Nations Unies A/CN.9/WG.IV/WP.163

Assemblée générale

Distr. limitée
20 février 2020
Français
Original : anglais

Commission des Nations Unies pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Soixantième session
New York, 6-9 avril 2020

Projet de dispositions relatives à l'utilisation et à la reconnaissance internationale de la gestion de l'identité et des services de confiance

Communication présentée par la Banque mondiale

Note du Secrétariat

La Banque mondiale a présenté une communication en vue de son examen par le Groupe de travail à sa soixantième session. On trouvera en annexe à la présente note la traduction du texte de cette communication tel qu'il a été reçu par le Secrétariat.

V.20-01483 (F)

Annexe

Commentaires formulés par la Banque mondiale au sujet du document A/CN.9/WG.IV/WP.162

En vue de la session que le Groupe de travail tiendra à New York du 6 au 9 avril 2020, la Banque mondiale a le plaisir de lui présenter les commentaires ci-après concernant le document A/CN.9/WG.IV/WP.162, intitulé « Projet de dispositions relatives à l'utilisation et à la reconnaissance internationale de la gestion de l'identité et des services de confiance » (le « projet de dispositions »).

I. Commentaires et observations d'ordre général

1. Priorité accordée à la gestion de l'identité. D'une manière générale, la Banque mondiale approuve les travaux du Groupe de travail IV, notamment en ce qui concerne la gestion de l'identité. Comme elle s'intéresse principalement à ce domaine, les commentaires ci-après portent essentiellement sur les sections du projet de dispositions en rapport avec la gestion de l'identité.

2. Systèmes de gestion de l'identité et opérations liées à l'identité. Le projet de dispositions traite essentiellement des systèmes de gestion de l'identité et des prestataires de services de gestion de l'identité, au détriment des opérations liées à l'identité. Eu égard à l'importance des opérations électroniques liées à l'identité, en particulier du point de vue du respect de la législation et de la reconnaissance juridique, et au fait qu'il est possible, et même courant, de les effectuer sans utiliser de système de gestion de l'identité ni passer par un prestataire de services de gestion de l'identité, le Groupe de travail devrait envisager d'aborder les questions relatives à ces opérations.

3. Rôles. Le projet de dispositions vise principalement à réglementer les systèmes de gestion de l'identité et les activités des prestataires de services de gestion de l'identité, et ne tient pas réellement compte (si ce n'est aux articles 5 et 8) des besoins des parties utilisatrices, des sujets ou des autres entités qui peuvent participer à un système de gestion de l'identité ou à une opération liée à l'identité. Par exemple, le projet de dispositions ne traite pas du droit d'une partie utilisatrice de faire appel à un tiers pour vérifier l'identité lorsqu'elle est légalement tenue de le faire. S'agissant des opérations liées à l'identité, le Groupe de travail voudra peut-être examiner plus avant les questions en rapport avec les entités pouvant jouer un rôle dans un système de gestion de l'identité qui ne sont pas des prestataires de services de gestion de l'identité.

4. Rapport entre systèmes publics et privés de gestion de l'identité. Le projet de dispositions porte sur les systèmes privés de gestion de l'identité et sur les prestataires de services de gestion de l'identité du secteur privé. De prime abord, il ne s'applique pas aux systèmes publics de gestion de l'identité, par exemple aux systèmes nationaux de gestion de l'identité, ni aux prestataires de services de gestion de l'identité du secteur public. De ce fait, le projet de dispositions, forme envisagée pour le produit des travaux du Groupe de travail, ne couvre pas les nombreux systèmes nationaux de gestion de l'identité exploités par le gouvernement (comme ceux de l'Inde et de l'Estonie, entre autres).

Toutefois, il importe d'avoir à l'esprit qu'il y aura probablement une interaction importante entre les systèmes publics et privés de gestion de l'identité. On peut ainsi supposer que le projet de dispositions s'appliquera dans les cas où un organisme public est client (par exemple, en tant que partie utilisatrice ou sujet de données) d'un prestataire de services de gestion de l'identité du secteur privé, ou utilise un système d'identité fédéré privé plutôt qu'un système de gestion de l'identité exploité par le gouvernement. En outre, les processus de contrôle et d'authentification de l'identité utilisés par les prestataires de services de gestion de l'identité du secteur privé

reposent couramment sur des justificatifs d'identité fondamentale délivrés par des systèmes publics, qui sont souvent considérés comme très fiables et font autorité.

Par conséquent, le Groupe de travail devrait examiner et préciser la nature du rapport existant entre les systèmes publics et privés de gestion de l'identité, en s'intéressant notamment, sans toutefois s'y limiter, à la question de savoir quand et/ou comment il pourrait être approprié pour des opérateurs de systèmes privés de gestion de l'identité d'utiliser des informations relatives à l'identité fondamentale et des procédés d'authentification fournis par un gouvernement. Il pourrait, par exemple, envisager d'élaborer des règles applicables aux systèmes privés de gestion de l'identité pour les opérations suivantes :

- Utilisation de numéros d'identification ou d'autres informations d'identification fournis par un gouvernement ;
- Utilisation de justificatifs d'identité délivrés par un gouvernement ;
- Accès à des bases de données gouvernementales pour le contrôle et l'authentification de l'identité ; ou
- Utilisation, de manière générale, d'informations ou de processus d'identification fournis par un gouvernement.

5. Cadres de confiance. Le projet de dispositions ne dit rien sur le rôle des règles contractuelles qui régissent l'exploitation d'un système donné de gestion de l'identité, souvent appelées cadre de confiance, règles de système ou règles d'exploitation (collectivement désignées ci-après par le terme « cadre de confiance »), ni sur la manière dont il interagit avec ces règles[1]. Le Groupe de travail devrait envisager de modifier le texte de manière à préciser cette interaction et à expliquer en quoi le projet de dispositions devrait se différencier, sur le plan tant des questions traitées que du niveau d'exhaustivité, du cadre de confiance applicable à un système de gestion de l'identité donné. Des questions comme les obligations des entités participantes, la fiabilité et les niveaux de garantie, par exemple, sont souvent abordées dans le cadre de confiance propre à un système de gestion de l'identité donné.

Dans le même ordre d'idées, le Groupe de travail voudra peut-être réfléchir à la mesure dans laquelle les termes d'un cadre de confiance pourraient modifier ou remplacer ceux du projet de dispositions. Par exemple, nonobstant les termes du projet de dispositions en matière de responsabilité, il est difficile de savoir si les parties peuvent définir leurs propres règles de responsabilité dans le cadre de confiance qu'elles adoptent relativement à leur propre système de gestion de l'identité.

6. Utilisation de modèles juridiques relatifs aux signatures électroniques. La structure et l'approche adoptées dans le projet de dispositions se fondent largement sur la Loi type de la CNUDCI sur les signatures électroniques, et ne tiennent donc pas compte du fait que les questions relatives aux signatures sont très différentes de celles qui interviennent en matière d'identité (bien que l'identité soit parfois une composante d'une signature). Ainsi, alors qu'il est possible de définir, dans l'environnement électronique, un équivalent juridique unique de l'exigence de signature, il est difficile d'en faire de même pour l'exigence de vérification de l'identité.

Le problème vient en partie du fait que les lois qui exigent une signature exigent toutes la même chose (à savoir une signature), alors que celles qui exigent l'identification d'une personne imposent souvent plusieurs exigences distinctes concernant le processus d'identification (selon le type d'identité à établir (« fondamentale » ou « fonctionnelle »)[2], le but de l'identification, les risques en

[1] L'expression « règles qui régissent l'exploitation du système de gestion de l'identité » apparaît aux articles 6 c), 6 f), 10-1 b) et 23-1 a) du projet de dispositions, mais ces règles ne sont nulle part définies ni traitées en détail.

[2] Voir, par exemple, Banque mondiale, *Practitioners Guide* (2019), p. 12 et 13 (entre autres), disponible (en anglais seulement) à l'adresse https://id4d.worldbank.org/guide.

présence, etc.). Par conséquent, s'il est relativement facile de définir un équivalent juridique du concept unitaire de signature, il n'est pas nécessairement possible d'en faire de même pour l'identification, qui fait l'objet d'approches juridiques diverses. Il importe donc que le Groupe de travail ne se cantonne pas à une structure prédéfinie inspirée de la Loi type sur les signatures électroniques, mais examine de manière indépendante les questions juridiques à prendre en compte dans le cas de l'identité.

7. Options envisageables pour la vérification de l'identité. Pour vérifier l'identité d'une personne à qui elle a affaire, une partie utilisatrice dispose de deux options, à savoir :

- Procéder elle-même à la vérification de l'identité ; ou
- Faire appel à un tiers prestataire de services de gestion de l'identité.

Bien que la plupart des parties utilisatrices aient recours à la première option, le projet de dispositions n'envisage que la seconde. Le Groupe de travail voudra peut-être se demander si le projet de dispositions devrait aborder le thème de l'identité dans une optique plus large, en couvrant les questions qui entrent en jeu dans les deux situations.

8. Droit d'une partie utilisatrice de se fier à certains éléments. Idéalement, le projet de dispositions devrait traiter des questions relatives au droit d'une partie utilisatrice de se fier à certains éléments. Il pourrait s'agir, par exemple, du droit d'une partie utilisatrice : i) de se fier à un justificatif d'identité en général ; ii) de se fier à un justificatif délivré par un tiers pour satisfaire aux exigences d'une loi particulière qui impose une obligation d'identification ; et iii) de faire appel à un tiers prestataire de services de gestion de l'identité pour satisfaire à l'obligation juridique qui lui incombe d'identifier une personne.

9. Droit d'une partie utilisatrice de faire appel à un tiers. En lien avec ce qui précède, alors que certaines des lois qui imposent une obligation d'identification autorisent expressément les parties utilisatrices à faire appel à un tiers prestataire de services (voir, par exemple, le règlement d'application de la loi californienne sur le respect de la vie privée des consommateurs[3]), nombre d'entre elles ne disent rien à ce sujet (ou exigent que les parties utilisatrices procèdent elle-même à l'identification). Les délibérations du Groupe de travail relatives à l'identité devraient également porter sur cette question.

II. Commentaires article par article

1. Article premier. Définitions

a) **Termes manquants** : Plusieurs termes, bien qu'ils soient employés tout au long du projet de dispositions, ne sont pas définis. Les termes utilisés mais non définis sont les suivants :

- « facteurs d'identification électronique », article 6 d) i) ;
- « mécanismes d'identification électronique », articles 6 d) ii), 8 a) et 8 b) ;
- « gestion de l'identité », utilisé comme terme modificatif tout au long du texte, mais défini à aucun endroit ;
- « identifiant », article 1 b) ;
- « règles qui régissent les systèmes de gestion de l'identité », articles 6 c), 6 f), 10 b) et 23 a) ;

[3] Voir règlement d'application de la loi californienne sur le respect de la vie privée des consommateurs (California Consumer Privacy Act Regulations), article 4, par. 999.323 b), disponible à l'adresse https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf?.

- Cette expression pourrait désigner le cadre de confiance relatif à un système donné de gestion de l'identité, mais pourrait également, dans son libellé actuel, s'appliquer à toute loi ou règlement régissant le système de gestion de l'identité. Il faudrait en clarifier l'utilisation ;

• « vérification », article 6 a) ii) ;

- Il serait peut-être également important de préciser le concept de « vérification », car ce terme est souvent une grande source de confusion. Le terme « vérification de l'identité », par exemple, s'emploie fréquemment pour désigner, dans certains cas, l'identification du sujet de données, et, dans d'autres, l'authentification de ce sujet de données. Compte tenu de la fréquence de ce terme, il convient d'en préciser soigneusement le sens et de l'utiliser à bon escient tout au long du texte.

b) **Authentification** : Les termes « authentification » et « identification électronique » sont utilisés pour désigner essentiellement la même chose, le premier étant employé dans le contexte des services de confiance, le second dans celui des services de gestion de l'identité. Puisqu'il s'agit de deux concepts identiques, le Groupe de travail pourrait envisager de les désigner par le même terme.

c) **Identification électronique** : Le fait de remplacer le seul terme « identification » par les termes « contrôle d'identité » et « identification électronique » constitue un pas important vers la clarification du processus d'identification et l'établissement d'une distinction entre les deux aspects qu'il recouvre. Toutefois, on pourrait se préoccuper du fait que le terme « identification électronique » décrit l'ensemble du processus comprenant le contrôle d'identité, l'émission d'un justificatif et l'authentification du lien entre les données du justificatif et la personne concernée, ou qu'il tend par confusion à être interprété dans ce sens. Il est donc recommandé au Groupe de travail de réfléchir à un autre terme pour remplacer « identification électronique ».

En outre, l'emploi du mot « électronique » pour ce terme, qui est censé décrire le « processus utilisé pour obtenir une garantie quant au lien unissant un sujet à une identité » pourrait créer une certaine confusion quant à la nature des processus, systèmes et services visés par le projet de dispositions. Le même problème se pose pour les « services de gestion de l'identité » et les « systèmes de gestion de l'identité », dont la définition prévoit qu'ils se présentent « sous forme électronique ». L'approche qui consiste à décrire le processus d'association comme étant « électronique », ou les services et systèmes de gestion de l'identité comme revêtant une « forme électronique » ne tient pas compte du fait que, dans certains cas, tout ou partie du processus peut ne pas être de nature électronique. Par exemple, certaines fonctions peuvent être exécutées sous forme non électronique, ou au moyen de documents papier, comme c'est le cas notamment pour le contrôle d'identité. Par conséquent, il est recommandé au Groupe de travail de tenir compte du fait que les processus, systèmes et services visés par le projet de dispositions peuvent très bien comporter un certain nombre d'éléments non électroniques.

d) **Identité** : Le fait de définir l'identité comme un « ensemble d'attributs qui permet à [un sujet] [une personne] d'être identifié[e] "de manière unique" dans un contexte particulier » semble trop restrictif. Dans bien des cas, l'identification est utilisée à des fins de sélection, et non d'unicité. Par exemple, elle peut simplement servir à déterminer si une personne donnée est membre d'un groupe particulier, et consister à poser une question comme « Avez-vous plus de 18 ans ? », « Êtes-vous membre du club ? », ou encore « Êtes-vous un(e) citoyen(ne) ? ». On peut supposer que de nombreuses personnes posséderaient ces attributs, de sorte que l'identité n'aurait pas besoin d'être unique, mais permettrait de caractériser suffisamment le sujet de données dans un contexte où seule une identité limitée est requise.

e) **Justificatifs d'identité** : Le Groupe de travail devrait tenir compte des faits nouveaux concernant les moyens de communiquer des informations relatives à

l'identité. Même si la revendication et la vérification de l'identité se font généralement à l'aide de justificatifs d'identité, il est bon d'avoir à l'esprit que de nombreux systèmes de gestion de l'identité récents n'utilisent pas de justificatifs d'identité proprement dits. Dès lors, bien que la définition ne soit pas nécessairement incorrecte, il convient de veiller à ne pas laisser supposer, dans le projet de dispositions, qu'un justificatif d'identité sera toujours utilisé. En outre, on note que la définition est limitée à l'identité « sous forme électronique ». Le Groupe de travail voudra peut-être se demander si le projet de dispositions devrait également couvrir l'identification traditionnelle au moyen de documents papier ou en personne.

f) **Contrôle d'identité** : Le processus de contrôle d'identité ne doit pas « établir et confirmer » complètement l'identité d'un sujet. On peut s'attendre à ce qu'il comprenne la collecte, la vérification et/ou la validation d'un ou de plusieurs attributs qui, même s'ils ne sont pas en soi suffisants pour définir et confirmer une identité, pourraient être utilisés par d'autres pour confirmer une identité. Le Groupe de travail voudra donc peut-être envisager d'élargir la définition du terme « contrôle d'identité ».

g) **Partie utilisatrice** : Il n'était peut-être pas souhaitable de supprimer la définition de ce terme pour la remplacer par celle du terme « abonné ». Le concept d'abonné suppose la participation active au système d'une personne qui est tenue au respect de règles. Cela peut certes être le cas d'une partie utilisatrice, mais d'autres personnes ou entités peuvent conclure un accord pour la prestation de services de gestion de l'identité. Il peut s'agir, par exemple, de sujets. Ainsi, le fait de ne pas établir de distinction entre parties utilisatrices et sujets (ou autres utilisateurs d'un système de gestion de l'identité) risque de créer une certaine confusion lors de l'application des règles énoncées dans le projet de dispositions. Il est proposé au Groupe de travail d'envisager de maintenir une définition du terme « partie utilisatrice », afin que les questions abordées dans les sections suivantes s'appliquent, selon qu'il convient, soit aux parties utilisatrices, soit aux sujets.

h) **Sujet** : Dans le contexte des services de gestion de l'identité, un sujet est une personne ou un objet qui est identifié ou, du moins, qui se soumet au processus de contrôle d'identité. Le fait de supprimer la référence à l'identification rend ce terme générique, et probablement peu utile.

i) **Abonné** : Comme indiqué ci-dessus, le concept d'abonné en tant que personne « qui conclut un accord avec un prestataire de services de gestion de l'identité ou un prestataire de services de confiance en vue de la fourniture de tels services » semble trop large, car il pourrait s'appliquer à de nombreux rôles au sein d'un système d'identité, ainsi qu'aux sujets. Par exemple, le libellé du paragraphe 3 de l'option C de l'article 12 part du principe que les abonnés sont des parties utilisatrices. Toutefois, les abonnés pourraient également être des sujets ou jouer l'un des nombreux autres rôles existant au sein d'un système de gestion de l'identité, auquel cas les dispositions de cet article seraient erronées.

2. Article 2. Champ d'application

Le Groupe de travail devrait envisager de réexaminer le champ d'application du projet de dispositions en ce qui concerne la gestion de l'identité. Selon le libellé actuel de l'article 2, seuls deux aspects en sont couverts, à savoir : 1) l'***utilisation*** de ***systèmes de gestion de l'identité*** ; et 2) la ***reconnaissance internationale*** de ***systèmes de gestion de l'identité***.

Le Groupe de travail voudra peut-être se demander si le champ d'application devrait également inclure les ***opérations de gestion de l'identité***, et, éventuellement, faire référence au ***fonctionnement*** d'un système de gestion de l'identité et/ou à la ***prestation*** de services de gestion de l'identité.

En outre, puisqu'il reconnaît ne pas être habilité à élaborer de règles pour les systèmes de gestion de l'identité exploités par des gouvernements (par exemple, les systèmes nationaux), le Groupe de travail devrait envisager de modifier l'article 2 afin de

préciser que le projet de dispositions « s'applique […] aux systèmes ***privés*** de gestion de l'identité ».

3. Article 3. Caractère volontaire de l'utilisation de systèmes de gestion de l'identité et de services de confiance

Selon l'article 3-2, le consentement d'une personne à utiliser un système de gestion de l'identité est déduit de son comportement. Toutefois, le Groupe de travail devrait prendre note du fait que cette déduction est inappropriée dans le cas où l'identité de la personne a été usurpée, par exemple lorsqu'un voleur d'identité utilise un faux justificatif, ou qu'il utilise un justificatif authentique délivré à quelqu'un d'autre. Dans de tels cas, la personne dont le consentement est déduit n'est pas celle qui adopte le comportement considéré.

4. Article 4. Interprétation

Le Groupe de travail voudra peut-être envisager de faire en sorte que le projet de dispositions ne crée pas de discrimination entre les modèles de systèmes de gestion de l'identité, en introduisant le concept de **neutralité des systèmes de gestion de l'identité** (ou neutralité des opérations liées à l'identité). Dans la mesure où il existe des méthodes très diverses pour effectuer des opérations en ligne liées à l'identité (systèmes à fournisseur d'identité unique, systèmes fédérés (fournisseurs d'identité multiples), systèmes contrôlés par l'utilisateur ou axés sur l'utilisateur, systèmes de type plateforme, systèmes DLT, systèmes sans justificatifs, systèmes d'identité auto-souveraine, etc.), il importe que le projet de dispositions n'exige ou ne suppose l'adoption d'aucune approche particulière pour la conduite des processus d'identification et/ou d'authentification, ou pour ce qui est du système utilisé à cette fin. Par conséquent, le Groupe de travail devrait réfléchir aux moyens de faire en sorte que le projet de dispositions ne suppose ni n'exige l'utilisation d'un modèle de système particulier.

5. Article 5. Reconnaissance juridique de la gestion de l'identité

Il convient peut-être de mener un examen et une analyse supplémentaires au sujet de l'article 5 a), qui dispose que l'identification électronique n'est pas privée d'effets juridiques au seul motif qu'elle a lieu sous forme électronique. Les auteurs de la présente communication supposent (mais n'ont pas vérifié) que certaines lois relatives à l'utilisation de justificatifs d'identité exigent la présentation d'un document papier ou d'un autre élément matériel et non d'un moyen d'identification électronique. C'est pourquoi, avant d'aller à l'encontre de ce type de lois, il est recommandé au Groupe de travail de mener un examen et une analyse plus poussés, afin de déterminer les incidences de cette disposition.

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

Bien-fondé de l'application d'un modèle unique. L'article 6 énonce un ensemble d'obligations qui incombent aux prestataires de services de gestion de l'identité. Les obligations énumérées correspondent au modèle des systèmes de gestion de l'identité traditionnels, et partent du principe que l'ensemble des fonctions d'un système de gestion de l'identité est assuré par le prestataire de services de gestion de l'identité ou relève de sa responsabilité. Toutefois, les modèles de systèmes de gestion de l'identité étant actuellement l'objet d'évolutions et d'expérimentations diverses, il y a lieu de craindre que l'utilisation de cette liste d'obligations ne se fonde sur un modèle ancien qui risque d'être inadapté aux systèmes de gestion de l'identité récents et/ou de contraindre excessivement la conduite de nouvelles expérimentations. Dans nombre de systèmes de gestion de l'identité récents, il arrive, par exemple, que certaines des fonctions des prestataires de services énumérées à l'article 6 soient confiées à diverses autres entités (prestataires de services de confiance, bureaux d'enregistrement, agents d'inscription, prestataires de services de justificatifs d'identité, mandataires, prestataires de services d'authentification, plateformes, etc.).

Au vu de la diversité croissante des modèles de systèmes de gestion de l'identité, le Groupe de travail devrait se demander s'il est encore opportun d'imposer un seul et même ensemble d'obligations à tous les prestataires de services de gestion de l'identité dans le projet de dispositions.

Source des obligations. Le Groupe de travail voudra peut-être également se pencher sur une question préliminaire essentielle, qui est de savoir si les obligations des prestataires de services de gestion de l'identité du secteur privé (ou de toutes autres entités jouant un rôle au sein d'un système privé de gestion de l'identité) devraient être énoncées dans le projet de dispositions et s'appliquer à tous les systèmes de gestion de l'identité, ou si ces obligations devraient être définies, pour chaque système privé de gestion de l'identité, dans le cadre de confiance de nature contractuelle qui s'y applique. Si les obligations liées à chaque rôle étaient prévues dans le cadre de confiance applicable à un système donné de gestion de l'identité, cela permettrait à l'opérateur du système et aux autres entités qui y participent de les adapter à l'objet et à l'utilisation du système, ainsi que de se conformer à la loi applicable.

Règles régissant le système de gestion de l'identité. Enfin, il convient de noter que cet article fait référence aux « règles qui régissent les systèmes de gestion de l'identité », lesquelles ne sont pas définies. Il est difficile de savoir, par exemple, si ces règles sont censées correspondre au cadre de confiance de nature contractuelle qui s'applique à un système donné de gestion de l'identité, ou à autre chose.

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

Obligation d'intervention en cas de violation des données. Dans son libellé actuel, l'article 7 semble opérer une confusion entre systèmes de gestion de l'identité et prestataires de services de gestion de l'identité, en partant du principe qu'un système de gestion de l'identité sera sous le contrôle d'un seul et même prestataire de services assurant toutes les fonctions du système. En outre, cet article impose des obligations aux prestataires de services dès qu'une atteinte à la sécurité ou une perte d'intégrité a lieu, sans poser la question de savoir s'ils ont connaissance de cette atteinte ou de cette perte, si elle relève de leur responsabilité ou s'ils ont un certain contrôle sur elle. Toutefois, dans la pratique, il arrive que de multiples parties jouent un rôle au sein d'un système de gestion de l'identité, et que nombre d'entre elles ne soient aucunement responsables du réseau, système ou serveur, des employés, ou de toute autre personne ou tout autre dispositif directement touchés ou concernés par l'incident, et n'aient aucun contrôle sur eux.

Dans de nombreuses approches récentes en matière de systèmes de gestion de l'identité, certaines de ces fonctions peuvent être assurées par des entités distinctes (prestataires de services de confiance, bureaux d'enregistrement, agents d'inscription, prestataires de services de justificatifs d'identité, prestataires de services d'authentification, plateformes, etc.). Chacun de ces rôles peut, de manière indépendante, être à l'origine d'une violation des données, dont le prestataire de services de gestion de l'identité n'aura peut-être même pas connaissance.

Par conséquent, lorsqu'il examinera ce sujet, le Groupe de travail devrait tenir compte de la *différence entre systèmes de gestion de l'identité et prestataires de services de gestion de l'identité*, et du fait que de *multiples prestataires de services de gestion de l'identité* (et de multiples entités jouant d'autres rôles) peuvent participer à un seul et même système de gestion de l'identité. Dès lors, en cas de violation des données, la première question à se poser sera probablement de savoir qui est responsable du ou des éléments touchés, et à qui il incombe de notifier l'incident.

Idéalement, les obligations d'intervention en cas de violation des données prévues à l'article 7 (par exemple, l'obligation de remédier à l'atteinte, de révoquer les justificatifs, d'informer les autorités ou d'informer les sujets de données ou les parties utilisatrices) devraient être imposées uniquement à la partie précisément touchée ou autrement responsable du serveur, réseau ou système précisément atteint ou compromis. Par exemple, dans le cas d'un système de gestion de l'identité comportant

de multiples prestataires de services de gestion de l'identité ou de multiples rôles, il conviendrait peut-être i) d'imposer l'obligation de remédier à l'atteinte à l'entité qui a été effectivement touchée et qui est à même de la limiter et d'y remédier, et ii) d'imposer l'obligation d'informer les sujets à l'entité qui est en rapport avec eux.

Atteinte de niveau systémique. En lien avec ce qui précède, le Groupe de travail devrait envisager de modifier l'article 7 afin d'envisager la possibilité qu'un système de gestion de l'identité comprenant plusieurs prestataires de services de gestion de l'identité soit touché par une atteinte majeure de niveau systémique (par exemple, la compromission d'une clef racine privée) qui compromette l'intégralité du système et présente un risque pour tous les prestataires de services, selon le type et la structure du système. En pareil cas, tous les prestataires de services pourraient être touchés, qu'ils soient ou non responsables de l'atteinte proprement dite. Dès lors, il faudra probablement faire face à la situation d'une manière différente, et tous les prestataires de service devront sans doute assumer des obligations d'intervention, même s'ils ne seront peut-être pas responsables de l'atteinte.

Responsabilité en cas de perte d'intégrité. Enfin, on note que l'article 7-1 b) impose aux prestataires de services de gestion de l'identité l'obligation de « remédier à l'atteinte ou à la ***perte*** ». S'il peut sembler approprié de les obliger à remédier à une atteinte (ou, du moins, à une atteinte sur laquelle ils ont un certain contrôle), le Groupe de travail devrait se demander s'il convient de les obliger également à remédier à une « perte », qui pourrait se révéler importante. Pour déterminer si et dans quelle mesure un prestataire de services de gestion de l'identité est responsable des pertes subies, il conviendrait de se référer aux règles applicables en matière de responsabilité, quelle que soit la manière dont elles sont déterminées.

8. Article 8. Obligations incombant aux abonnés

Obligations liées aux différents rôles. À titre de remarque générale, si le projet de dispositions devait traiter des obligations des entités participant à un système de gestion de l'identité (voir, par exemple, art. 6, 7 et 8), le Groupe de travail voudra peut-être envisager de traiter les obligations de ***toutes*** ces entités (agents d'inscription, fournisseurs d'attributs, prestataires de services de gestion de l'identité, prestataires de services de vérification de l'identité, utilisateurs, plateformes, parties utilisatrices, prestataires de services de confiance, abonnés, etc.). Cette démarche semble également importante pour l'attribution des responsabilités conformément à l'article 12, examiné ci-après.

À quel endroit définir les obligations. Par ailleurs, le Groupe de travail voudra peut-être se demander à quel endroit il serait le plus indiqué de définir les obligations des prestataires de services de gestion de l'identité, des abonnés et des autres entités participant à un système de gestion de l'identité. Les articles 6, 7 et 8 du projet de dispositions prévoient un modèle unique pour ce qui est des obligations des prestataires de services de gestion de l'identité et des abonnés. Toutefois, compte tenu de la diversité des systèmes de gestion de l'identité, il conviendrait peut-être mieux d'autoriser ou d'obliger les parties à chaque système à définir les obligations liées aux différents rôles dans un cadre de confiance adapté à la technologie, à la méthodologie et à la finalité propres au système, plutôt que d'utiliser le projet de dispositions pour imposer un modèle unique à tous les systèmes. Cela tient en partie au fait que les catégories et définitions des rôles des systèmes de gestion de l'identité, ainsi que les obligations des entités qui exercent ces rôles, seront probablement très variables d'un système à un autre. L'un des facteurs à l'origine de cette disparité est le but dans lequel chaque système de gestion de l'identité est créé (par exemple, pour faciliter les communications en ligne dans l'industrie pharmaceutique, comme le système SAFE BioPharma ; pour faciliter la mise en commun des informations universitaires, comme le système InCommon, utilisé par les universités ; ou pour faciliter les communications entre organismes publics, comme le système eIDAS).

En outre, comme indiqué ci-dessus au sujet de l'article 6, les modèles de systèmes de gestion de l'identité sont actuellement l'objet d'évolutions et d'expérimentations

diverses, ce qui soulève des doutes quant à l'opportunité d'établir une liste type d'obligations, cette démarche risquant d'imposer un modèle obsolète mal adapté à de nombreux systèmes actuels et de contraindre la conduite de nouvelles expérimentations.

Obligations des abonnés. L'article 8 traite des abonnés (c'est-à-dire des personnes qui concluent un accord pour la prestation de services de gestion de l'identité). Cette notion recouvre probablement de nombreuses entités participant à un système de gestion de l'identité, comme les parties utilisatrices, les sujets de données qui sont des personnes, et peut-être diverses entités jouant d'autres rôles. L'article 8 impose aux abonnés l'obligation d'informer le prestataire de services de gestion de l'identité lorsqu'ils savent que des justificatifs d'identité ou des mécanismes d'identification électronique du système de gestion de l'identité ont été compromis, ou que des circonstances dont ils ont connaissance engendrent un risque important que tel ait été le cas.

Dans le cas des abonnés qui sont des personnes (par exemple, des sujets de données), cette disposition pourrait représenter une exigence lourde et déraisonnable. Par exemple, il existe probablement de nombreuses situations où une personne abonnée à un système de gestion de l'identité pourra avoir connaissance de circonstances indiquant une compromission potentielle, mais n'en comprendra tout simplement pas la signification. De plus, dans la mesure où l'obligation en question semble s'appliquer au système dans son intégralité (et non, par exemple, à un seul justificatif d'identité délivré à une personne donnée), cette disposition semble imposer une charge importante aux personnes (tout comme, d'ailleurs, aux autres abonnés au système), qui pourront avoir connaissance de certaines informations ayant une incidence sur l'ensemble du système, mais n'en mesureront tout simplement pas la portée.

Même lorsque c'est le justificatif d'identité d'une personne qui a été perdu ou compromis, il ne serait peut-être pas toujours approprié que celle-ci soit soumise à une obligation de déclaration. Le fait d'exiger des sujets qu'ils signalent ce type d'incidents (par exemple, le vol de leur numéro de carte bancaire) pourrait se révéler tout simplement irréaliste, voire inapproprié (en particulier lorsqu'il s'agit d'utilisateurs peu expérimentés, ou dans le cas d'atteintes survenant en ligne ou dans d'autres contextes où ils pourraient ne pas être aptes au discernement). En outre, dans le cas de systèmes de gestion de l'identité qui ne reposent pas sur l'utilisation de justificatifs matériels, il se peut très bien qu'un sujet n'ait aucune idée que les données de son justificatif (par exemple, son numéro d'identification) ont été compromises.

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

Bien-fondé de l'approche consistant à supplanter les lois existantes. L'article 9 est largement inspiré de la Loi type sur les signatures électroniques et de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux, et semble se substituer aux dispositions des lois existantes qui définissent des exigences uniques pour l'identification dans des circonstances particulières. Dans le cas des signatures électroniques, l'approche générale consistant à supplanter toutes les autres lois existantes a bien fonctionné. Toutefois, le Groupe de travail voudra peut-être se demander s'il en va nécessairement de même pour l'identification d'un sujet. En effet, dans la mesure où certaines lois exigent une simple identification, tandis que d'autres sont très précises quant aux modalités et à la méthode d'identification (y compris des lois sur le respect de la vie privé, le principe « Connaissez votre client », le notariat, etc.), il ne serait peut-être pas opportun d'adopter une règle générale qui fasse reposer la conformité sur le simple respect d'une norme de fiabilité.

On peut avoir des doutes sur le fait qu'un processus d'identification général, même « fiable », satisfasse aux diverses exigences de l'ensemble des lois existantes en matière d'identification. En outre, si les parties à une opération commerciale ont

adopté leurs propres exigences concernant l'identification, un substitut électronique conforme à la norme générale de « fiabilité » pourrait ne pas être suffisant pour satisfaire aux exigences particulières ou uniques convenues par les parties.

Conflit potentiel entre articles. Par ailleurs, le Groupe de travail devrait examiner le conflit potentiel qui semble exister entre les articles 2-3 et 9. L'article 2-3 tient compte du fait que de nombreuses lois existantes imposent aux parties du secteur privé des exigences diverses en matière d'identification, en disposant ce qui suit : « Aucune disposition du présent [instrument] n'a d'incidence sur une exigence légale selon laquelle un [sujet] [une personne] doit être identifié[e] suivant une procédure définie ou prescrite par la loi. » Toutefois, l'article 9, qui prévoit l'application d'un modèle unique, semble être en contradiction avec cette disposition.

L'option A de l'article 9 s'énonce comme suit :

> « Lorsqu'une règle de droit exige ou permet l'identification d'[un sujet] [une personne], cette règle est satisfaite dans le cas de la gestion de l'identité si une méthode fiable est employée pour l'identification électronique de [ce sujet] [cette personne]. »

L'option B de l'article 9, similaire à l'option A, s'énonce comme suit :

> « Un sujet peut être identifié au moyen de services de gestion de l'identité si une méthode fiable est employée pour l'identification électronique de [ce sujet] [cette personne]. »

Étant donné que les différentes lois existantes prévoient des exigences très diverses concernant les processus d'identification, il ne paraît pas réaliste de vouloir appliquer le modèle unique prévu à l'article 9. Le problème, semble-t-il, vient en partie du fait que l'identification est traitée de la même façon que les signatures électroniques. Toutefois, si la création d'une signature électronique conformément à la Loi type satisfait aux exigences de toute loi qui requiert une signature, il n'en va pas de même pour les exigences liées à l'identification.

Les exigences légales d'identification d'une personne varient considérablement selon la loi considérée, l'objet de l'identification (identité fondamentale ou fonctionnelle) et l'importance de l'opération à effectuer. Par exemple, le règlement d'application de la loi californienne sur le respect de la vie privée des consommateurs, publié récemment, impose de nombreuses exigences d'identification aux fins de l'émission ou de la suppression de données personnelles à la demande d'une personne qui prétend être le sujet[4]. De même, dans le secteur financier, les règles relatives au principe « Connaissez votre client » imposent un certain nombre d'exigences précises en matière d'identification. Par conséquent, le Groupe de travail voudra peut-être également se demander si, ou dans quelles circonstances, il serait approprié d'adopter une formule globale unique pour indiquer que l'utilisation d'un système fiable permet de satisfaire à une exigence légale d'identification.

Le conflit existant entre ces deux dispositions illustre la difficulté de chercher à établir un ensemble de règles sur l'identité à l'aide de la même approche que celle déjà utilisée pour les signatures électroniques.

Caractère relatif de la fiabilité. En outre, il importe de se demander si l'article 9 tient suffisamment compte du fait que la fiabilité (de même que la sécurité) est un concept relatif. En effet, une méthode fiable dans un certain contexte peut ne pas l'être dans un autre. Par exemple, l'identification électronique d'une personne au moyen de Facebook ou Google est souvent suffisamment fiable si le but est simplement d'accéder à un compte sur un site Web, mais pas s'il s'agit d'autoriser l'accès à un compte bancaire et la réalisation d'un virement en ligne à partir de ce compte. Par conséquent, s'il devait maintenir l'approche consistant à faire reposer la validité

[4] Voir règlement d'application de la loi californienne sur le respect de la vie privée des consommateurs (California Consumer Privacy Act Regulations), article 4, disponible à l'adresse https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf?.

juridique sur la fiabilité, le Groupe de travail est encouragé à envisager de modifier le libellé de l'article 9 de façon à tenir compte du fait que le concept de « méthode fiable » est relatif. Il pourrait, par exemple, faire intervenir le concept de « fiabilité suffisante », déjà employé dans la Convention sur les communications électroniques, qui correspond au cas où la méthode utilisée est : i) soit une méthode dont la fiabilité est suffisante au regard de l'objet pour lequel l'identification a été demandée, 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 est suffisamment fiable.

Multiplicité des processus liés à la fiabilité. En faisant porter l'exigence de fiabilité uniquement sur la méthode employée pour l'identification électronique[5], l'article 9 semble également faire abstraction de tous les autres processus nécessaires à l'identification, qui pourraient également avoir une incidence sur la fiabilité du résultat, et des méthodes potentiellement utilisées pour leur mise en œuvre. Ces processus comprennent le contrôle d'identité, l'inscription, la sécurité des justificatifs, l'authentification, les logiciels, la sécurité des données, les employés, etc. Par exemple, il ne sert à rien d'employer une méthode objectivement fiable pour l'identification électronique d'une personne si le processus de contrôle d'identité n'est pas lui-même suffisamment fiable.

10. Article 10. Facteurs pertinents pour déterminer la fiabilité

L'article 10 présente uniquement les facteurs pertinents pour déterminer la fiabilité de la « méthode […] [d]'identification électronique »[6] mentionnée à l'article 9. Toutefois, il ne précise pas les facteurs à prendre en compte pour déterminer la fiabilité d'autres processus essentiels accomplis par un système de gestion de l'identité, comme le contrôle d'identité.

L'article 10 est axé sur quatre catégories de facteurs, à savoir :

- La conformité avec les obligations prévues à l'article 6 ;
- La conformité des « règles qui régissent l'exploitation du système de gestion de l'identité » aux normes et procédures internationales reconnues, notamment au cadre relatif aux niveaux de garantie ;
- Toute supervision ou toute certification fournie pour le système de gestion de l'identité ; et
- Tout « accord entre les parties ».

Toutefois, si les quatre types de facteurs énumérés ont trait à la conformité avec des règles ou des normes, à la certification et à l'existence d'un accord entre les parties, ils ne permettent pas nécessairement d'établir la fiabilité. Le fait que des règles et normes, une certification ou un accord existent et qu'un système de gestion de l'identité leur soit conforme ne signifie pas nécessairement que ce système est fiable pour un usage particulier. Par conséquent, si le Groupe de travail décide d'examiner les facteurs à prendre en compte pour déterminer la fiabilité d'une « méthode […] [d]'identification électronique », il voudra peut-être se demander à quels processus particuliers est liée la fiabilité (contrôle d'identité, inscription, sécurité des justificatifs, authentification, identification électronique, logiciels, sécurité des données, employés, etc.), puis chercher à déterminer quelles sont les règles ou normes qui permettent d'établir la fiabilité de chacun de ces processus.

Par ailleurs, comme le laisse supposer la liste précédente, les systèmes de gestion de l'identité font intervenir de nombreux processus distincts, dont chacun peut être mis

---

[5] Voir l'article 1 d) du projet de dispositions, qui définit l'identification électronique comme un « processus utilisé pour obtenir une garantie suffisante quant au lien unissant [un sujet] [une personne] à une identité ».

[6] Telle que définie à l'article 1 d), l'identification électronique se limite au « processus utilisé pour obtenir une garantie suffisante quant au lien unissant un sujet/une personne et une identité ». Elle ne couvre pas les nombreux autres processus nécessaires au fonctionnement d'un système de gestion de l'identité.

en œuvre à l'aide d'une ou de plusieurs « méthodes » de nature diverse, qui peuvent ou non être fiables. Ainsi, le fait d'établir qu'une « méthode […] [d]'identification électronique » est fiable ne garantit pas nécessairement que celle employée aux fins du contrôle d'identité sous-jacent l'est aussi.

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

Critères et compétences. L'article 11 donne à une personne ou autorité relevant du secteur public ou privé indiquée par l'État (désignée ci-après comme « **autorité responsable en matière de fiabilité** ») le droit de désigner les systèmes de gestion de l'identité considérés comme fiables. Toutefois, il n'énonce aucun critère qui permette de déterminer si celle-ci est compétente pour procéder à ce type de désignation. De plus, il ne donne aucune information concernant la procédure à suivre, hormis une exigence de prise en compte de toutes les circonstances pertinentes, y compris les facteurs énumérés à l'article 10, et une exigence générale de conformité aux « normes et procédures internationales reconnues de détermination de la fiabilité », sans donner de précision sur ces normes et procédures. Au vu de ce manque d'indication, on peut craindre que des autorités responsables en matière de fiabilité dépourvues des qualifications requises n'évaluent la fiabilité selon des critères inappropriés et que, partant, des systèmes de gestion de l'identité non fiables soient désignés comme fiables. En outre, il est probable que la désignation des systèmes de l'identité fiables soit très variable d'un État à l'autre, y compris pour un même système. Compte tenu de l'importance de cette désignation dans l'optique de l'article 9 (qui part du principe que les systèmes de gestion de l'identité désignés utilisent des « méthodes fiables », ce qui confère des effets juridiques à l'identification), cette situation pourrait causer des problèmes considérables.

Le Groupe de travail voudra peut-être également se demander comment les États évalueront la compétence de l'autorité responsable en matière de fiabilité et veilleront à ce qu'elle dispose des savoir-faire, des procédures et des ressources nécessaires pour désigner les systèmes de gestion de l'identité « fiables ». Il pourra se demander, par exemple, si l'autorité responsable en matière de fiabilité indiquée par l'État devrait faire l'objet d'une certification avant de se voir confier ce rôle.

Choix entre fiabilité des systèmes et fiabilité des opérations. Étant donné que la fiabilité est un concept relatif, il sera probablement nécessaire, pour l'évaluer, de se demander à quelle fin elle est requise. Se pose donc la question de savoir, avant toute chose, si le Groupe de travail devrait s'intéresser à la fiabilité des systèmes de gestion de l'identité en général (indépendamment du type d'opérations liées à l'identité qu'ils servent à effectuer) ou à la fiabilité des opérations de gestion de l'identité (qui permettent d'évaluer la fiabilité dans un contexte particulier).

Conflit entre la fiabilité des systèmes de gestion de l'identité et la fiabilité d'une « méthode […] [d]'identification électronique ». L'article 11 traite de la fiabilité des « systèmes de gestion de l'identité », tandis que l'article 9 vise à déterminer les effets juridiques de l'identification sur la base de la fiabilité de la « méthode […] [d]'identification électronique ». Ces deux approches semblent incompatibles, notamment en raison du fait que la fiabilité d'une méthode d'identification électronique n'est qu'une composante de la fiabilité de l'ensemble des fonctions d'un système de gestion de l'identité.

Questions pratiques. Au vu du rôle central que l'article 11 confère à l'autorité responsable de la fiabilité (et de l'importance que celle-ci revêt pour l'obtention des effets juridiques prévus à l'article 9), il paraît nécessaire de mettre en place, dans chaque État, un mécanisme institutionnel centralisé pour l'évaluation des systèmes de gestion de l'identité, et de faire intervenir les pouvoirs publics, au moins pour la sélection de l'autorité responsable en matière de fiabilité. Le Groupe de travail est encouragé à se demander si cette démarche pourrait être mise en pratique.

En outre, il voudra peut-être examiner la question de savoir si la nécessité pour les systèmes de gestion de l'identité d'être désignés comme fiables ne risque pas de créer une discrimination à l'égard des systèmes dont les opérateurs ne seront pas en mesure

d'assumer les dépenses liées au processus de désignation. Il voudra peut-être également étudier les questions suivantes :

- Quelle entité convient-il de désigner comme autorité responsable en matière de fiabilité ?
- Comment déterminer si une autorité responsable en matière de fiabilité est qualifiée et compétente ?
- Dans quelle mesure peut-on se fier à une désignation faite par une autorité responsable en matière de fiabilité (puisqu'il s'agit d'une évaluation faite à un moment donné) ? À quelle fréquence doit-on répéter le processus de désignation ?
- Les États devraient-ils s'occuper de la sélection des autorités responsables de la désignation des systèmes privés de gestion de l'identité, ou subordonner certains effets juridiques à l'obtention d'une désignation en tant que système fiable ?
- Cela aura-t-il pour effet, dans la pratique, d'imposer à tous les systèmes de gestion de l'identité une obligation de conformité aux normes sélectionnées par l'État ou l'autorité responsable en matière de fiabilité (puisque tous les opérateurs souhaiteront que leur système soit désigné comme fiable), et ainsi de freiner les évolutions ultérieures ?
- Quels sont les critères qui caractérisent une « norme internationale reconnue » ? Par qui une telle norme est-elle « reconnue » ? Que se passe-t-il en cas de modification de la norme ?
- Est-ce que l'évaluation de la conformité avec une norme sélectionnée et imposée pourrait nécessiter des procédures de certification coûteuses et complexes ?
- Quel est le lien entre les facteurs pertinents pour déterminer la fiabilité (art. 10) et les exigences relatives à la désignation des systèmes de gestion de l'identité fiables (art. 11) ?

Enfin, l'article 11 envisage la désignation des systèmes de gestion de l'identité indépendamment de l'emplacement géographique, et le Groupe de travail devrait se demander s'il ne sera pas dès lors nécessaire, dans la pratique, de chercher à obtenir la désignation d'un système de gestion de l'identité dans chaque État où les abonnés au système effectueront des opérations commerciales, et si cela ne risque pas d'entraver les opérations internationales.

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

Les dispositions du projet relatives à la responsabilité soulèvent un certain nombre de préoccupations que le Groupe de travail voudra peut-être examiner.

Hypothèse sous-jacente. L'article 12 (au moins les options B et C), de même que l'article 6, semble reposer sur l'hypothèse selon laquelle les mêmes règles peuvent s'appliquer à tous les systèmes d'identité. Toutefois, au vu de la diversité sans cesse croissante des systèmes de gestion de l'identité, que ce soit sur le plan du type, de l'objet, de la portée, des fonctionnalités, de l'exploitation, ou des rôles et responsabilités des entités participantes, il semble très peu probable que les règles prévues à l'article 6, ou celles ayant trait à la responsabilité prévues dans les options B et C de l'article 12, conviennent dans tous les cas. Pour le comprendre, il suffit d'observer les différences entre les systèmes d'identité traditionnels fondés sur les infrastructures à clefs publiques (ICP), les systèmes d'identité basés sur les chaînes de blocs, les systèmes d'identité axés sur l'utilisateur et les systèmes d'identité autosouveraine. Compte tenu des grandes différences existant entre systèmes de gestion de l'identité, toute approche normative en matière d'attribution des responsabilités risque de ne pas être adaptée à l'ensemble d'entre eux. Par conséquent, le Groupe de travail voudra peut-être se demander s'il convient d'adopter un modèle unique pour ce qui est de la responsabilité.

Rôles couverts. L'article 12 ne traite que de la responsabilité des prestataires de services de gestion de l'identité. Si le Groupe de travail parvient à la conclusion que le projet de dispositions devrait aborder la question de la responsabilité, il serait peut-être bon qu'il envisage de répartir les responsabilités entre toutes les entités participantes. Il pourrait notamment examiner la responsabilité des prestataires de services de gestion de l'identité, des agents d'inscription, des fournisseurs d'attributs, des fournisseurs d'identité, des sujets, des utilisateurs, des plateformes, des prestataires de services de vérification, des prestataires de services de confiance, des parties utilisatrices, etc. Il s'agit là d'un point important, car le fait de traiter la responsabilité liée à l'un des rôles du système ne permet pas d'atténuer ou d'éliminer les dommages qui pourraient découler d'un problème. Cela ne fait que transférer la perte subie à une autre entité participante. Le régime d'attribution des responsabilités devrait viser à déterminer qui doit assumer cette perte.

Droit de déni ou de limitation de la responsabilité. Le Groupe de travail voudra peut-être se demander si les prestataires de services de gestion de l'identité (ou d'autres entités participant au système) devraient avoir le droit de décliner ou de limiter leur responsabilité, par contrat ou d'une autre manière. Dans le cadre de l'option A, ce droit pourrait leur être accordé, au moins dans la mesure autorisée par la loi applicable. A priori, cette approche reconnaît qu'il existe de nombreux autres cas de figure et types de responsabilité pour lesquels les prestataires de services de gestion de l'identité ou d'autres entités pourraient légitimement chercher à décliner ou limiter leur responsabilité, et offre sur ce plan au moins autant de souplesse que la loi applicable.

Si l'option C donne bien aux prestataires de services de gestion de l'identité le droit de décliner leur responsabilité, elle est à cet égard de portée très limitée et n'offre aucune souplesse. Se pose en outre la question de savoir si, de manière générale, les dispositions des options B ou C interdisent aux prestataires de services de gestion de l'identité de dénier toute responsabilité (comme le ferait le plus souvent une entité publique).

Par ailleurs, dans la mesure où les options B et C limitent la responsabilité des prestataires de services de gestion de l'identité à un manquement aux obligations qui leur incombent en vertu de l'article 6, se pose la question de savoir comment cette limitation sera interprétée en cas de vol d'identité. Plus précisément, si un prestataire de services de gestion de l'identité identifie électroniquement un voleur d'identité ou lui délivre un justificatif sans enfreindre les dispositions de l'article 6, qui sera responsable de la perte ? Une victime de vol d'identité, qui n'a peut-être aucune interaction ou aucun contrat avec le prestataire, devrait-elle assumer la perte ?

Limitations de la responsabilité selon l'option C. L'article 12-3, tel que libellé dans l'option C, repose sur l'hypothèse selon laquelle : 1) il est possible de fixer des limitations concernant l'objet ou la valeur de telle ou telle opération liée à l'identité (sans toutefois qu'il ne soit précisé où ni comment sont imposées ces limitations) ; et 2) il est facile pour les parties utilisatrices de prendre connaissance de ces limitations avant d'utiliser le système de gestion de l'identité concerné. Cette hypothèse semble être une trace de l'approche adoptée à l'origine pour certains systèmes ICP, dans laquelle le certificat délivré par l'autorité de certification prévoyait une limitation de l'objet ou du montant des opérations, dont les parties utilisatrices étaient censées prendre connaissance avant toute utilisation. Compte tenu de la grande diversité des systèmes de gestion de l'identité actuels, le Groupe de travail voudra peut-être se demander s'il est possible de mettre en œuvre un régime de limitation de la responsabilité fondé sur les opérations. Il pourrait, par exemple, modifier le libellé de l'article de façon à indiquer qu'il est possible de prévoir ce type de limitations dans le cadre de confiance ou le contrat établi entre le prestataire de services de gestion de l'identité et les parties utilisatrices, plutôt qu'au niveau des opérations.

Interaction avec les systèmes publics. Enfin, le Groupe de travail voudra peut-être également examiner l'éventuelle interaction avec les systèmes publics de gestion de l'identité. Dans bien des cas, les prestataires de services de gestion de l'identité se

fient à des déclarations d'attributs faites par des tiers, tels que des systèmes nationaux de gestion de l'identité ou d'autres bases de données publiques (par exemple, les bases de données DMV). Puisque les systèmes publics de gestion de l'identité font souvent autorité, bien qu'ils refusent généralement d'assumer toute responsabilité en cas d'erreur, il conviendrait de se demander qui est responsable de la perte dans le cas où des informations d'origine publique présentent des erreurs. Il pourrait être nécessaire d'adopter une approche différente lorsque des entités publiques sont concernées.

Le Groupe de travail est instamment prié d'envisager de s'abstenir de toute tentative d'attribution des responsabilités, eu égard, en particulier, à la grande diversité des systèmes et processus de gestion de l'identité ainsi que des entités participantes. S'il décide de traiter la question de la responsabilité, le Groupe de travail est encouragé à indiquer les méthodes par lesquelles celle-ci peut être établie, mais à ne pas prescrire de normes, spécifications ou règles de responsabilité particulières. Ces méthodes peuvent faire référence, par exemple, à loi existante (comme dans l'option A) ou aux cadres de confiance que les parties à un système de gestion de l'identité adoptent par contrat.

13. Article 26. Reconnaissance internationale de la gestion de l'identité et des services de confiance

- Concernant la question de la « reconnaissance » internationale, le Groupe de travail voudra peut-être s'attacher à répondre plus précisément aux trois questions fondamentales suivantes : quel est l'objet de la reconnaissance ? Qui est chargé de la reconnaissance ? Quel est le but de la reconnaissance ?

- Quel est l'objet de la reconnaissance ? L'article 26-1 semble répondre à cette question en mettant l'accent sur les « systèmes de gestion de l'identité » et les « effets juridiques » de ces systèmes. Toutefois, il est difficile de savoir comment un système de gestion de l'identité peut avoir des effets juridiques, ou quels pourraient être les effets juridiques d'un tel système. Le fait de se fier aux processus de contrôle d'identité et d'identification électronique exécutés par un système de gestion de l'identité pourrait sans doute avoir des effets juridiques, mais il n'est pas évident de savoir comment un tel système pourrait être considéré comme ayant des effets juridiques en soi.

De manière analogue, les États reconnaissent les passeports délivrés par d'autres États en se fondant sur les normes de l'OACI. Chaque État reconnaît a priori la validité de ces normes, et peut ou non chercher à déterminer si le système d'émission de passeports de chaque autre État y est conforme, mais c'est le justificatif – c'est-à-dire le passeport délivré par le système de chaque État – qui produit des « effets juridiques » à la frontière.

- Qui est chargé de la reconnaissance ? On peut supposer que l'entité par laquelle est reconnu un système de gestion de l'identité étranger est : 1) soit une entité publique, par exemple un gouvernement ou un tribunal qui applique le système juridique ou légal pertinent (le but pouvant être de satisfaire à une exigence juridique de vérification de l'identité ou de déterminer si des preuves sont recevables devant un tribunal) ; 2) soit une partie utilisatrice (relevant du secteur public ou privé). Le projet d'article 26 met a priori l'accent sur la première option, puisqu'il fait référence aux « effets juridiques » de l'objet de la reconnaissance, quel qu'il soit. Par ailleurs, la seconde option n'exige pas de conclusion juridique ou légale, les parties utilisatrices étant certainement libres de décider elles-mêmes si elles reconnaîtront les systèmes de gestion de l'identité ou l'identité, ou si elles s'y fieront, aux fins de l'opération à laquelle elles procèdent, quelle qu'elle soit.

- Quel est le but de la reconnaissance ? Que signifie le fait qu'un « système de gestion de l'identité » est reconnu par la loi d'un État étranger ? L'idée de conférer des effets juridiques à un système de gestion de l'identité semble quelque peu déroutante. Par exemple, cela signifie-t-il que l'État étranger acceptera automatiquement les résultats d'une identification électronique

effectuée par le système reconnu, ou simplement que ce système pourra servir à réaliser des opérations dans l'État étranger, mais que ses processus devront éventuellement être modifiés pour satisfaire aux exigences juridiques que cet État impose à ses propres systèmes de gestion de l'identité ?

Le Groupe de travail devrait envisager de clarifier ce que signifie le fait qu'un système de gestion de l'identité exploité en dehors de [l'État adoptant] a les mêmes effets juridiques dans [l'État adoptant] qu'un système de gestion de l'identité exploité dans [l'État adoptant].

14. Article 27. Coopération

Le but de l'article 27 n'est pas clair. L'accent semble y être mis sur l'échange d'informations, de données d'expérience et de bonnes pratiques, ce qu'il n'y a certainement pas lieu de contester, cet échange devant même, idéalement, être encouragé, en particulier s'il est volontaire et ne suppose pas la négociation d'accords contraignants pour les entités qui ne sont pas parties à la coopération. Toutefois, le cas échéant, il ne semble pas nécessaire d'exiger que l'entité qui échange les informations soit indiquée par l'État adoptant comme compétente. En outre, il ne semble pas non plus nécessaire d'axer la coopération sur les trois aspects visés à l'article 27.

Si la coopération et l'échange étaient obligatoires, ou servaient de fondement à la reconnaissance juridique par un État ou à la négociation d'accords contraignants pour les entités non parties à la négociation, cela soulèverait probablement diverses préoccupations qui mériteraient un examen et des éclaircissements supplémentaires de la part du Groupe de travail.

Par ailleurs, il convient de noter que l'article 27 autorise (ou oblige) toute entité ou tout organisme indiqué par l'État adoptant comme compétent à coopérer avec des « entités étrangères ». Il est difficile de savoir à quoi fait référence le terme « entités étrangères » (s'agit-il du gouvernement étranger ? d'un prestataire de services de gestion de l'identité qui se trouve opérer sur le territoire de l'État étranger ? etc.). A priori, la coopération avec des « entités étrangères » devrait se limiter à celles qui sont également indiquées comme compétentes par l'État étranger.