Nations Unies A/CN.9/WG.IV/WP.145

Assemblée générale

Distr. limitée
20 février 2017
Français
Original: anglais

**Commission des Nations Unies pour le droit commercial international**
**Groupe de travail V (Droit de l'insolvabilité)**
**Cinquante-cinquième session**
New York, 24-28 avril 2017

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

# Proposition des États-Unis d'Amérique

## Note du Secrétariat

Les États-Unis d'Amérique ont transmis au Secrétariat un document pour examen à la cinquante-cinquième session du Groupe de travail. On trouvera en annexe à la présente note la traduction du texte de la proposition tel qu'il a été reçu par le Secrétariat.

V.17-01090 (F)

# Annexe

## I. Introduction

À sa cinquante-quatrième session, le Groupe de travail IV (Commerce électronique) a commencé à examiner la question de la gestion de l'identité et des services de confiance. Ses premières conclusions provisoires ont été les suivantes:

> 118. À l'issue de la discussion, le Groupe de travail est convenu que ses travaux futurs sur la gestion de l'identité et les services de confiance devraient se limiter à l'utilisation commerciale des systèmes de gestion de l'identité et ne pas tenir compte du caractère privé ou public du prestataire de services.
>
> 119. Le Groupe de travail est également convenu que les travaux sur la gestion de l'identité pourraient être tenus à titre prioritaire. Il est en outre convenu que l'accent devrait être mis sur les systèmes d'identité multipartites et sur les personnes physiques et morales, sans qu'un examen des systèmes d'identité bipartites et des objets matériels et numériques soit exclu, s'il y avait lieu.
>
> 120. Enfin, il a été convenu que le Groupe de travail poursuivrait ses travaux en précisant encore les objectifs et la portée du projet, en recensant les principes généraux applicables et en élaborant les définitions nécessaires.

(A/CN.9/897, par. 118 à 120).

Pour faciliter les débats de la cinquante-cinquième session du Groupe de travail et ceux menés ensuite, la délégation des États-Unis d'Amérique a établi le présent document, qui a pour but de donner un aperçu des questions à examiner par le Groupe. Il y aura sans doute beaucoup d'autres questions à examiner, mais on espère que la liste initiale suivante pourra servir de point de départ, guidant les débats initiaux et aidant à focaliser les activités. Nous espérons que l'examen de ces questions et d'autres qui pourraient être recensées par le Groupe donnera au Secrétariat des indications pour l'élaboration d'un document de travail sur la gestion de l'identité.

Nous croyons savoir que pendant la période intersessions, des experts ont engagé un débat informel sur la terminologie applicable. Bien que nous estimions qu'il faudra, au bout du compte, examiner attentivement le libellé des définitions des termes à utiliser dans ce projet, nous recommandons, à ce stade initial, que le Groupe de travail envisage d'utiliser les définitions initiales simplement comme base pour faciliter le débat. Nous reconnaissons cependant qu'il faudra peut-être, pour finir, s'entendre sur des définitions juridiques et techniques plus détaillées.

## II. Buts et objectifs du projet

Pour commencer, le Groupe de travail voudra peut-être prendre en considération les buts et objectifs généraux du projet. Compte tenu de la décision prise initialement de se concentrer sur l'utilisation des systèmes de gestion de l'identité à des fins commerciales, le Groupe de travail voudra peut-être se demander lesquels des buts et objectifs suivants pourraient convenir à ce projet:

- Promouvoir le développement d'un écosystème d'identité privé;
- Recenser et lever les obstacles juridiques aux transactions liées à l'identité commerciale;
- Lever les ambiguïtés concernant l'applicabilité du droit existant aux transactions liées à l'identité commerciale;
- Encourager l'utilisation commerciale et le recours à des justificatifs d'identité numériques de tiers;
- Faciliter l'établissement de la confiance requise pour les transactions liées à l'identité commerciale en ligne;

- Aider, en leur fournissant une base, les parties privées à décider s'il faut se fier à l'identité numérique dans les transactions commerciales;
- Recenser et lever les obstacles transfrontières à l'authentification électronique;
- Faciliter la reconnaissance transfrontière de l'identité numérique;
- Favoriser la confiance dans le commerce électronique.

# III. Nature du produit proposé du Groupe de travail IV

Il pourrait être utile de commencer à examiner le type de produit que le Groupe de travail souhaiterait développer dans le domaine de la gestion de l'identité commerciale.

# IV. Principes directeurs

Indépendamment de la forme ultime de ce qu'aura à produire le Groupe de travail, il existe plusieurs principes généraux que ce dernier pourra souhaiter envisager et, au besoin, adopter pour guider ses travaux relatifs à la gestion de l'identité. Comme pour la Loi type sur le commerce électronique et la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux, ces principes généraux pourront servir à guider le Groupe de travail dans ses délibérations. Ils pourront, en outre, être utiles pour aider à préciser la portée des travaux. Les principes directeurs que le Groupe de travail pourra souhaiter envisager sont notamment les suivants:

## A. Source de l'obligation légale d'identifier

Pour commencer, le Groupe de travail voudra peut-être se demander s'il faudrait qu'une législation relative à la gestion de l'identité prévoie l'obligation d'identifier une partie dans une transaction commerciale, indépendamment de celle qui s'applique en vertu d'autres lois. Si la législation relative à la gestion de l'identité ne prévoyait aucune obligation d'identifier une partie, l'obligation de le faire dans une transaction commerciale relèverait d'autres lois existantes telles que celles qui régissent la notarisation, la règle qui oblige à "connaître son client", les lois contre le blanchiment de capitaux ou celles qui régissent l'accès aux données personnelles. C'est cette approche que le Groupe de travail a adoptée pour les signatures électroniques lorsqu'il a élaboré la Loi type sur le commerce électronique et la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux.

## B. Autonomie des parties

Vu que les systèmes de gestion de l'identité seront généralement régis par des règles contractuelles convenues par les participants, il pourrait être important de déterminer si et dans quelle mesure il faudrait qu'une loi qui régit les transactions liées à l'identité reconnaisse ces règles et s'y soumette.

Ainsi le Groupe de travail voudra-t-il peut-être se demander s'il faudrait que le principe de l'autonomie des parties s'applique aux systèmes d'identité commerciale pour permettre aux parties à un système d'identité de modifier d'un commun accord les dispositions d'une ou de certaines règles juridiques.

## C. Neutralité technologique

De nombreux types différents de systèmes d'identité peuvent être conçus et mis en œuvre aux fins de transactions commerciales. Ces systèmes peuvent utiliser un large

éventail de technologies. Il peut s'agir de simples noms d'utilisateur et mots de passe, de systèmes plus complexes fondés sur la norme x.509 applicable aux infrastructures à clefs publiques, ou d'autres normes telles que SAML ou OpenID Connect. En outre, il se conçoit actuellement des systèmes à l'aide de nouvelles technologies telles que la chaîne de blocs.

Ainsi, le Groupe de travail voudra peut-être se demander s'il faudrait qu'un produit lié à la gestion de l'identité indique clairement que les règles y relatives ne devraient pas exiger l'utilisation d'une technologie particulière.

Le Groupe de travail souhaitera peut-être s'interroger plus avant sur la meilleure façon, pour la CNUDCI, de traiter l'existence et l'utilisation de multiples systèmes d'identité commerciale.

Une législation autre que celle propre à la gestion de l'identité pourra, bien sûr, exiger que les parties utilisent des systèmes qui répondent à certaines exigences. En outre, les parties elles-mêmes pourront insister pour que les personnes et entités avec lesquelles elles font affaire utilisent un système d'identité particulier. Par exemple, une entité commerciale pourra restreindre l'accès à ses services aux utilisateurs qui utilisent un ou plusieurs systèmes d'identité dont il est membre.

## D. Neutralité des modèles de système

Outre les diverses technologies qu'ils emploient, les systèmes d'identité commerciale expérimentent actuellement beaucoup en ce qui concerne les structures et approches organisationnelles et commerciales mises en œuvre. Nous pouvons probablement nous attendre à voir, à l'avenir, une grande diversité de modèles de système d'identité, même s'ils utilisent la même technologie sous-jacente. Il s'agira notamment d'arrangements de type courtier ou plate-forme, de modèles à fournisseur d'identité unique, de modèles à partie utilisatrice unique, de modèles d'organisation et de nombreuses autres approches différentes.

En conséquence, le Groupe de travail voudra peut-être se demander s'il devrait adopter comme principe le concept de neutralité des modèles de système, c'est-à-dire la reconnaissance du fait que le produit développé ne devrait pas être écrit d'une manière qui suppose ou nécessite l'utilisation d'un modèle commercial, organisationnel ou structurel particulier, et devrait pouvoir intégrer les futurs changements d'approche, de structure et de modèle commercial des systèmes.

## E. Non-Discrimination

Le Groupe de travail voudra peut-être également envisager d'appliquer le principe de non-discrimination dans le contexte de l'utilisation de systèmes d'identité à des fins commerciales. En vertu de ce principe, notamment, l'effet juridique (satisfaction d'une exigence légale d'identification, par exemple) et la recevabilité comme preuve, en justice, d'un justificatif d'identité électronique ne doivent pas être niés uniquement au motif que cette identification s'est faite sous forme électronique.

## F. Relation entre le droit de la gestion de l'identité et le droit de la vie privée

Les transactions liées à l'identité commerciale impliquant la délivrance ou l'utilisation d'un justificatif d'identité comporteront fréquemment des données personnelles. Dans ces cas, il pourra être important de respecter la confidentialité de ces données.

Les lois relatives à la vie privée traitent généralement de la protection des données personnelles conformément aux politiques publiques en vigueur. Peut-être, en conséquence, le Groupe de travail voudra-t-il examiner la relation qui existe entre ces lois et les systèmes de gestion de l'identité.

### G. Relation entre le droit de la gestion de l'identité et le droit de la sécurité des données

La sécurité des données est essentielle au bon fonctionnement et à la fiabilité des transactions liées à l'identité, du point de vue tant de la protection de la confidentialité des données personnelles impliquées dans ces transactions que du bon fonctionnement et de la fiabilité des communications de justificatifs formant la transaction elle-même.

Les lois relatives à la protection des données traitent souvent de la sécurité des données personnelles conformément aux politiques publiques en vigueur. Elles peuvent également faire de même en ce qui concerne la protection d'autres aspects des communications de transactions liées à l'identité. Peut-être, en conséquence, le Groupe de travail voudra-t-il examiner la relation qui existe entre ces lois et les systèmes de gestion de l'identité.

### H. Relation entre les règles contractuelles et les autres lois

Vu que les systèmes de gestion de l'identité seront généralement régis par des règles contractuelles (c'est-à-dire des cadres de confiance) convenues par les participants, peut-être le Groupe de travail voudra-t-il examiner la relation qui existe entre ces règles et les lois applicables qui ne sont pas directement liées à l'identité.

## V. Questions de fond

### A. Reconnaissance juridique

Le Groupe de travail voudra peut-être examiner la question de la reconnaissance juridique des identités authentifiées dans une transaction commerciale. À cet égard, il voudra peut-être s'interroger sur ce que cette reconnaissance est, sur ce qu'elle cherche à atteindre et sur les conditions requises pour l'obtenir; sur l'entité qui l'accorde; sur les raisons pour lesquelles on l'accorde; sur la relation qui existe entre la reconnaissance juridique et les lois qui exigent une certaine forme d'identification, telles celles qui régissent la notarisation, la règle qui oblige à "connaître son client", et les lois qui combattent le blanchiment d'argent et régissent l'accès aux données personnelles; enfin, le cas échéant, sur la façon dont cette reconnaissance s'applique à l'identité d'entités juridiques, de dispositifs ou d'objets numériques.

### B. Reconnaissance mutuelle transfrontière

Le concept de reconnaissance mutuelle est important pour faciliter l'utilisation commerciale des justificatifs d'identité et le recours à ces derniers, tant entre systèmes d'identité qu'entre pays.

Il existe de nombreuses questions que le Groupe de travail voudra peut-être examiner à propos de la reconnaissance mutuelle. Il pourra notamment se demander: a) s'il devrait exister une obligation de reconnaître les justificatifs; b) dans l'affirmative, qui serait tenu de le faire; c) dans l'affirmative, les justificatifs de quelle partie il faudrait reconnaître; d) quel est le but de cette reconnaissance mutuelle; e) ce qu'elle signifie exactement; f) quels critères (niveaux de garantie, par exemple) il faudrait remplir; g) s'il devrait exister des limites temporelles à la reconnaissance mutuelle; et h) si cette dernière devrait s'appliquer à l'identité d'entités juridiques, de dispositifs ou d'objets numériques.

## C. Attribution d'une identité à un sujet

L'attribution de données d'identité à un sujet (en vue de leur inclusion dans un justificatif) est souvent un élément critique des systèmes de gestion de l'identité. Une question fondamentale, à ce propos, sera de déterminer quand et dans quelles circonstances on attribuera les données d'identité d'un justificatif à un sujet donné.

Le Groupe de travail voudra peut-être examiner cette question sous deux angles. Premièrement, comment un fournisseur d'identité devra-t-il s'assurer que les données qui figurent dans un justificatif d'identité décrivent effectivement le sujet qui y est mentionné? Deuxièmement, lorsqu'un justificatif d'identité sera utilisé, comment une partie utilisatrice pourra-t-elle s'assurer que les données qui y figurent se rapportent à la personne qui le présente?

## D. Confiance/Attribution d'une action, d'un message de données ou d'une signature à un sujet

Une question clef, pour les participants à un système d'identité, est de savoir quand et dans quelles circonstances le fait, pour une partie, de se fier à un justificatif d'identité est approprié et raisonnable. Le caractère raisonnable de la confiance d'une partie peut soulever diverses questions, y compris lorsqu'on se fie à un justificatif erroné.

En ce qui concerne les signatures électroniques, par exemple, cette question est traitée à l'article 13 de la Loi type sur le commerce électronique.

## E. Responsabilité/répartition des risques

Les questions de responsabilité et de répartition des risques sont souvent citées comme obstacles majeurs à la mise en œuvre de systèmes d'identité commerciale. Les problèmes sont notamment les suivants: a) crainte des fournisseurs d'identité et des participants à des systèmes d'identité que le risque de responsabilité qui leur est alloué en vertu du droit actuel soit inapproprié ou simplement trop onéreux pour leur permettre de procéder; et b) crainte des participants à des systèmes d'identité que la loi soit trop vague, ambiguë ou incertaine pour leur permettre d'évaluer correctement leurs risques de participation.

Peut-être le Groupe de travail voudra-t-il se demander s'il devrait aborder la question de la responsabilité et, le cas échéant, pour quels rôles des systèmes d'identité et comment. Parmi les lois qui traitent de la responsabilité dans le contexte des systèmes de gestion de l'identité, on peut citer le règlement eIDAS de l'Union européenne et la loi de l'État de Virginie sur la gestion de l'identité électronique.

## F. Transparence

Les processus, les procédures et la technologie utilisés par un fournisseur d'identité pour délivrer et valider des justificatifs peuvent avoir une importante incidence sur la fiabilité d'une transaction liée à l'identité qui utilise ces justificatifs. En conséquence, il peut être important que les autres participants à un système d'identité comprennent comment ces processus, procédures et technologies sont mis en œuvre, afin de pouvoir évaluer par eux-mêmes la fiabilité des transactions qui en résultent. À cette fin, peut-être le Groupe de travail voudra-t-il se demander s'il existe un niveau approprié de transparence de la part de certains participants à un système d'identité. De même, en cas de violation ou de compromis dans l'un ou l'une quelconque des processus, procédures, technologies, bases de données ou justificatifs tenus par une partie dans le contexte d'un système d'identité, peut-être le Groupe de travail voudra-t-il se demander s'il faudrait divulguer des informations concernant ce compromis.

Parfois, des exigences de transparence sont également utilisées comme substitut à une réglementation imposant certains processus, procédures ou technologies. Une

approche fondée sur la transparence permet aux parties de prendre, en matière de fiabilité, leurs propres décisions sur la base d'informations plus complètes.

## G. Fiabilité/Niveaux de garantie

De nombreux systèmes d'identité définissent ce que l'on appelle des "niveaux de garantie" pour aider les participants à prendre des décisions en ce qui concerne la fiabilité de justificatifs d'identité et de transactions y relatives. Il existe plusieurs niveaux de schémas, qui impliquent souvent des degrés de garantie différents. Par exemple, l'Union européenne définit, dans son règlement eIDAS, trois niveaux de garantie ("faible", "élevé" et "substantiel"), alors qu'aux États-Unis et ailleurs, on utilise quatre niveaux.

Peut-être le Groupe de travail voudra-t-il étudier la meilleure façon d'accroître la confiance des participants dans un système d'identité. Bien que le concept de niveaux de garantie soit couramment utilisé, peut-être le Groupe de travail voudra-t-il également demander s'il l'on pourrait, pour accroître la confiance, utiliser d'autres mécanismes tels que la transparence imposée, la certification par une tierce partie ou d'autres approches.