

**Assemblée générale**

Distr. générale
14 juin 2022
Français
Original : anglais/espagnol

**Commission des Nations Unies
pour le droit commercial international**
Cinquante-cinquième session
New York, 27 juin-15 juillet 2022

**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

	<i>Page</i>
II. Compilation des commentaires	2
F. Bankers Association for Finance and Trade	2
G. État plurinational de Bolivie	4
H. République islamique d'Iran	5
I. Bulgarie	10
J. Singapour	11



II. Compilation des commentaires

F. Bankers Association for Finance and Trade

[Original : anglais]

[27 mai 2022]

1. La Bankers Association for Finance and Trade (BAFT) apprécie l'occasion qui lui est donnée de commenter le « Projet de loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance ».
2. La BAFT est une association internationale du secteur des services financiers regroupant diverses institutions financières et entreprises d'ingénierie financière (FinTech). Formant un forum mondial d'analyse, de discussion et de défense des intérêts des services financiers internationaux, ses quelque 300 membres jouent un rôle de premier plan dans la recherche de consensus pour préserver la sécurité et l'efficacité du système financier international. Les institutions membres de la BAFT considèrent la numérisation du financement du commerce international comme une priorité essentielle du secteur, et la gestion de l'identité est un élément essentiel pour que la numérisation progresse.
3. L'impératif de mise en place de la gestion de l'identité touche de nombreuses facettes des opérations bancaires internationales, notamment le financement du commerce et celui de la chaîne d'approvisionnement, les paiements, et les domaines de conformité tels que la connaissance de l'identité de son client (de l'anglais « Know Your Customer » – KYC) et la lutte contre le blanchiment d'argent. À ce titre, la BAFT soutient pleinement les efforts de la CNUDCI dans la formulation du projet de loi type.
4. Les transactions bancaires mondiales comportent plusieurs lignes d'action dont l'objectif est de doter le secteur d'un écosystème entièrement numérique. La numérisation est très prometteuse ; cependant, on ne peut pas dire que le taux de réalisation et d'adoption ait été satisfaisant à ce jour. Il est clair qu'on n'aura pas d'un seul coup un « big bang » de la numérisation, mais qu'il faudra progresser par le biais d'initiatives complémentaires les unes des autres permettant des avancées durables.
5. Le marché a besoin de règles claires pour pouvoir faire progresser la numérisation dans les opérations quotidiennes. À cet égard, l'initiative sur les normes numériques (Digital Standards Initiative ou DSI) a été lancée par la Chambre de commerce internationale, la Banque asiatique de développement et le Gouvernement de Singapour pour traiter des questions liées aux normes et à l'interopérabilité des plateformes et des relations avec les entreprises d'ingénierie financière¹. En termes de soutien juridique, une feuille de route a été établie afin d'encourager les gouvernements à adopter des textes législatifs spécifiques pour le commerce numérique, comme le préconise la Loi type de la CNUDCI sur les documents transférables électroniques². La BAFT participe aux efforts visant à favoriser l'adoption de cette Loi type dans le monde entier. Outre les efforts portant sur le cadre juridique, le secteur travaille à l'élaboration de normes d'interopérabilité. En août 2020, la BAFT a publié un document sur les meilleures pratiques sectorielles en ce qui concerne l'utilisation de registres distribués pour les engagements de paiement (« Distributed Ledger Payment Commitment – Industry Best Practices ») en vue d'élaborer des orientations sectorielles sur les engagements de paiement interopérables exécutés dans un registre distribué³.

¹ Initiative sur les normes numériques de la Chambre de commerce internationale, mars 2020.

² Loi type de la CNUDCI sur les documents transférables électroniques, juillet 2017.

³ BAFT : Distributed Ledger Payment Commitment, mai 2020.

6. Le projet de loi type fournit le cadre général de la gestion de l'identité et des services de confiance en évitant de suivre la moindre approche prescriptive. Il déclare sans ambiguïté que « tout comme certains textes antérieurs de la CNUDCI, le projet de loi type se fonde sur les principes d'autonomie des parties, de neutralité technologique, d'équivalence fonctionnelle et de non-discrimination à l'égard de l'utilisation des moyens électroniques, sous réserve de certaines modifications. Le principe de l'autonomie des parties permet aux parties à un contrat de choisir les règles applicables, dans les limites du droit impératif. Il reconnaît que ces parties sont peut-être les mieux placées pour déterminer les règles qui sont les mieux adaptées à une transaction donnée. »

7. Le projet de loi type prévoit que les services de gestion de l'identité seront soumis à certaines exigences en matière de fiabilité, comme l'exige l'article 10, mais ne précise pas comment le cadre relatif aux niveaux de garantie devrait être élaboré. Il confirme que la dimension internationale est essentielle pour l'utilisation de services de confiance et de gestion de l'identité et, plus généralement, de services électroniques. Il confirme néanmoins également que deux types d'obstacles existent, à savoir i) les incompatibilités techniques entraînant un manque d'interopérabilité, et ii) les obstacles juridiques à la reconnaissance internationale.

8. Afin de fournir une orientation pour surmonter ces deux obstacles en particulier, la BAFT appuierait une référence directe dans le projet de loi type aux efforts et progrès importants accomplis par la Global Legal Identifier Foundation (GLEIF)⁴ dans la mise en œuvre de l'identifiant d'entité juridique (LEI). Approuvé par les autorités réglementaires, le système mondial du LEI fournit un mécanisme d'identification électronique des entités juridiques reconnu et fiable sur la planète entière. L'identifiant d'entité juridique est une norme mondiale (ISO 17442) qui relie des informations de référence clés permettant une identification claire et unique des entités juridiques. Sur recommandation du G20 en 2011, le Conseil de stabilité financière a créé la GLEIF, fondation suisse à but non lucratif dont les activités sont supervisées au sein du Comité de contrôle réglementaire par 65 agents de réglementation et 19 observateurs issus d'une cinquantaine de pays.

9. La base de données associées au LEI accessible au public peut être considérée comme un répertoire mondial améliorant considérablement la transparence sur le marché mondial. Le LEI constitue un véritable bien public qui devrait être mis à profit pour assurer la compatibilité technique aux niveaux national et international.

10. Le projet de loi type vise à harmoniser les règles par la voie législative. Cette approche débouchera sur une pléthore de normes techniques nationales qui ne permettront aucune interopérabilité et épuiseront les ressources consacrées à l'analyse et à la compréhension de données hétérogènes. L'utilisation d'une multitude d'identifiants et de normes techniques nationales sous-jacentes peut entraver la capacité d'identifier chaque partie aux transactions électroniques d'une manière fiable, homogène et comparable. Par conséquent, même si la CNUDCI souhaite éviter toute préférence et conserver sa neutralité en matière de technologie, elle devrait envisager d'inclure le LEI dans le projet de texte, où il apparaîtrait comme l'identifiant de base facilitant l'identification et la vérification internationales des entités juridiques. Le système mondial du LEI n'est pas un choix technologique. Il s'agit d'un bien public envisagé par le Groupe des Vingt (G20) et réalisé par le Conseil de stabilité financière (CSF).

11. Les données de référence du LEI comprenant déjà le numéro d'enregistrement local de l'entité, des informations sur l'adresse, l'horodatage de la dernière mise à jour des données et des informations sur les champs de données qui ont été mis à jour,

⁴ GLEIF (www.gleif.org).

le système est à même de promouvoir l'uniformité des données relatives aux entités à l'échelle mondiale.

12. Le projet de loi type reconnaît déjà que des règles uniformes peuvent : renforcer l'efficacité en favorisant l'acceptation, par tous les systèmes, du résultat de l'application de la gestion de l'identité et des services de confiance ; réduire les coûts de transaction en facilitant le respect des exigences réglementaires ; renforcer la prévisibilité et la sécurité juridiques des opérations électroniques sur la base d'un traitement commun des questions, notamment par des mécanismes de reconnaissance internationale ; et contribuer à réduire la fracture numérique grâce à une plus grande disponibilité de solutions communes.

13. Dans le cas où des approches divergentes se feraient jour, l'article 27 suggère que la coopération pourrait contribuer à la définition commune de normes techniques, y compris des niveaux de garantie et des niveaux de fiabilité. Toutefois, l'existence d'intérêts nationaux concurrents pourrait provoquer des goulets d'étranglement ou, au mieux, des retards dans la conclusion d'un accord sur les normes techniques requises et les autres cadres de qualité des données sous-jacents. Le rôle moteur de la CNUDCI dans l'établissement du LEI comme identifiant de référence pour l'identification des entités juridiques peut accélérer le processus de mise en œuvre de l'identification électronique transfrontière et tirer parti d'un système établi par des agents de réglementation pour remédier aux lacunes des systèmes d'identification nationaux/régionaux/privés. Éprouvé et fonctionnel, le système du LEI offre une solution interopérable et techniquement impartiale.

14. La transformation numérique dans le domaine des transactions bancaires mondiales est susceptible de réduire les coûts, d'améliorer l'efficacité, d'assurer de meilleurs contrôles réglementaires avec moins de risques et des opportunités de collaboration pour les parties prenantes de l'économie mondiale. La création et l'adaptation de la gestion de l'identité est une première étape fondamentale du processus de numérisation. Le LEI étant la seule norme mondiale pour identifier les entités juridiques, la BAFT approuve son inclusion dans le texte du projet de loi type.

G. État plurinational de Bolivie

[Original : espagnol]

[27 mai 2022]

On trouvera ci-après, pour examen, les commentaires et observations formulés par l'Autorité de réglementation des télécommunications et des transports de l'État plurinational de Bolivie sur le projet de loi susmentionné.

Article 6 : Obligations incombant aux prestataires de services de gestion de l'identité

Commentaire/observation :

Il est recommandé de considérer comme une obligation le fait de garantir la disponibilité en ligne et le bon fonctionnement d'un système de validation d'identité ou de signature électronique, qui permet de vérifier l'identité du signataire et la validité de la chaîne de confiance de l'organe de certification compétent dans son pays d'origine.

Article 16. Signatures électroniques

Commentaire/observation :

Il est recommandé d'envisager un mécanisme permettant de détecter toute modification du message de données et de garantir l'authenticité, l'intégrité et la non-répudiation de ce dernier.

Article 17. Cachets électroniques

Commentaire/observation :

L'authenticité, l'intégrité et la non-répudiation du message de données doivent être garanties, ainsi que sa validité juridique et probatoire conformément à la réglementation du pays où réside le prestataire de services de gestion de l'identité.

H. République islamique d'Iran

[Original : anglais]
[30 mai 2022]

1. Champ d'application

Utilisation et reconnaissance internationale de la gestion de l'identité et des services de confiance

1. **Difficulté** : Conformément au mandat de la CNUDCI d'harmoniser et de moderniser le droit du commerce international et compte tenu que le Groupe de travail IV s'est vu confier la tâche d'éliminer les obstacles au commerce électronique international, la République islamique d'Iran est d'avis que le champ d'application de la loi type est extrêmement large et doit être limité uniquement au domaine international et aux circonstances impliquant un élément de fait étranger. En d'autres termes, selon notre compréhension, dans les cas d'utilisation et de reconnaissance nationales de la gestion de l'identité et des services de confiance, lorsqu'aucun élément étranger n'entre en jeu et que tous les participants intervenant dans le cycle de vie de la gestion de l'identité et des services de confiance se trouvent dans le même pays, le droit interne des États devrait régir la situation et gouverner les affaires nationales.

Solution proposée

2. Il est recommandé de limiter le champ d'application de la loi type à l'utilisation et à la reconnaissance internationale de la gestion de l'identité et des services de confiance et de préciser que l'instrument ne vise ni à s'immiscer dans les infrastructures nationales liées à la gestion de l'identité et aux services de confiance établies dans les États membres ni à prévaloir sur le droit national régissant les affaires internes de ces États. En même temps, nous notons qu'il peut tout de même y avoir une marge de manœuvre pour que les États qui adopteraient la loi type en étendent l'applicabilité à leurs affaires nationales, uniquement s'ils le souhaitent.

Services touchant au commerce

3. **Difficulté** : En ce qui concerne le terme « services touchant au commerce » (qui figure à l'article 2), il convient de noter que, malgré les indications fournies au paragraphe 95 du document explicatif, nous sommes d'avis que ce terme reste vague, qu'il n'est pas facilement identifiable par les utilisateurs et qu'il pourrait être interprété plus largement que ce qui était envisagé dans la loi type ou qu'il pourrait couvrir, de manière inappropriée, tous les systèmes actifs d'un pays dans le domaine de la gestion de l'identité et des services de confiance qui ne sont pas nécessairement liés au commerce.

Solution proposée

4. Il est recommandé que la loi type se concentre sur les situations rencontrées dans le cadre des activités commerciales. Néanmoins, la note explicative pourrait préciser que « rien dans la loi type ne devrait empêcher un État adoptant d'étendre le champ d'application de la loi type pour couvrir l'utilisation et la reconnaissance

internationale de la gestion de l'identité et des services de confiance dans le contexte des services liés au commerce ».

2. Protection de la souveraineté et de l'ordre public des États

5. **Difficulté** : Notre délégation s'inquiète des répercussions implicites de cette loi type sur la question de la souveraineté des États dont les ressortissants ou les entreprises sont des utilisateurs de services de confiance et de gestion de l'identité internationaux. Pour comprendre cette préoccupation, il peut être suffisant d'examiner la réalité du marché du point de vue des pays en développement et de considérer comment tous les secteurs pertinents de ces pays ont été dominés par des entreprises numériques mondiales situées dans quelques pays numériques de premier plan qui fournissent leurs services à des abonnés du monde entier. En outre, l'intervention des prestataires de services numériques dans le domaine des services de gestion de l'identité, alors qu'ils n'avaient pas été préalablement chargés de ces tâches par les gouvernements concernés, et en particulier lorsque les attributs qu'ils collectent sont étroitement liés à l'identité fondamentale des personnes, pourrait non seulement être irrationnelle et conduire à des résultats non fiables, mais également, en raison de la compétence exclusive des États concernant la gestion de l'identité de leurs citoyens tout au long du cycle de vie, entraîner une ingérence dans leurs fonctions souveraines. Dans les pays en développement, ce phénomène risque aussi d'entraîner des pertes en matière de données, de technologie et de souveraineté numérique, ainsi qu'en ce qui concerne la protection que les lois impératives offrent aux citoyens. Les conséquences délétères de telles pratiques deviennent plus évidentes si l'on considère la position de subordination des pays en développement et les fortes pressions qu'ils subissent dans les forums commerciaux mondiaux pour adopter le modèle d'économie numérique général et dominant de la poignée de pays qui hébergent la plupart des géants du numérique. C'est pourquoi la République islamique d'Iran est fermement convaincue que, pour que les pays en développement bénéficient des travaux des organisations internationales, ils doivent d'abord être en mesure de sauvegarder leur souveraineté et leurs politiques publiques. Dans ce contexte, nous sommes d'avis qu'il manque, dans les dispositions de la loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance, une référence explicite à la protection de la souveraineté des États, à l'égalité et à la non-intervention dans les affaires qui relèvent exclusivement de leur compétence nationale.

6. La préservation de l'ordre public des États adoptants est tout aussi importante. Aujourd'hui, les flux de données transfrontaliers et l'accès des prestataires de services étrangers aux données des ressortissants et des entreprises d'autres pays sont devenus une préoccupation majeure de politique publique pour de nombreux pays en développement. Contrairement aux textes antérieurs de la CNUDCI (par exemple, les articles 6, 7, 8, 11, 12, 15 et 17 de la Loi type sur le commerce électronique), le projet de loi type ne prévoit aucune procédure permettant de limiter le champ d'application de l'instrument ou les effets de l'un ou l'autre de ses articles si cela s'avère nécessaire, notamment pour des motifs liés à l'ordre public des États adoptants. Selon nous, dans la mesure où la mise en œuvre de cette loi type pourrait soulever diverses questions liées à l'ordre public qui doivent être laissées à la discrétion de chaque État, il conviendrait d'autoriser un certain degré de souplesse, de façon à permettre aux tribunaux de l'État adoptant ou aux autorités responsables de l'application de la loi type de refuser ou d'annuler les effets juridiques résultant de l'utilisation de services de confiance ou de gestion de l'identité étrangers sur la fondement de raisons impératives, y compris liées à l'ordre public.

Solution proposée

7. Il faudrait qu'il soit explicitement précisé dans l'instrument que l'application de la loi type doit se faire dans le respect des principes de souveraineté des États, d'égalité et de non-ingérence dans leurs affaires intérieures. En outre, l'instrument ne doit pas autoriser les prestataires étrangers de services de confiance et de gestion de l'identité à exercer des fonctions qui sont de nature souveraine et relèvent exclusivement de la compétence des États nationaux conformément à leur droit interne. De même, on s'attend à ce que ce fait soit énoncé en tant que principe général et concept clef dans la section F de la note explicative.

8. Afin de répondre aux préoccupations liées à l'ordre public et conformément à la position traditionnellement adoptée par la CNUDCI dans ses textes antérieurs, il convient d'envisager trois options :

Premièrement : inclure dans la loi type des dispositions qui permettraient aux pays qui l'adoptent d'exclure l'application ou les effets de certains de ses articles dans des situations qui seraient contraires à leur ordre public (il existe plusieurs précédents à cet effet dans des textes antérieurs de la CNUDCI).

Deuxièmement : formuler certains articles de manière souple, pour atténuer toute application absolue. On pourrait par exemple ajouter un segment de phrase à l'alinéa 3 des articles 10 et 22 afin de préciser que : « pour déterminer la fiabilité de la méthode, sous réserve que l'organe juridictionnel ne le juge pas nécessaire, il n'est pas tenu compte... ». Dans le même ordre d'idées, l'alinéa 4 des articles 11 et 23 pourrait être modifié comme suit : « pour désigner un service de gestion de l'identité/de confiance, sous réserve que [la personne, l'organe ou l'autorité, de droit public ou privé, indiqué(e) par l'État adoptant comme compétent(e) en la matière] ne le juge pas nécessaire, il n'est pas tenu compte... ». En outre, le fait de remplacer l'indicatif par des formules au conditionnel (en anglais, remplacement de l'auxiliaire « shall » par « may ») dans les articles 25 et 26 introduirait une certaine souplesse dans la formulation de ces articles, pour répondre aux préoccupations liées à l'ordre public. Cette modification semble aussi raisonnable compte tenu de l'absence de clarté en ce qui concerne les « normes internationalement reconnues » évoquées aux articles 25-2 et 26-2.

Troisièmement : s'il est impossible d'appliquer l'une ou l'autre des deux options susmentionnées, il serait utile de prévoir une règle générique dans la loi type qui fasse référence à l'exception d'ordre public et laisse à chaque pays adoptant le soin de préciser les détails dans sa propre législation.

3. Lois de police

9. **Difficulté** : De nos jours, les fournisseurs proposent leurs services de confiance et de gestion de l'identité aux ressortissants et aux entreprises de pays étrangers. Bien que ce phénomène soit inévitable et constitue un élément indispensable du commerce électronique mondial, des mesures de précaution devraient être prises pour garantir que les prestataires de services respectent les lois de police auxquelles il ne saurait être dérogé.

10. La République islamique d'Iran est consciente du fait que l'instrument est sans incidence sur l'application de toute loi impérative qui pourrait survenir dans le cadre de ses dispositions et est également consciente du fait que la loi type n'a pas pour objet d'empiéter sur les règles du droit international privé. Néanmoins, nous sommes fermement d'avis qu'il faut inclure dans cet instrument une disposition spécifique qui donnerait effet au droit impératif du pays où la gestion de l'identité ou le service de confiance est fourni ou vers lequel il est dirigé. Cette démarche tient à plusieurs raisons. La première raison concerne l'accès des prestataires de services aux données des citoyens, des entreprises et des organisations du pays considéré. Sachant que les données constituent un bien de valeur qui, dans le cas de services extraterritoriaux,

peut se retrouver entre les mains de prestataires de services étrangers, nous estimons que les propriétaires de données seraient dans la meilleure position si les données étaient placées sous le régime de la protection et du droit impératif du pays où le service est fourni ou vers lequel il est destiné. La deuxième raison serait l'absence de règles claires, en droit international privé, qui spécifieraient la loi et les lois de police applicables pour la protection des utilisateurs de services de commerce électronique. Bien qu'il semble y avoir un consensus général concernant la législation applicable à la protection des consommateurs dans les contrats de consommation, une ambiguïté pourrait surgir pour ce qui est de la protection des abonnés dans les contrats avec des prestataires de services numériques, contrats qui pourraient ne pas relever de la loi sur la protection des consommateurs. La troisième raison est liée au déséquilibre contractuel entre les abonnés et les fournisseurs de services. Les abonnés sont souvent en position asymétrique lorsqu'il s'agit de conclure un contrat dans un environnement numérique et de consentir aux règles, politiques et pratiques de fonctionnement qui le régissent. Il nous apparaît que les dispositions figurant dans les contrats entre abonnés et prestataires de services sont rarement négociées et qu'elles contiennent généralement des clauses de droit applicable ou d'élection de for qui sont essentiellement favorables aux fournisseurs de services et au détriment des abonnés. L'absence de toute référence à la loi du pays où le service est fourni ou vers lequel il est dirigé en vertu de la loi type, ou l'absence d'effet de cette loi, priverait les abonnés de la protection nécessaire à laquelle ils ont droit.

Solution proposée

11. La recherche de garanties et de solutions adéquates pour répondre aux préoccupations susmentionnées nécessite une collaboration internationale et un dialogue politique accru, avec la pleine participation des pays en développement, qui sont la plupart du temps les destinataires des services transfrontaliers. On trouvera néanmoins ci-dessous quelques-unes de nos suggestions :

- « La conformité des règles, politiques et pratiques de fonctionnement du prestataire de services de gestion de l'identité ou de services de confiance avec le droit impératif du lieu où le service est fourni ou vers lequel il est dirigé » devrait être une obligation faite à ces prestataires conformément aux articles 6 et 14 et également un élément à prendre en compte à la fois pour déterminer la fiabilité de la méthode (*ex post*) aux articles 10-2 et 22-2, et pour la désignation des services fiables (*ex ante*) aux articles 11-2 a) et 23-2 a), et comme norme à appliquer pour accorder un effet juridique dans le cadre de l'application transfrontalière des services aux articles 25 et 26.
- Dans le but de donner effet au droit impératif du lieu où le service est fourni ou vers lequel il est dirigé, il serait nécessaire d'énoncer, aux articles 6 et 14, des obligations supplémentaires à imposer aux prestataires de services, ce qui pourrait être expliqué plus avant aux paragraphes 113 et 175 de la note explicative. Par exemple, la coopération des prestataires de services avec les forces de l'ordre du pays où le service est fourni ou vers lequel il est dirigé (notamment en matière de protection des données ou de situations qui pourraient entraîner une responsabilité délictuelle ou criminelle, y compris s'agissant de prévention et de détection des délits, d'enquêtes et de poursuites relatives aux infractions) et, à cette fin, l'établissement d'une présence locale ou la désignation d'un représentant dans le pays concerné, la modification des conditions de services et des politiques des fournisseurs de services conformément au droit impératif du lieu où le service est fourni ou vers lequel il est dirigé, etc. Nous sommes d'avis que la violation de ces obligations devrait fonder la responsabilité de la gestion d'identité ou des services de confiance en vertu des articles 12 et 24.

- Le respect des obligations susmentionnées pourrait faciliter la réalisation de l'objectif de reconnaissance mutuelle visé aux articles 25 et 26. Par conséquent, il serait hautement souhaitable que les pays adoptants fassent connaître leurs exigences légales impératives par le biais de l'échange d'informations prévu à l'article 27. Ces informations pourraient permettre aux prestataires de services étrangers qui souhaitent offrir leurs services de manière extraterritoriale de modifier à l'avance leurs conditions de services et leurs politiques en fonction des réglementations pertinentes. Les détails de cette forme de coopération pourraient être précisés au paragraphe 234 de la note explicative.

4. Caractère volontaire de l'utilisation des services de gestion de l'identité et des services de confiance

12. **Difficulté** : La République islamique d'Iran s'inquiète de la possibilité de déduire le consentement d'une personne d'après son comportement, évoquée à l'article 3-2 du projet de loi type. Bien qu'il s'agisse d'une règle établie conformément à des textes antérieurs de la CNUDCI, nous sommes d'avis qu'elle serait au détriment des personnes peu au courant de la technologie, car celles-ci ne seraient pas nécessairement conscientes du fait qu'en s'inscrivant à un service ou en utilisant un logiciel de commerce électronique spécifique, elles autorisent l'utilisation d'un système de gestion de l'identité ou d'un service de confiance supporté par ce logiciel. En outre, cette situation pourrait avoir des effets encore plus négatifs si l'on considère la position « à prendre ou à laisser » devant laquelle se retrouvent les abonnés au moment de conclure des contrats numériques et parfois leur acceptation aveugle de clauses qui ne leur sont pas du tout favorables et qui indiquent des situations dans lesquelles ils peuvent être présumés avoir exprimé leur consentement aux conditions contractuelles. Nous souhaitons attirer l'attention de la Commission sur le fait que, si les consommateurs européens sont protégés contre les clauses standard abusives par la directive 93/13/CEE du Conseil des Communautés européennes concernant les clauses abusives dans les contrats conclus avec les consommateurs, il nous semble qu'il n'existe que peu de lois en la matière dans les pays non européens.

Solution proposée

13. Nous souhaitons suggérer qu'il devrait y avoir suffisamment de souplesse quant à la possibilité de déduire le consentement d'une personne à utiliser un service de gestion de l'identité ou un service de confiance d'après son comportement et souligner que ce consentement implicite devrait être déterminé de manière plus claire et plus prévisible. Il serait donc utile que les États membres examinent ce point plus en détail et trouvent des solutions pour mieux répondre à cette exigence en ce qui concerne les contrats dans l'environnement numérique. À notre avis, il serait utile que le consentement implicite des parties prenne la forme d'une présomption qui pourrait être réfutée à un stade ultérieur.

5. Archivage électronique

14. **Difficulté** : Nous sommes conscients du fait que la loi type n'affecte pas les lois applicables à la protection et à la confidentialité des données. Néanmoins, compte tenu de la pertinence de ce domaine du droit dans le cas de l'archivage électronique, nous pensons qu'il est nécessaire de souligner, à l'article 19, que, dans le cadre de l'archivage électronique, il faut tenir compte des lois impératives sur la protection et la confidentialité des données. En ce qui concerne le droit impératif pertinent en l'espèce, il convient de prêter attention aux fonctions des prestataires de services internationaux de confiance et de gestion de l'identité et à leur dépendance étroite à l'égard des données des citoyens, des entreprises et des organisations d'autres pays. Compte tenu du fait que le transfert transfrontalier de ces données constitue une préoccupation majeure de politique publique et qu'il peut priver les abonnés de

régimes de protection des données auxquels ils ont droit, nous sommes d'avis que la loi type devrait pouvoir donner un effet juridique à la législation sur la protection des données du pays où le service est fourni ou vers lequel il est dirigé et où les abonnés reçoivent ce service. La République islamique d'Iran souhaite attirer l'attention de la Commission sur le fait que, bien que les personnes visées en Europe soient protégées par le vaste champ d'application territorial du Règlement général européen sur la protection des données (RGPD), il n'existe pas toujours de réglementation aussi étendue ailleurs dans le monde, en particulier dans les pays du tiers monde, qui serait obligatoire pour les prestataires de services étrangers et pourrait les contraindre à respecter la législation sur la protection des données du lieu où leur service est fourni ou vers lequel il est dirigé.

Solution proposée

15. Réaffirmer explicitement à l'article 19 que : « la conservation des documents, documents d'activité ou informations visés à l'article 19 devrait faire l'objet de garanties appropriées au regard de la législation sur la protection et la confidentialité des données ». Afin de répondre à la deuxième préoccupation citée ci-dessus, nous suggérons d'insérer un paragraphe selon lequel l'archivage électronique ne priverait pas les personnes abonnées à des services internationaux de gestion de l'identité ou de confiance du régime de protection des données auquel elles ont droit en vertu du lieu où le service est fourni ou vers lequel il est dirigé.

6. Points manquants

16. Afin d'élaborer un texte plus complet à bien des égards, il convient d'envisager d'inclure dans le texte de la loi type certains éléments qui en sont absents. Il faudrait par exemple définir les termes « niveau de garantie », « niveau de fiabilité » et « partie utilisatrice » à l'article 1, décrire les droits et obligations des parties utilisatrices, et adopter une approche explicite et plus complète en ce qui concerne les droits des abonnés.

I. Bulgarie

[Original : anglais]

[8 juin 2022]

1. La législation bulgare nationale et celle de l'Union européenne sur l'identification électronique et les services de confiance (certification) sont fondées sur le Règlement de l'Union européenne n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur abrogeant la directive 1999/93/CE. Les pouvoirs de la Commission de réglementation sont définis à l'article 32 de la loi sur les documents électroniques et les services de certification électronique, qui prévoit que la Commission est l'autorité de surveillance nationale dans le domaine des services de certification électronique chargée de mettre en œuvre les dispositions dudit Règlement de l'Union européenne.

2. Le Règlement de l'Union européenne n° 910/2014 établit un cadre juridique commun pour l'utilisation des services de certification dans les États membres de l'Union, et la reconnaissance des services de certification provenant de pays tiers est réglementée à son article 14. Ces services peuvent être reconnus en vertu d'un accord conclu entre l'Union et le pays tiers concerné ou une organisation internationale conformément à l'article 218 du Traité sur le fonctionnement de l'Union européenne.

3. Compte tenu de ce qui précède, la Commission de réglementation bulgare estime que le projet de loi type élaboré par la CNUDCI répond aux principaux objectifs et principes énoncés dans le Règlement de l'Union européenne n° 910/2014.

J. Singapour

[Original : anglais]
[13 juin 2022]

1. Singapour remercie le Groupe de travail IV des travaux qu'il a réalisés dans le cadre de l'élaboration du projet de loi type sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance.
2. Nous souhaitons attirer l'attention de la Commission sur trois aspects du projet de loi type (tel qu'il figure dans le document A/CN.9/1112) qui méritent d'être examinés attentivement et qui sont résumés ci-après.

a) Premièrement, il est nécessaire :

- i) D'exprimer plus clairement la relation entre l'article 9 et l'article 10-1 (pour les services de gestion de l'identité) en insérant les mots « conforme au paragraphe 1 de l'article 10 » dans l'article 9, de sorte que la fin de celui-ci se lise comme suit : « *si une méthode conforme au paragraphe 1 de l'article 10 est employée pour l'identification électronique de cette personne à cette fin* » ; et
- ii) D'exprimer plus clairement la relation entre chacun des articles 16 à 21 et l'article 22-1 (pour les services de confiance) en insérant les mots « conforme au paragraphe 1 de l'article 22 » dans chacun d'eux, de sorte qu'ils contiennent tous le membre de phrase « *si une méthode conforme au paragraphe 1 de l'article 22 est utilisée pour ...* ».

(Pour plus de détails, voir les paragraphes 3 et 4 ci-dessous)

b) Le deuxième aspect a trait au maintien des « clauses de sauvegarde » contenues à l'article 10-1 b) (en ce qui concerne la fiabilité des services de gestion de l'identité) et à l'article 22-1 b) (en ce qui concerne la fiabilité des services de confiance). Ces clauses de sauvegarde, qui font pendant aux clauses de l'article 9-3 b) ii) de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux de 2007 (CCE)⁵ et de l'article 12 b) de la Loi type de la CNUDCI sur les documents transférables électroniques de 2017, visent à éviter les contestations juridiques infondées (arguant que la méthode utilisée n'est pas suffisamment fiable en *théorie*), en prévoyant qu'une méthode satisfait aux conditions énoncées à l'article 9 ou aux articles 16 à 21 si elle a démontré dans les faits qu'elle a rempli la fonction décrite à l'article 9 ou les fonctions respectives visées aux articles 16 à 21 (c'est-à-dire une fiabilité *de fait*), soit par elle-même, soit avec d'autres preuves. À notre avis, les articles 10-1 b) et 22-1 b) constituent des garanties essentielles contre de telles contestations infondées et devraient être conservés sous leur forme actuelle. Par ailleurs, la suppression (ou le déplacement) de ces articles ne permettrait plus d'assurer l'alignement entre le projet de loi type et la CCE ou la Loi type sur les documents transférables électroniques. Dans ce cas, la Commission devrait a) se prononcer sur les mesures à prendre par les États qui sont parties à la CCE ou ont adopté la Loi type sur les documents transférables électroniques pour remédier à cette incohérence ; et b) décider si elle continuerait de recommander la CCE et la Loi type sur les documents transférables électroniques (malgré l'incohérence de leurs dispositions) aux États qui envisagent de devenir partie à la première ou de mettre en œuvre la seconde. Nous proposons de modifier les paragraphes 142 et 143 du projet de note explicative afin de décrire plus précisément l'objet et les effets du projet d'article 10-1 b).

(Pour plus de détails, voir les paragraphes 5 à 16 ci-dessous.)

⁵ De la même manière que l'article 10-1 définit les critères de fiabilité applicables à une méthode utilisée à des fins d'identification électronique, l'article 9-3 b) de la CCE définit les exigences de fiabilité applicables à une méthode utilisée pour créer une signature électronique.

c) Le troisième aspect concerne l'expression « *un niveau de fiabilité au moins équivalent* » figurant dans les articles 25 et 26. À notre avis, il n'est pas viable d'exiger une équivalence exacte en matière de fiabilité comme condition à la reconnaissance croisée d'un service de gestion de l'identité ou d'un service de confiance étranger. Les niveaux de fiabilité ne peuvent être déterminés avec une précision exacte et exiger une équivalence exacte ne peut que susciter des difficultés pratiques en matière de reconnaissance internationale. L'expression « *un niveau de fiabilité substantiellement équivalent ou supérieur* »⁶ serait plus appropriée dans un contexte multilatéral.

(Pour plus de détails, voir les paragraphes 17 à 19 ci-dessous.)

I. Relation entre l'article 9 et l'article 10-1, et entre les articles 16 à 21 et l'article 22-1

3. Le projet de loi type est structuré comme suit :

a) L'article 9 énonce la règle d'équivalence fonctionnelle pour l'identification d'une personne au moyen de services de gestion de l'identité, tandis que l'article 10-1 énonce les critères de fiabilité auxquels la méthode d'identification visée à l'article 9 doit satisfaire ;

b) De même, les articles 16 à 21 énoncent des règles d'équivalence fonctionnelle pour les signatures électroniques (art. 16), les cachets électroniques (art. 17), les horodatages électroniques (art. 18), l'archivage électronique (art. 19), les services d'envoi recommandé électroniques (art. 20) et l'authentification de site Web (art. 21), tandis que l'article 22-1 énonce les critères de fiabilité auxquels chacune des méthodes mentionnées aux articles 16 à 21 doit satisfaire.

4. À notre avis, la relation entre l'article 9 et l'article 10-1, et entre chacun des articles 16 à 21 et l'article 22-1 devrait être clarifiée par l'insertion des mots « *conforme au paragraphe 1 de l'article 10* » immédiatement après les mots « *si une méthode* » à l'article 9, et par l'insertion des mots « *conforme au paragraphe 1 de l'article 22* » immédiatement après les mots « *si une méthode* » dans chacun des articles 16 à 21. Il est ainsi précisé que l'exigence est satisfaite si une méthode conforme à l'article 10-1 ou à l'article 22-1 est utilisée pour remplir les fonctions visées, de manière à éviter toute suggestion tendant à ce que *n'importe quelle* méthode soit suffisante. Les versions révisées de ces articles sont reproduites dans l'**appendice** ci-dessous.

II. Article 10-1 b) et article 22-1 b)

A. Prévenir les contestations juridiques infondées

5. L'article 10-1 du projet de loi type dispose ce qui suit :

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

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

a) 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.

⁶ Cette formule a été examinée lors de la soixante-troisième session du Groupe de travail.

6. L'article 22-1 du projet de loi type, qui présente une structure similaire, est libellé comme suit :

Article 22. Critères de fiabilité pour les services de confiance

1. Aux fins des articles 16 à 21, la méthode doit :
 - a) 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.

7. Les « clauses de sauvegarde » en question se trouvent aux paragraphes 1 b) des articles 10 et 22. Elles font pendant aux articles 9-3 b) ii) de la Convention sur les communications électroniques et 12 b) de la Loi type sur les documents transférables électroniques et poursuivent le même objectif, à savoir empêcher toute contestation juridique fallacieuse de la validité.

a) L'article 9-3 de la CCE, qui contient la règle d'équivalence fonctionnelle pour les signatures électroniques, se lit comme suit :

3. Lorsque la loi exige qu'une communication ou un contrat soit signé par une partie, ou prévoit des conséquences en l'absence d'une signature, cette exigence est satisfaite dans le cas d'une communication électronique :

- a) Si une méthode est utilisée pour identifier la partie et pour indiquer la volonté de cette partie concernant l'information contenue dans la communication électronique; et
- b) Si la méthode utilisée est :
 - i) Soit une méthode dont la fiabilité est suffisante au regard de l'objet pour lequel la communication électronique a été créée ou transmise, compte tenu de toutes les circonstances, y compris toute convention en la matière ;
 - ii) Soit une méthode dont il est démontré dans les faits qu'elle a, par elle-même ou avec d'autres preuves, rempli les fonctions visées à l'alinéa a) ci-dessus.

Le problème auquel l'article 9-3 b) ii) de la CCE visait à remédier était le risque que la validité d'une signature électronique soit contestée, non pas au motif que le signataire supposé n'avait pas signé, ou que le document qu'il avait signé avait été modifié, mais au seul motif que la méthode de signature utilisée n'était pas *suffisamment fiable* dans les circonstances (c'est-à-dire que la fiabilité en principe/théorie n'était pas appropriée dans les circonstances)⁷. L'article 9-3 b) ii)

⁷ Ceci est expliqué en détail au paragraphe 164 de la note explicative relative à la Convention (reproduite ci-dessous) :

« 164. La CNUDCI a toutefois estimé que la Convention ne devrait pas permettre à une partie d'invoquer le "critère de fiabilité" pour annuler sa signature dans des cas où la véritable identité et la volonté effective de la partie pouvaient être prouvées. L'exigence selon laquelle une signature électronique doit être une méthode "dont la fiabilité est suffisante" ne devrait pas amener un tribunal ou un juge des faits à invalider un contrat dans son ensemble au motif que la signature électronique n'est pas *suffisamment* fiable, s'il n'y a pas de litige quant à l'identité du signataire ou quant à l'acte de signature (c'est-à-dire quant à l'authenticité de la signature électronique). Un tel résultat serait particulièrement fâcheux, car il permettrait à une partie à une opération dans laquelle une signature était exigée d'essayer de se soustraire à ses obligations en contestant la validité de sa signature (ou de la signature de l'autre partie) – non parce que le signataire supposé n'avait pas signé, ou que le document qu'il avait signé avait été modifié, mais au seul motif que la méthode de signature utilisée *n'était pas "suffisamment fiable"* dans les circonstances. Pour éviter cette situation, le sous-alinéa ii) de l'alinéa b) du paragraphe 3 valide toute méthode de

permet donc de mettre fin à une telle contestation juridique fallacieuse en prouvant que la méthode utilisée a rempli les fonctions décrites à l'article 9-3 a), c'est-à-dire en démontrant la fiabilité *de fait* de la méthode utilisée.

b) L'article 12 b) de la Loi type sur les documents transférables électroniques contient une « clause de sauvegarde » similaire pour la même raison⁸.

8. Il convient tout d'abord de noter que les mots « *suffisamment fiable* » sont utilisés dans les articles 10-1 a) et 22-1 a) car le *caractère approprié* de la fiabilité de la méthode utilisée dépend de l'objet pour lequel le service concerné est utilisé, compte tenu de toutes les circonstances pertinentes, qui peuvent inclure celles mentionnées aux articles 10-2 et 22-2. Une circonstance particulièrement pertinente serait tout accord conclu entre les parties quant à la méthode à utiliser. En d'autres termes, le caractère approprié de la fiabilité de la méthode utilisée dans une transaction particulière dépend des circonstances de celle-ci, et les articles 10-1 a) et 22-1 a) font référence à un niveau de fiabilité qui est relatif plutôt qu'unique et monolithique.

9. À l'instar de l'article 9-3 b) ii) de la CCE et de l'article 12 b) de la Loi type sur les documents transférables électroniques, les articles 10-1 b) et 22-1 b) visent à prévenir les contestations juridiques fallacieuses fondées sur le caractère approprié en théorie de la fiabilité de la méthode utilisée (*fiabilité en théorie*), en prévoyant que la méthode satisfait à l'article 9 ou aux articles 16 à 21 si elle a démontré dans les faits qu'elle a rempli la fonction décrite dans l'article concerné (*fiabilité de fait*), que ce soit par elle-même ou avec d'autres preuves.

10. La suppression des articles 10-1 b) et 22-1 b) ouvrirait la porte à ce type de contestations, ce qui n'est pas souhaitable :

a) Sans l'article 10-1 b), des acteurs opportunistes (comme une partie à une opération impliquant une identification électronique qui souhaite se soustraire à ses obligations, ou même un tiers qui bénéficie de l'invalidation de l'identification électronique) risquent d'être encouragés à contester la validité de l'identification qui en résulte – non pas au motif que celle-ci n'a pas eu lieu, mais au motif (frivole) que la méthode d'identification électronique utilisée n'était pas « *suffisamment fiable* » dans les circonstances ;

b) La même analyse s'applique dans le contexte des services de confiance. Si l'on prend les signatures électroniques à titre d'exemple, on constate que sans l'article 22-1 b), une partie à une transaction impliquant une signature électronique risque d'être encouragée à essayer de se soustraire à ses obligations en contestant la

signature – quel que soit son degré de fiabilité, en principe – dès lors qu'il est démontré dans les faits que la méthode utilisée identifie le signataire et indique la volonté de ce dernier concernant l'information contenue dans la communication électronique. »

[Les caractères gras sont ajoutés]

⁸ Voir les paragraphes 136 et 137 de la note explicative relative à la loi type (reproduits ci-dessous) :

« 136. L'alinéa b) prévoit une "clause de sauvegarde" visant à **prévenir des actions en justice abusives en validant des méthodes qui ont effectivement rempli leur fonction indépendamment de toute évaluation de leur fiabilité**. Il fait référence à l'exécution de la fonction dans le cas particulier faisant l'objet du litige et ne vise pas à prédire la fiabilité future sur la base des résultats antérieurs de la méthode. Cette disposition peut s'appliquer à toutes les fonctions visées par l'utilisation de documents transférables électroniques. Un mécanisme analogue est prévu à l'alinéa 3 b) ii) de l'article 9 de la Convention sur les communications électroniques, relatif à l'équivalence fonctionnelle des signatures électroniques.

137. Dans la pratique, le fait que la méthode employée ait rempli la fonction pour laquelle elle était mise en œuvre **préviendra toute discussion concernant l'évaluation de sa fiabilité conformément à l'alinéa a)**. »

[Les caractères gras sont ajoutés]

validité de sa propre signature (ou de celle de la contrepartie) – non parce que le signataire supposé n’a pas signé, ou que le document qu’il a signé a été modifié, mais au motif (frivole) que la méthode de signature utilisée n’était pas « *suffisamment fiable* » dans les circonstances. Un tiers qui a un intérêt dans l’annulation de la transaction peut également être incité à tenter la même chose.

11. On pourrait faire valoir que l’existence des articles 10-1 a) et 22-1 a) suffit à elle seule à prévenir les résultats indésirables décrits ci-dessus. En effet, un tribunal ou un juge des faits pourra rejeter la contestation opportuniste en concluant *ex post* que la méthode utilisée dans la transaction était « *suffisamment fiable* » au regard de l’objet pour lequel le service était utilisé, tel que décrit à l’article 9 (identification) ou aux articles 16 à 21 (services de confiance). Cependant, une telle approche recèle deux problèmes à notre avis. Le premier est que, même si de telles contestations juridiques n’aboutissent pas en fin de compte, elles n’en entraînent pas moins des litiges inutiles dans les transactions de commerce électronique, ce qui n’est pas souhaitable.

12. Le second problème, plus important, que pose la suppression des clauses de sauvegarde contenues dans les articles 10-1 b) et 22-1 b), qui exposerait au risque de contestations infondées toutes les transactions électroniques effectuées en vertu de la législation nationale incorporant la Loi type – et pouvant impliquer une identification électronique (art. 9), des signatures électroniques (art. 16), des cachets électroniques (art. 17), des horodatages électroniques (art. 18), un archivage électronique (art. 19), des services d’envoi recommandé électroniques (art. 20) ou une authentification de site Web (art. 21) – est qu’elle est source d’incertitudes dans des transactions commerciales consensuelles. Ce problème est illustré par l’exemple suivant :

a) Supposons qu’en 2023 (lorsque la Loi type aura été incorporée dans le droit interne de certains pays), deux parties conviennent de signer un contrat au moyen d’une signature numérique qui utilise le hachage SHA2-256 (qui génère un hachage de 256 bits) ;

b) Il n’est pas contesté que les parties ont signé le contrat. Il n’est pas non plus allégué que le contrat a été modifié de quelque manière que ce soit ;

c) Pourtant, sans clause de sauvegarde, la partie A (qui, par exemple, voudrait dénoncer le contrat qu’elle a signé avec la partie B parce qu’il s’est avéré être une mauvaise affaire) pourrait contester la validité des signatures numériques utilisées pour signer le contrat en alléguant que l’algorithme de hachage n’était pas « *suffisamment fiable* », et qu’il aurait fallu utiliser le hachage SHA3-512 plutôt que SHA2-256, qui n’est pas suffisamment fiable.

Une telle situation serait regrettable. Selon nous, si le critère « *suffisamment fiable* » est suffisamment souple, il est nécessaire d’aborder le risque de contestations juridiques fondées sur le caractère approprié en théorie de la fiabilité de la méthode utilisée. Afin d’assurer la certitude en matière commerciale, il ne convient pas de se fier uniquement au critère du « *suffisamment fiable* ». Comment les entreprises (comme la partie B dans notre exemple ci-dessus) pourraient-elles avoir la certitude que les transactions électroniques qu’elles concluront en 2023 ne risquent pas de faire l’objet d’une contestation juridique abusive à l’avenir ? Les clauses de sauvegarde contenues dans les articles 10-1 b) et 22-1 b) du projet de loi type visent à garantir que cela ne se produira pas.

B. Maintenir la cohérence du projet de loi type avec la Convention sur les communications électroniques et la Loi type sur les documents transférables électroniques

13. En conservant les articles 10-1 b) et 22-1 b) sous leur forme actuelle, le projet de loi type resterait également aligné sur la Convention sur les communications électroniques, qui est l’instrument le plus récemment élaboré par la CNUDCI sur les

transactions électroniques. Il est essentiel qu'il reste conforme à l'article 9-3 b) ii) de la Convention. De nombreux États (dont Singapour) sont parties à la Convention et ne pourraient par conséquent pas incorporer dans leur droit interne de loi incompatible avec celle-ci. Il existe également des États qui n'y sont pas parties mais ont adopté une législation sur les transactions électroniques fondée sur celle-ci, y compris une clause de sauvegarde⁹. La suppression des articles 10-1 b) et 22-1 b) (et en particulier du second) rendra le projet de loi type incompatible avec l'article 9-3 b) ii) de la Convention, ce qui posera également problème aux futurs États parties à la Convention.

14. Les États qui ont incorporé la Loi type sur les documents transférables électroniques dans leur droit interne ou envisagent de le faire s'inquiètent également de la suppression des articles 10-1 b) et 22-1 b) du projet de loi type, car celle-ci aurait pour conséquence de rendre le projet de loi type incompatible avec la Loi type sur les documents transférables électroniques.

15. Au cas où ces articles ne seraient pas conservés sous leur forme actuelle, la Commission devrait a) se prononcer sur les mesures à prendre par les États qui sont parties à la CCE ou ont adopté la Loi type sur les documents transférables électroniques pour remédier à cette incohérence ; et b) décider si elle continuerait de recommander la CCE et la Loi type sur les documents transférables électroniques (malgré l'incohérence de leurs dispositions) aux États qui envisagent de devenir partie à la première ou de mettre en œuvre la seconde.

C. Modifications à apporter au projet de note explicative pour préciser l'objet des articles 10-1 b) et 22-1 b)

16. Pour assurer une compréhension correcte de l'objectif des « clauses de sauvegarde » contenues aux articles 10-1 b) et 22-1 b), il faudrait modifier les paragraphes 142 et 143 du projet de note explicative comme suit :

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 **suffisamment** 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 1 b) n'entend pas promouvoir ni valider l'utilisation de méthodes non fiables. 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 prévoit** qu'en vertu de la Loi type, **la méthode doit être suffisamment fiable au regard de l'objet pour lequel le service de**

⁹ Par exemple, l'article 10 b) ii) de la loi australienne sur les transactions électroniques de 1999 suit l'article 9-3 b) ii) de la CCE. Il stipule ce qui suit :

Si, en vertu d'une loi du Commonwealth, la signature d'une personne est requise, cette exigence est considérée comme étant satisfaite dans le cas d'une communication électronique si :

- a) Dans tous les cas, une méthode est utilisée pour identifier la personne et pour indiquer sa volonté concernant l'information communiquée ; et
- b) Dans tous les cas – la méthode utilisée est :
 - i) Soit une méthode dont la fiabilité est suffisante au regard de l'objet pour lequel la communication électronique a été créée ou transmise, compte tenu de toutes les circonstances, y compris toute convention en la matière ; ou
 - ii) ***Soit une méthode dont il est démontré dans les faits qu'elle a, par elle-même ou avec d'autres preuves, rempli les fonctions visées à l'alinéa a)...***

[Les caractères gras sont ajoutés]

gestion de l'identité est utilisé, ou peut avoir démontré qu'elle a satisfait à l'identification ~~peut être assurée~~ dans les faits ~~ou par l'utilisation d'une méthode fiable~~. En d'autres termes, la preuve de l'aboutissement de l'identification dans les faits évite de devoir évaluer le caractère approprié de la fiabilité de la méthode utilisée.

III. Articles 25 et 26

17. Les articles 25 et 26 contiennent des dispositions qui facilitent la reconnaissance internationale respectivement de la gestion de l'identité et des services de confiance. Comme condition à la reconnaissance croisée de l'identification électronique et du résultat découlant de l'utilisation d'un service de confiance fournis en dehors de l'État adoptant, les projets d'articles 25 et 26 exigent actuellement que la méthode utilisée par le service de gestion de l'identité et celle utilisée par le service de confiance, respectivement, offrent « *un niveau de fiabilité au moins équivalent* ».

18. À notre avis, le critère du « *niveau de fiabilité au moins équivalent* » est problématique car il fonctionne de manière unidirectionnelle, et ne fonctionnerait pas dans un contexte multilatéral dans lequel de nombreux États différents adoptent cette même Loi type. En outre, le niveau de fiabilité d'une méthode utilisée qui est fonction de facteurs juridiques, techniques et de processus, constitue une norme qualitative et non quantitative. En d'autres termes, il serait très difficile pour un État cherchant à obtenir une reconnaissance croisée de ses services (État A) d'assurer une correspondance exacte entre le niveau de fiabilité de ses services et le niveau de fiabilité des services exigé par la législation de l'État accordant la reconnaissance (État B). Cela crée d'autres problèmes. Nous invitons la Commission à examiner le scénario hypothétique suivant :

a) Supposons que l'État A souhaite que son service de gestion de l'identité, qui a un niveau de fiabilité/garantie de « niveau 1 », soit reconnu dans l'État B. Le « niveau 1 » de l'État A est substantiellement équivalent au plus haut niveau de fiabilité/garantie de l'État B, qualifié lui d'« élevé ». Mais comme les lois de l'État B exigent que le niveau de fiabilité/garantie d'un service devant faire l'objet d'une reconnaissance croisée soit exactement équivalent ou supérieur, le service de gestion de l'identité émanant de l'État A ne peut pas faire l'objet d'une reconnaissance croisée dans l'État B, à moins que l'État A ne modifie ses normes juridiques et techniques de telle sorte que le niveau de fiabilité/garantie de son « niveau 1 » soit identique ou supérieur au « niveau élevé » de l'État B ;

b) Ce faisant, il est probable que le niveau accru de fiabilité/garantie de l'État A sera supérieur au niveau de fiabilité/garantie « élevé » de l'État B (la mesure de la fiabilité n'étant pas une science exacte, il y a des chances que l'État A veille, en augmentant son niveau de fiabilité/garantie, à ce qu'il soit supérieur au niveau « élevé », afin de garantir le succès de la reconnaissance transfrontière) ;

c) À la suite de la modification apportée par l'État A, le service de gestion de l'identité de « niveau 1 » de l'État A offrira un « *niveau de fiabilité au moins équivalent* » au niveau de fiabilité/garantie d'un service de gestion de l'identité de niveau « élevé » dans l'État B, si bien que ledit service pourra être reconnu comme offrant un niveau « élevé » dans l'État B. Toutefois, cela signifie inversement qu'un service de gestion de l'identité de niveau de fiabilité/garantie « élevé » de l'État B ne pourra pas être reconnu par les lois de l'État A comme équivalent au « niveau 1 », car le niveau « élevé » de l'État B sera désormais considéré comme inférieur au « niveau 1 » de l'État A (même s'il peut être substantiellement équivalent).

19. Un tel état de fait n'est pas souhaitable et rend la reconnaissance transfrontière sur une base mutuelle presque impossible, sans parler de la reconnaissance internationale sur une base multilatérale entre plusieurs États. Dans ces circonstances, il serait plus approprié que les articles 25 et 26 utilisent le critère du « *niveau de*

fiabilité substantiellement équivalent ou supérieur ». L'exigence d'un tel niveau permettrait de reconnaître les services de manière bidirectionnelle, entre deux États, sans exiger une équivalence exacte. Cela permettrait la reconnaissance croisée des services de l'État A, qualifiés de « niveau 1 », et des services de l'État B, qualifiés de « niveau élevé », pour autant qu'ils offrent tous deux un niveau de fiabilité/garantie substantiellement équivalent.

Appendice

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 **conforme au paragraphe 1 de l'article 10** est employée pour l'identification électronique de cette personne à cette fin.

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 **conforme au paragraphe 1 de l'article 22** est utilisée pour : [...]

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 **conforme au paragraphe 1 de l'article 22** est utilisée pour : [...]

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 **conforme au paragraphe 1 de l'article 22** est utilisée pour : [...]

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 **conforme au paragraphe 1 de l'article 22** est utilisée pour : [...]

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 **conforme au paragraphe 1 de l'article 22** est utilisée pour : [...]

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 **conforme au paragraphe 1 de l'article 22** est utilisée pour : [...]