenter le projet de loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance, ainsi que la note explicative (A/CN.9/1112).

2. La BAsD n'a pas de commentaires supplémentaires au sujet du projet de loi type.

3. En ce qui concerne la note explicative (annexe II), la BAsD a noté les points suivants, qu'elle soumet à l'examen du Secrétariat, du Groupe de travail IV et de la Commission :

i) Le paragraphe 48 a) traite des attributs qui constituent l'« identité fondamentale » d'une personne physique et d'une personne morale. Afin de mieux

faire connaître les attributs d'une organisation internationale aux prestataires de services de gestion de l'identité ou de services de confiance et aux États adoptants, il pourrait être utile d'inclure ces attributs (c'est-à-dire un traité international pour une organisation internationale) au paragraphe 48 a) ;

ii) Les obligations de la partie utilisatrice sont généralement mentionnées dans les accords contractuels conclus avec le fournisseur de services de gestion de l'identité ou de services de confiance et/ou peuvent être établies par d'autres lois/réglementations, et elles ne sont pas couvertes par le projet de loi type ni la note explicative. Il pourrait être utile d'inclure dans la note explicative un commentaire portant sur les obligations générales de la partie utilisatrice (à savoir la protection de la clef privée, la vérification du statut des certificats, etc.).

4. La BAsD félicite le Secrétariat et le Groupe de travail IV de la CNUDCI des efforts fournis dans le cadre de l'élaboration du projet de loi type et de la note explicative, qui traitent des éléments clefs (utilisation de services de gestion de l'identité et de services de confiance) nécessaires pour faciliter et promouvoir les activités de commerce électronique.