Nations Unies A/CN.9/WG.IV/WP.120

Assemblée générale

Distr. limitée
27 juillet 2012
Français
Original: anglais

Commission des Nations Unies pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Quarante-sixième session
Vienne, 29 octobre-2 novembre 2012

Informations générales sur la gestion de l'identité

Document d'information présenté par l'équipe juridique spéciale sur la gestion de l'identité de l'American Bar Association

Note du Secrétariat

Dans le cadre des préparatifs de la quarante-sixième session du Groupe de travail IV (Commerce électronique), l'équipe juridique spéciale sur la gestion de l'identité de l'American Bar Association a soumis le document ci-joint au Secrétariat.

Le texte figurant en annexe est la traduction d'un document reproduit tel qu'il a été reçu par le Secrétariat.

V.12-55147 (F)

I. Introduction

1. En 2011, l'OCDE a noté dans un rapport que la gestion de l'identité numérique était fondamentale pour la poursuite du développement de l'économie Internet[1]. C'est une nécessité de base pour toutes les principales formes de commerce électronique.

2. Le présent document traite de la question de la gestion de l'identité, de son rôle dans le commerce électronique, des questions juridiques qu'elle soulève et des obstacles juridiques qu'elle entraîne[2]. Ce document, qui a été établi à partir des travaux menés par l'équipe juridique spéciale sur la gestion de l'identité de l'American Bar Association (ABA)[3], est soumis au Groupe de travail à titre informatif[4].

3. À sa quarante-quatrième session en 2011, la Commission est convenue de reconvoquer le Groupe de travail IV (Commerce électronique) pour entreprendre des travaux dans le domaine des documents transférables électroniques[5]. À cette occasion, elle est également convenue que l'extension du mandat du Groupe de travail aux autres sujets mentionnés dans les documents A/CN.9/728 et Add.1 en tant que sujets distincts (et non en raison de l'incidence qu'ils peuvent avoir sur les documents transférables électroniques) serait examinée à une session future[6]. Parmi ces autres sujets figuraient la gestion de l'identité, les guichets uniques et les paiements mobiles[7].

4. Comme il est dit plus loin (par. 6 et 7), la gestion de l'identité est une question fondamentale pour chacun des sujets que la Commission a examinés à sa quarante-quatrième session (documents transférables électroniques, guichets uniques et paiements mobiles). Elle occupe par conséquent une place importante dans les travaux que le Groupe de travail mène actuellement dans le domaine des documents transférables électroniques, ainsi que dans tous ceux qu'il pourrait mener sur les autres sujets.

---

[1] OCDE (2011) "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy — Guidance for Government Policy Makers" *OECD Digital Economy Papers*, No. 196, Éditions OCDE, p. 3; disponible à l'adresse www.oecd-ilibrary.org/science-and-technology/digital-identity-management-for-natural-persons_5kg1zqsm3pns-en.

[2] Le présent document met l'accent sur les systèmes de gestion de l'identité destinés à être utilisés dans un contexte commercial, notamment pour les relations entre entreprises (B2B), entre entreprises et administrations (B2G) et entre entreprises et consommateurs (B2C).

[3] Identity Management Legal Task Force, Cyberspace Law Committee, American Bar Association, Section of Business Law; http://apps.americanbar.org/dch/committee.cfm?com=CL320041. Les vues exprimées dans le présent document n'ont pas été approuvées par l'Assemblée des délégués, ni par le Conseil d'administration de l'American Bar Association. Elles ne doivent par conséquent pas être interprétées comme représentant l'opinion de l'ABA sur la question.

[4] On trouvera des renseignements supplémentaires dans la documentation relative au colloque de la CNUDCI sur le commerce électronique qui s'est tenu du 14 au 16 février 2011 à New York, que l'on peut consulter à l'adresse http://www.uncitral.org/uncitral/en/commission/colloquia/electronic-commerce-2010.html.

[5] *Documents officiels de l'Assemblée générale, soixante-sixième session, Supplément n° 17* (A/66/17), par. 250.

[6] Ibid., par. 251.

[7] Ibid., par. 241 à 249.

5. Il est largement admis que la gestion de l'identité est indispensable à la mise en place d'un système de commerce électronique digne de confiance. Actuellement, de nombreux organismes intergouvernementaux, États, groupes internationaux privés et entités commerciales étudient les questions et possibilités liées à la gestion de l'identité, élaborent des normes techniques et des procédures opérationnelles et examinent les moyens d'instaurer des systèmes d'identité viables. On mentionnera notamment les exemples suivants:

a) Parmi les organismes intergouvernementaux qui examinent activement les questions et les normes relatives à la gestion de l'identité figurent l'Organisation de coopération et de développement économiques (OCDE)[8], l'Organisation internationale de normalisation (ISO)[9] et l'Union internationale des télécommunications (UIT)[10];

b) Selon une enquête réalisée par l'OCDE[11], 18 pays membres de l'Organisation suivent activement des stratégies nationales de gestion de l'identité (Allemagne, Australie, Autriche, Canada, Chili, Danemark, Espagne, États-Unis d'Amérique, Italie, Japon, Luxembourg, Nouvelle-Zélande, Pays-Bas, Portugal, République de Corée, Slovénie, Suède et Turquie)[12]. Plusieurs autres pays, tels que l'Estonie, l'Inde et le Nigéria, déploient également des stratégies de ce type;

c) Plusieurs projets régionaux relatifs à la gestion de l'identité sont en cours dans l'Union européenne, notamment le projet PrimeLife (projet soutenu dans le cadre du septième programme-cadre de la Commission européenne)[13], le projet GINI-SA (Global Identity Networking of Individuals – Support Action)[14], le projet STORK (visant à créer une plate-forme d'interopérabilité européenne pour l'eID)[15] et le projet de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[16];

d) Les organisations privées suivantes examinent la question des normes et politiques relatives à l'identité à l'échelle internationale: OASIS (Organization for the Advancement of Structured Information Standards)[17], Open Identity Exchange (OIX)[18], Kantara Initiative[19], Open ID Foundation[20], tScheme[21] et Internet Society[22];

---

[8] http://www.oecd.org/fr/internet/economiedelinternet/digitalidentitymanagementandelectronicauthentication.htm.

[9] http://www.iso.org/iso/fr/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45306.

[10] www.itu.int/ITU-T/studygroups/com17/fgidm.

[11] Bernat, L. (2011), "National Strategies and Policies for Digital Identity Management in OECD Countries", OECD Digital Economy Papers, No. 177, Éditions OCDE. DOI: 10.1787/5kgdzvn5rfs2-en; disponible à l'adresse www.oecd-ilibrary.org/content/workingpaper/5kgdzvn5rfs2-en.

[12] Ibid., voir liste de liens indiqués par les différents pays aux pages 28 à 35.

[13] www.primelife.eu.

[14] http://www.gini-sa.eu.

[15] https://www.eid-stork.eu/pilots/pilot1_FR_more.htm

[16] http://www.enisa.europa.eu/

[17] www.oasis-open.org/home/index.php.

[18] www.openidentityexchange.com.

[19] http://kantarainitiative.org, anciennement connue sous le nom de Liberty Alliance, www.projectliberty.org.

e) Certains systèmes d'identité commerciaux ont été mis sur pied et fonctionnent à l'échelle mondiale dans des domaines limités. Il s'agit notamment des programmes gérés par TSCP (Transglobal Secure Collaboration Program)[23] et CertiPath[24] pour les industries de l'aérospatiale et de la défense, par l'association SAFE-BioPharma[25] pour l'industrie biopharmaceutique, par IdenTrust[26] pour le secteur financier, par CA/Browser Forum[27] pour les certificats EV-SSL, et par FIXs (Federation for Identity and Cross-Credentialing Systems)[28]. Les travaux menés par ces groupes mettent plus l'accent sur les normes techniques et les procédures opérationnelles que sur les questions juridiques.

II. Quelle est la relation entre la gestion de l'identité et le commerce électronique?

6. La gestion de l'identité est une question essentielle pour la plupart des opérations de commerce électronique et autres activités en ligne. Il est essentiel de pouvoir vérifier l'identité de parties éloignées géographiquement pour déterminer l'identité d'une personne qui cherche à accéder à une base de données en ligne contenant des informations sensibles ou à transférer des fonds en ligne à partir d'un compte, d'une personne qui a signé un contrat électronique, autorisé un envoi de produits à distance ou envoyé un courrier électronique. Si pour de nombreuses opérations en ligne qui présentent un risque modéré, on est disposé à croire que l'on traite avec une personne ou une entité donnée, lorsqu'il s'agit d'une opération plus sensible ou portant sur une valeur plus élevée, on a besoin de disposer d'informations précises et fiables sur l'identité de son interlocuteur avant de prendre une décision basée sur la confiance.

7. La gestion de l'identité joue un rôle clef pour les signatures électroniques, les documents transférables électroniques, et les autres domaines qui pourraient faire l'objet de travaux futurs (guichets uniques et paiements mobiles)[29].

a) La détermination de l'identité du signataire est l'une des conditions nécessaires à la création d'une signature électronique valable. Tant l'article 7 de la Loi type de la CNUDCI sur le commerce électronique (1996) que l'article 9 de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (2005, Convention sur les communications électroniques) exigent, pour qu'une signature électronique soit valable, qu'il soit utilisé une méthode pour identifier la partie, dont la fiabilité soit suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué. Quant à l'article 2 de la Loi type de la CNUDCI sur les signatures électroniques, il

---

[20] http://openid.net/foundation.
[21] www.tscheme.org.
[22] http://www.internetsociety.org/fr.
[23] www.tscp.org.
[24] https://www.certipath.com.
[25] www.safe-biopharma.org.
[26] www.identrust.com.
[27] www.cabforum.org.
[28] www.fixs.org.
[29] *Documents officiels de l'Assemblée générale, soixante-sixième session, Supplément n° 17* (A/66/17), par. 241 à 252.

définit le terme “signature électronique” comme des données pouvant être utilisées pour identifier le signataire;

b) La vérification de l’identité est aussi une condition essentielle pour les documents transférables électroniques, les guichets uniques et les paiements mobiles. La législation actuelle relative aux documents transférables électroniques exige que l’on détermine l’identité tant du signataire du document que du porteur qui est habilité à s’en prévaloir[30]. Les processus impliquant un guichet unique exigeront que l’on détermine l’identité du signataire des documents douaniers, ainsi que celle de la personne ou de l’entité qui les présente, et de la personne ou de l’entité habilitée à s’en prévaloir[31]. Quant aux systèmes de paiement mobile, ils exigent, à l’instar des autres systèmes de paiement, que l’on identifie (à des fins d’autorisation) la personne qui envisage de transférer des fonds[32].

III. Qu’est-ce que la gestion de l’identité?

8. Au départ, la gestion de l’identité vise à répondre à deux questions simples que toute partie à une transaction en ligne se posera au sujet de son interlocuteur: “Qui êtes-vous” et “Comment pouvez-vous le prouver”? La capacité de répondre à ces questions de manière fiable et crédible devient de plus en plus une exigence essentielle pour les activités commerciales électroniques, surtout pour les transactions dont la nature, l’importance et le caractère sensible sont importants. Avec les réponses à ces deux questions, une partie à une transaction en ligne peut décider si elle souhaite, ou non, poursuivre la transaction (par exemple conclure un contrat avec l’autre partie, l’autoriser à accéder à une base de données sensibles, ou lui conférer tout autre accès ou privilège).

9. Toute entité qui procède à des transactions numériques pourrait créer son propre système pour identifier et authentifier chacun de ses partenaires commerciaux (c’est le cas de nombreuses entreprises qui utilisent à la fois un processus d’enregistrement individuel et un système fonctionnant par nom d’utilisateur et mot de passe), mais cela devient de plus en plus cher et complexe et pose des difficultés lorsque le système compte de nombreux utilisateurs. De plus, en raison de la nécessité croissante d’une collaboration entre les organisations, des craintes en matière de sécurité, et du problème de la gestion des mots de passe des utilisateurs, le système traditionnel du nom d’utilisateur et du mot de passe émis par l’entreprise ou le vendeur ne répond plus aux besoins.

10. Par conséquent, on privilégie de plus en plus les systèmes d’identité dans lesquels un fournisseur d’identité tiers (ou fournisseur d’attributs) joue un rôle clef. L’objectif est de permettre à des entreprises ou administrations d’effectuer des transactions électroniques avec des parties à distance en se fiant aux informations relatives à l’identité et aux processus d’authentification fournis par un fournisseur tiers (il en existe plusieurs, qui ne sont pas liés entre eux). Ce système est connu sous le nom de “système de fédération d’identité”. En d’autres termes, les informations relatives à l’identité vérifiées par une entité sont mises à la disposition, de manière convenue et contrôlée, de nombreuses parties issues de divers systèmes

---

[30] A/CN.9/WG.IV/WP.115, par. 24 à 26 et 45 à 48.

[31] A/CN.9/728/Add.1, par. 42 et 45.

[32] Voir A/CN.9/728, par. 52.

qui ont besoin de ces informations pour diverses raisons. Cela permet, par exemple, à un particulier ou à une entreprise d'utiliser le justificatif d'identité de son choix pour effectuer des transactions en ligne avec de nombreuses entreprises, de la même manière qu'un particulier peut utiliser son permis de conduire pour toute une série de transactions hors ligne avec différentes entités, comme l'achat d'alcool, l'accès à la zone d'embarquement d'un aéroport, ou l'ouverture d'un compte en banque.

11. La mise sur pied d'un système de fédération d'identité nécessite une combinaison de normes et systèmes techniques[33], de procédures et processus commerciaux et de règles juridiques qui, pris ensemble, créent un système digne de confiance pour: i) vérifier l'identité et la relier à un particulier, une entité juridique, un appareil ou un objet numérique; ii) fournir ces informations relatives à l'identité à une partie qui en a besoin pour autoriser une transaction; et iii) gérer et protéger ces informations pendant toute la durée de leur cycle de vie. Pour qu'un tel système fonctionne dans un contexte commercial, il faut le doter d'un cadre juridique approprié, généralement de nature contractuelle, qui définit les droits et les responsabilités des parties, répartit les risques et prévoit les conditions d'exécution. Ce cadre juridique est souvent désigné par le terme de "règles de fonctionnement" ou de "cadre général de confiance".

IV. Fondements de la gestion de l'identité

12. Si le terme de "gestion de l'identité" est relativement nouveau, tel n'est pas le cas du concept qu'il recouvre. Les processus sous-jacents sont depuis longtemps utilisés dans l'environnement hors ligne. Les passeports, les permis de conduire et les cartes d'employé sont tous des éléments de systèmes d'identité (c'est-à-dire qu'ils sont des justificatifs émis par une entité pour permettre à des personnes qu'elle a identifiées de prouver leur identité). L'identification de la personne et l'émission d'un justificatif peuvent être effectuées par la partie qui accepte également le justificatif (c'est le cas d'une carte d'employé émise par l'entreprise), ou par un tiers (c'est le cas du permis de conduire ou du passeport). Dans les systèmes fédérés, où l'émetteur est un tiers, l'utilisation des justificatifs d'identité n'est pas limitée aux transactions effectuées avec l'entité d'émission. Au contraire, ces systèmes sont conçus pour que des justificatifs soient acceptés par des tiers (par exemple les services de sécurité dans les aéroports, une banque, ou un barman dans le cas d'un permis de conduire) exigeant qu'une personne prouve certains attributs de son identité (par exemple son nom ou son âge).

13. La difficulté consiste à reproduire des possibilités similaires dans un environnement en ligne. C'est-à-dire à créer un système permettant que des justificatifs numériques sûrs, fiables et dignes de confiance soient utilisés à distance par différents systèmes et entités (en d'autres termes, il s'agit de développer un système de fédération d'identité). Ainsi, les personnes concernées peuvent utiliser le même justificatif pour s'identifier afin d'accéder à des ressources ou d'effectuer des transactions avec plusieurs organisations.

---

[33] L'infrastructure à clef publique est l'une des approches qui peuvent être utilisées pour instaurer un système d'identité. Toutefois, de nombreuses autres technologies et approches sont en passe d'être développées et appliquées.

14. S'il existe de nombreuses approches différentes en matière de gestion de l'identité, elles recouvrent pour l'essentiel deux processus fondamentaux: i) le processus consistant à réunir et à vérifier certains attributs de l'identité d'une personne (ou d'une entité, d'un appareil ou d'un objet numérique)[34] et à émettre un justificatif reflétant ces attributs ("identification"); et ii) le processus consistant à vérifier, ultérieurement, qu'une personne présentant ce justificatif et affirmant être la personne identifiée précédemment est bien cette personne ("authentification"). Chacun de ces processus de base peut comprendre différents sous-processus, en fonction de la nature des données et du contexte dans lequel les deux processus se déroulent. Une fois que les attributs d'une personne ont été authentifiés, l'entité qui veut pouvoir se fier à l'identité ainsi authentifiée pour déterminer les droits et privilèges à accorder à cette personne (par exemple conclure un contrat avec elle, lui donner accès à une base de données ou à un compte bancaire en ligne) lance un troisième processus, qui constitue le processus d'□autorisation".

A. Identification

15. Le processus d'identification vise à répondre à la question suivante: "Qui êtes-vous?". Ce processus, qui est effectué par quelqu'un qui joue le rôle de fournisseur d'identité[35], consiste à associer certains attributs identifiants (tels que le nom, le numéro de membre, l'adresse ou la date de naissance) avec une personne de manière à l'identifier et à la définir de manière suffisante par rapport à l'objectif poursuivi. Ce processus, que l'on appelle aussi "confirmation de l'identité" ou "inscription", n'intervient généralement qu'une seule fois. Il consiste, pour le fournisseur d'identité, à réunir des informations sur la personne à identifier (le "sujet"). Pour ce faire, celui-ci se repose souvent sur divers documents émis par des administrations publiques (par exemple acte de naissance, carte de sécurité sociale, permis de conduire et passeport), ainsi que sur des justificatifs émis par des entités du secteur privé (par exemple badge d'employé, carte SIM de téléphone portable ou carte de crédit). Même si ces pièces d'identité et justificatifs ont été émis à d'autres fins, ils peuvent souvent être réutilisés ultérieurement pour faciliter un processus d'identification dans un contexte différent. C'est le cas, notamment, lorsqu'une personne présente un permis de conduire pour prouver son identité afin de recevoir un badge d'employé.

16. Au terme du processus d'identification, les attributs pertinents du sujet sont généralement représentés par des données intégrées dans un document électronique émis par le fournisseur d'identité, que l'on désigne par le nom de justificatif. Un justificatif présente (ou renvoie à) des données utilisées pour authentifier l'identité numérique ou les attributs supposés d'une personne, d'une entité ou d'un appareil[36].

---

[34] Des informations relatives à l'identité peuvent être réunies et vérifiées, et un justificatif d'identité peut être émis, pour des particuliers, des entités juridiques, des appareils ou des objets numériques. Le présent document met l'accent sur les systèmes destinés aux particuliers.

[35] Dans certains cas, lorsque quelques attributs seulement sont nécessaires au processus d'identification, une entité connue sous le nom de "fournisseur d'attributs" remplit cette fonction.

[36] Orientations de l'OCDE pour l'authentification électronique (2007), page 13, disponibles à l'adresse: http://www.oecd.org/fr/sti/economiedelinternet/recommandationdelocdesurl authentificationelectroniqueetorientationspourlauthentificationelectronique.htm.

Un justificatif peut se présenter sous plusieurs formes. Dans le monde réel, il peut prendre la forme d'un sceau royal, d'un permis de conduire, d'un passeport, d'une carte de bibliothèque ou d'un badge d'employé. Dans le monde virtuel, le justificatif peut aller du simple identifiant informatique au certificat numérique basé sur la cryptographie, qui peut être stocké sur un ordinateur, un téléphone portable, une carte à puce, une carte de retrait bancaire, une clef USB ou un dispositif similaire.

B. Authentification

17. Lorsqu'une personne présente un justificatif (que ce soit en présentant son permis de conduire à l'aéroport ou en saisissant son identifiant dans un réseau d'entreprise), prétend être la personne identifiée par ce justificatif, et cherche à exercer un droit ou un privilège accordé à cette dernière (par exemple embarquer dans un avion, accéder à un réseau d'entreprise ou à une base de données sensibles), la "partie en confiance" suit un processus d'authentification pour déterminer si cette personne est bien celle qu'elle prétend être. En d'autres termes, une fois que la personne a décliné son identité (en affirmant être la personne identifiée par le justificatif), l'authentification sert à répondre à la question suivante: "Comment pouvez-vous le prouver?". C'est un processus lié à une transaction donnée, qui consiste à associer une personne avec un justificatif pour vérifier que la personne qui essaie d'effectuer la transaction est bien celle qui a été précédemment identifiée au moyen du justificatif.

18. Le processus d'authentification nécessite généralement un élément permettant d'associer la personne au justificatif, que l'on désigne habituellement par le terme d'"authentifiant". Si le justificatif est un permis de conduire ou un passeport, l'authentifiant sera la photo et l'association sera effectuée en comparant celle-ci avec la personne qui présente le permis ou le passeport. Avec des justificatifs électroniques, l'authentifiant est généralement quelque chose que la personne concernée "connaît" (par exemple un mot de passe secret ou un numéro d'identification personnel), quelque chose qu'elle "possède" (par exemple une clef cryptographique privée, un objet physique tel qu'une carte à puce, un jeton USB ou autre type de jeton), ou quelque chose qu'elle "est", par exemple une caractéristique physique (photo, empreinte digitale ou autre donnée biométrique).

C. Autorisation

19. Une fois qu'une personne a pu être authentifiée, la partie en confiance peut utiliser son propre processus d'autorisation pour déterminer les droits et privilèges qui lui seront accordés (par exemple autoriser ou non cette personne à accéder à un site Internet, une base de données, un bar, ou à la zone d'embarquement d'un aéroport). Ce processus vise à répondre à la question suivante: "Qu'êtes-vous autorisé à faire?". L'authentification n'est donc pas une fin en soi. Elle sert souvent à faciliter les décisions qu'une partie en confiance prendra en matière d'autorisation, comme la décision d'octroyer des droits ou privilèges (comme l'accès à des ressources en ligne), ou d'effectuer une transaction. Ainsi, une fois que l'identité d'une personne qui cherche à accéder à un réseau informatique a été authentifiée, le propriétaire du système (c'est-à-dire la partie en confiance) peut utiliser un processus d'autorisation pour déterminer les droits d'accès qu'elle voudra

lui conférer. De même, une fois que l'identité d'une personne qui cherche à effectuer une transaction électronique (par exemple à conclure un contrat électronique) a été authentifiée, une partie en confiance peut utiliser un processus d'autorisation pour déterminer si elle souhaite ou non poursuivre cette transaction avec le sujet ou se fier autrement à la communication.

D. Fédération d'identité

20. Pour les transactions en ligne, l'identification et l'émission d'un justificatif sont généralement effectuées par la même partie que celle qui veut pouvoir se fier au justificatif. Ainsi, une entreprise identifiera un employé et lui attribuera un nom d'utilisateur et un mot de passe pour lui permettre d'accéder au réseau de l'entreprise. Dans ce cas, cette dernière agit à la fois en tant que fournisseur d'identité (puisqu'elle identifie la personne en tant qu'employé et émet un justificatif) et en tant que partie en confiance (puisqu'elle accepte ce justificatif, auquel elle se fie pour accorder un accès à son réseau).

21. Dans un système de fédération d'identité, les fonctions du fournisseur d'identité et de la partie en confiance ne sont pas nécessairement remplies par la même entité. Plutôt, de nombreuses parties en confiance non liées entre elles peuvent se fier à un justificatif émis par l'un quelconque de plusieurs fournisseurs d'identité, qui sont indépendants les uns des autres. Avec ce modèle, plusieurs organisations peuvent ainsi se fier à un seul justificatif, même si elles n'ont pas été directement impliquées dans l'émission de ce justificatif.

22. Un exemple bien connu de processus de gestion fédérée de l'identité dans le monde réel est celui du permis de conduire. Délivré par une administration publique, il est utilisé par diverses parties, non liées entre elles, qui s'y fient pour vérifier les attributs de l'identité de son titulaire. Ainsi, il peut être utilisé aussi bien par un agent de sécurité qui souhaite vérifier le nom d'une personne cherchant à pénétrer dans la zone d'embarquement d'un aéroport, que par un barman qui souhaite vérifier l'âge d'une personne commandant une boisson alcoolisée.

23. Un exemple en ligne de système de fédération d'identité est celui du réseau de distributeurs automatiques. Lors d'un retrait d'espèces, une personne détenant un compte à la banque A peut utiliser le justificatif d'identité émis par sa banque (sa carte de retrait) pour obtenir des espèces à un distributeur de la banque B (avec laquelle il n'entretient pas de relation). Afin d'autoriser cette transaction malgré l'absence de relation avec cette personne, la banque B contacte la banque A par le biais du réseau de distributeurs automatiques pour déterminer si cette personne est bien cliente à la banque A, demander à cette dernière d'authentifier l'identité de la personne (c'est-à-dire vérifier que elle a bien saisi le mot de passe correct) et obtenir certaines informations y relatives (par exemple la présence de fonds suffisants sur le compte pour couvrir le retrait, ainsi que le solde du compte pour que la banque B puisse indiquer cette information sur le reçu de la transaction).

IV. Risques liés à un système d'identité

24. Le fait de participer à un système d'identité et de se fier à des données relatives à l'identité comporte plusieurs risques potentiels:

a) Risque lié à l'identification: La fiabilité des informations réunies et vérifiées en relation avec le sujet est essentielle pour l'utilisation de tout système d'identité. Le risque lié à l'identification désigne le risque que des données relatives aux attributs de l'identité qui ont été réunies et associées à un sujet donné soient inexactes. Il est souvent fonction de la qualité des justificatifs d'identité physiques présentés par le sujet à des fins de vérification de son identité;

b) Risque lié à l'authentification: L'identification d'un sujet n'a pas de valeur à moins qu'une partie en confiance ne puisse l'authentifier (c'est-à-dire associer les attributs supposés au sujet correspondant). Les risques liés à l'authentification sont de deux types: risque qu'un sujet légitime ne puisse pas être correctement authentifié et risque qu'un processus d'authentification n'indique, à tort, qu'un imposteur est un sujet légitime;

c) Risque en matière de confidentialité: La gestion de l'identité d'un particulier implique qu'un fournisseur d'identité réunisse et vérifie des informations personnelles relatives à ce sujet et partage ces informations avec plusieurs parties en confiance. Par ailleurs, les transactions basées sur l'identité permettent de surveiller les activités d'une personne, ce qui génère des informations personnelles supplémentaires. Le risque en matière de confidentialité recouvre l'usage non autorisé, ou abusif, des informations personnelles relatives au sujet par une partie ayant accès à ces informations, ainsi que les obligations qui doivent être respectées en matière de traitement et de protection de ces données;

d) Risque lié à la sécurité des données: Dans tout système d'identité, il est indispensable de protéger les informations personnelles relatives aux sujets humains, ainsi que d'assurer la sécurité des processus nécessaires pour créer des justificatifs d'identité sûrs, communiquer des informations exactes sur l'identité, vérifier le statut des justificatifs et authentifier les sujets. On entend par risque lié à la sécurité des données le risque qu'un tiers non autorisé n'obtienne un accès à des données personnelles, ainsi que le risque que l'un des processus essentiels au fonctionnement général du système ou qu'une transaction relative à l'identité ne soit compromis;

e) Risque de responsabilité: Dans tout système d'identité, des erreurs se produiront inévitablement, entraînant des dommages. Les participants à un système d'identité doivent tenir compte du fait qu'ils risquent d'être jugés responsables de dommages subis par autrui du fait d'un problème qu'ils auront causé ou dont ils seront tenus juridiquement responsables. Un aspect clef du risque de responsabilité est l'incertitude juridique entourant la responsabilité liée à toute action ou inaction de la part d'un participant à un système d'identité, surtout si ce dernier opère sur plusieurs pays et secteurs d'activité;

f) Risque lié au défaut d'exécution: Le risque lié au défaut d'exécution et le risque de responsabilité sont complémentaires. Le risque lié au défaut d'exécution désigne le risque qu'un participant ne soit pas en mesure de faire valoir i) son droit au respect des règles par un autre participant, ou ii) son droit de toucher des

dommages-intérêts s'il subit un dommage et qu'un autre participant est tenu juridiquement "responsable". Il survient lorsqu'un problème se pose et que quelqu'un cherche à obtenir des dommages-intérêts. Il survient aussi lorsqu'un problème ne s'est pas encore déclaré, mais que le défaut d'exécution de la part d'un ou plusieurs participants risque de mettre tout le système en danger. C'est surtout important pour les systèmes qui couvrent plusieurs pays. Dans ce cas, le risque lié au défaut d'exécution vise à la fois la capacité de détecter ce problème et la capacité d'exiger que le participant concerné s'exécute ou se retire du système;

g) Risque en matière de respect de la législation: Dans de nombreux cas, la participation à un système d'identité soulève des questions en matière de respect de la législation par un ou plusieurs participants (c'est-à-dire la question de savoir si la conduite du participant est compatible avec la législation locale applicable). Dans d'autres cas, une entité participe justement à un système d'identité pour respecter les obligations juridiques qui lui incombent. Ainsi, un établissement financier peut participer à un système, et se fier à ses justificatifs d'identité, pour satisfaire à l'obligation juridique qui lui incombe d'authentifier correctement les personnes bénéficiant d'un accès aux comptes et aux possibilités de paiement en ligne. Dans de tels cas, la question est de savoir si cette participation satisfait aux obligations juridiques de l'entité concernée.

25. Comme dans tout système, les risques mentionnés ci-avant dépendent de la technologie utilisée, des différents processus mis en œuvre, et de la manière dont les participants s'acquittent – ou ne s'acquittent pas – de leurs obligations (voire de l'influence de tiers). Si l'on veut instaurer un système d'identité fiable, il faut prendre des mesures pour pallier ces risques, c'est-à-dire des mesures visant à promouvoir la confiance des participants dans la technologie utilisée (qui doit fonctionner correctement), les processus appliqués (qui doivent produire les bons résultats) et les autres participants (qui doivent s'acquitter correctement de leurs obligations).

V. Règles de fonctionnement

26. Pour faire fonctionner un système de fédération d'identité dans un environnement en ligne, tout en tenant compte des risques mentionnés ci-dessus, il faut non seulement utiliser la technologie appropriée, mais aussi exiger que tous les participants (par exemple sujets, fournisseurs d'identité et parties en confiance) respectent une série de normes techniques, d'exigences opérationnelles et de règles juridiques communes. Généralement, les systèmes d'identité commerciaux cherchent à atteindre cet objectif en élaborant des règles de fonctionnement appropriées (parfois désignées par le terme "cadre général de confiance"), auxquelles les participants sont liés contractuellement.

27. Les règles de fonctionnement d'un système d'identité comprennent deux catégories générales d'éléments: i) les règles et spécifications commerciales et techniques nécessaires pour que le système puisse fonctionner de manière fiable, et ii) les règles juridiques contractuelles qui, à côté des lois et réglementations applicables, définissent les droits et obligations juridiques des parties au système concerné et facilitent l'exécution si nécessaire:

a) Les règles de fonctionnement commerciales et techniques définissent les conditions nécessaires au bon fonctionnement du système d'identité, les rôles et les responsabilités opérationnelles des participants, et donnent des garanties suffisantes concernant l'exactitude, l'intégrité, la confidentialité et la sécurité de ses processus et données (pour qu'il soit digne de confiance et que les différentes parties soient disposées à y participer). Ces règles se fondent souvent sur des normes existantes;

b) Les règles juridiques contractuelles sont constituées par les accords contractuels liant les participants, qui définissent et régissent les droits et les responsabilités des parties en relation avec le système d'identité concerné, précisent les risques juridiques qu'elles assument en y participant (comme les garanties, la responsabilité en cas de perte, les risques pour les données personnelles), et prévoient des possibilités de recours en cas de différend entre les parties, y compris des méthodes de règlement des différends, des mécanismes d'exécution des décisions, des droits de résiliation, et le montant des dommages-intérêts, les peines et autres formes de responsabilité. Par ailleurs, elles rendent les règles de fonctionnement commerciales et techniques juridiquement contraignantes et exécutoires pour les participants.

28. Tant les règles de fonctionnement commerciales et techniques que les règles juridiques contractuelles sont soumises aux droits et obligations découlant des dispositions législatives et réglementaires applicables aux parties, sur lesquelles elles s'appuient généralement. Elles sont également soumises aux lois et règlements applicables dans le(s) pays où le système fonctionne ou est utilisé.

29. Les règles de fonctionnement applicables aux systèmes d'identité ressemblent aux règles de fonctionnement applicables aux systèmes de carte de crédit ou de paiement électronique. En effet, tous ces systèmes doivent pouvoir gérer de nombreux participants, dans de nombreux pays, conformément à un ensemble de règles communes. Ainsi, les règles de fonctionnement applicables aux systèmes de carte de crédit contiennent des dispositions relatives à l'émetteur, à l'organisme de traitement, au commerçant et au titulaire de carte, et définissent les spécifications et règles applicables aux participants à des opérations de crédit en ligne et au traitement y relatif[37]. De même, les règles de fonctionnement applicables aux systèmes de transfert électronique de fonds régissent les responsabilités de toutes les banques impliquées dans le processus de paiement ainsi que, dans une moindre mesure, des consommateurs ou autres payeurs impliqués, et définissent les spécifications et règles applicables aux participants lorsque des transferts

---

[37] Les règles de fonctionnement applicables aux systèmes de carte de crédit comprennent les spécifications et règles relatives à l'émetteur de la carte (voir par exemple le règlement de Visa International à l'adresse http://usa.visa.com/merchants/operations/op_regulations.html, ou les normes du secteur des cartes de paiement (PCIDSS) à l'adresse https://www.pcisecuritystandards.org/security_standards/index.php), qui sont contraignantes pour les organismes de traitement et les commerçants, ainsi que les contrats conclus entre les émetteurs des cartes et les organismes de traitement, ceux conclus entre les organismes de traitement et les commerçants, et ceux conclus entre les organismes de traitement et les titulaires de carte. Elles sont complétées par les lois et règlements applicables au traitement des cartes de crédit dans chaque pays.

électroniques de fonds (par exemple transferts SWIFT) sont utilisés pour faciliter le paiement dans une transaction en ligne[38].

30. S'il est généralement admis qu'il est nécessaire d'élaborer des règles de fonctionnement relatives aux systèmes d'identité contenant des règles juridiques appropriées, la phase d'élaboration elle-même laisse encore souvent à désirer. Il reste de nombreux obstacles et questions juridiques à recenser et à traiter.

VI. Législation régissant les systèmes d'identité

31. Dans la plupart des pays, il existe de nombreuses lois et réglementations qui auront des incidences réglementaires importantes (voire imposeront des obstacles, des exigences en matière de respect et et/ou prévoiront des risques de responsabilité) sur la participation à un système d'identité. En outre, les différences entre les législations des différents pays, examinées dans le contexte mondial d'Internet, créent un paysage réglementaire hétérogène qui peut rendre la structuration juridique difficile. Si certaines de ces lois et réglementations mettent spécifiquement l'accent sur les activités liées à l'identité, la plupart d'entre elles ont été élaborées dans un contexte qui n'avait rien à voir avec la gestion de l'identité (par exemple le droit des délits, le droit des contrats et le droit des garanties). Elles pourraient néanmoins avoir des incidences importantes, y compris des répercussions que personne n'avait anticipées lors de leur adoption.

32. Les catégories de lois suivantes sont applicables aux systèmes d'identité (ou aux participants à ces systèmes):

a) Lois régissant l'exactitude des informations relatives à l'identité: Les principales activités des systèmes d'identité sont la collecte et la vérification, par des fournisseurs d'identité ou d'attributs, d'informations relatives aux sujets, et la communication de certaines données aux parties en confiance. Il s'agit souvent de situations dans lesquelles l'exactitude et/ou la fiabilité de ces informations sont importantes. C'est pourquoi les lois qui contiennent des dispositions relatives à la fourniture d'informations fausses ou incorrectes, qu'elle soit intentionnelle ou résulte d'une négligence, ont des incidences sur les droits, les obligations et les responsabilités des participants à un système d'identité. On mentionnera notamment le droit des délits, qui régit l'assertion négligente et inexacte, la recommandation négligente et la diffamation, ainsi que le droit des garanties, les lois sur l'usurpation d'identité et les lois régissant les pratiques commerciales déloyales et trompeuses;

b) Lois régissant la confidentialité des informations relatives à l'identité: La gestion de l'identité implique, de par sa nature, qu'un fournisseur d'identité (ou son agent) réunisse des informations personnelles sur un sujet et les divulgue à une

---

[38] Les règles de fonctionnement applicables aux systèmes de transfert électronique de fonds comprennent les spécifications et règles relatives aux transactions de transfert électronique de fonds (voir par exemple les règles de fonctionnement et les directives de la NACHA, association américaine de paiements électroniques, à l'adresse http://www.nacha.org/), qui sont contraignantes pour les organismes de traitement et les commerçants, ainsi que les contrats conclus entre les commerçants et les payeurs individuels. Elles sont complétées par les lois et règlements applicables aux transferts électroniques de fonds, notamment la loi américaine pertinente (Electronic Funds Transfer Act and Regulation E).

partie en confiance[39]. Les lois sur la protection des données, les lois sur la confidentialité et les autres lois et réglementations régissant la collecte, l'utilisation, le traitement, le transfert et le stockage de données personnelles auront par conséquent des incidences importantes sur les activités liées à la gestion de l'identité. Si bon nombre d'entre elles ont été rédigées avant l'avènement des systèmes d'identité numérique et ne pouvaient pas, par conséquent, prévoir les processus particuliers, ni les dangers potentiels qui leur seraient associés, elles peuvent néanmoins avoir un impact direct sur ces activités;

c) Lois régissant la collecte d'informations relatives à l'identité: Tout comme les lois sur la confidentialité et sur la protection des données, les lois régissant la réutilisation des informations du secteur public ont des incidences sur les entreprises qui créent des produits d'information et des services à partir de données fournies par le secteur public. Elles peuvent créer des obstacles juridiques à l'utilisation à large échelle des données gérées par des administrations publiques dans le cadre des services liés à l'identité[40];

d) Lois régissant la sécurité des informations et processus relatifs à l'identité: De nombreuses législations imposent des obligations aux entreprises en matière de sécurité des informations personnelles (notion dont la définition varie dans les différents pays et en fonction de la législation applicable à un secteur donné) et des autres données en leur possession. En plus des lois et réglementations imposant l'obligation de prendre des mesures de protection des données, de nombreux pays ont aussi adopté des lois et réglementations qui imposent l'obligation de divulguer aux personnes touchées toute défaillance du système de sécurité impliquant leurs données personnelles;

e) Lois mettant l'accent sur le devoir d'identification: De nombreuses lois et règlementations exigent l'identification parmi d'autres éléments, en particulier dans un environnement électronique. Ainsi, la Convention sur les communications électroniques exige expressément l'identification en tant qu'élément d'une signature électronique juridiquement valable. En effet, elle prévoit, lorsque la loi exige qu'une communication ou un contrat soit signé par une partie, que l'exigence de signature est satisfaite 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[41];

f) Lois mettant l'accent sur le devoir d'authentification: Plusieurs lois régissent un ou plusieurs éléments de l'authentification. Certaines imposent aux entreprises le devoir d'authentifier les personnes avec lesquelles elles traitent à distance, d'autres régissent certains aspects du processus d'authentification. On mentionnera notamment l'exemple des autorités américaines de régulation bancaire, qui exigent l'authentification dans les activités bancaires en ligne. Ainsi, les établissements financiers qui proposent des produits et services sur Internet à leurs

---

[39] Sauf lorsque le sujet n'est pas un être humain (le sujet peut être par exemple une société, un appareil, un logiciel, etc.).

[40] Pour plus d'informations, voir le document intitulé "Global Networking of Individuals (GINI), Legal provisions for Deploying INDI Services" (5 octobre 2011), section 5, à l'adresse www.gini-sa.eu/images/stories/2011.11.06_GINI_D3.1_Legal%20Provisions%20for%20Deploying%20INDI%20Services_FINAL.pdf

[41] Article 9-3 de la Convention sur les communications électroniques.

clients sont tenus de recourir à des méthodes efficaces pour authentifier l'identité des clients qui les utilisent[42]. D'autres pays, tels que Singapour, ont adopté des exigences similaires[43];

g) Lois régissant expressément les activités des systèmes d'identité: Certains pays ont des lois qui régissent expressément certains aspects des activités liées à la gestion de l'identité. On mentionnera par exemple la Directive de l'UE sur les signatures électroniques[44], qui exige que les États membres réglementent la collecte, par certains fournisseurs d'identité (qu'elle nomme "prestataires de service de certification"), de données à caractère personnel et réglemente l'émission de justificatifs[45]. De même, la Loi type de la CNUDCI sur les signatures électroniques régit, aux articles 8 à 12, l'émission et l'utilisation des justificatifs d'identité requis pour la création de certaines signatures électroniques.

H. Difficultés et obstacles juridiques

33. Les catégories de lois et de réglementations présentées ci-dessus, ainsi que d'autres, soulèvent plusieurs difficultés fondamentales en ce qui concerne la création et le fonctionnement de systèmes d'identité du secteur privé. On mentionnera notamment les difficultés suivantes:

a) Inadéquation de la législation à la gestion de l'identité: Bon nombre de nouvelles questions soulevées par les processus liés à la gestion de l'identité ne sont tout simplement pas couvertes par la législation existante. La plupart des lois existantes qui s'appliquent dans ces contextes n'ont pas été rédigées pour des systèmes d'identité numérique et traitent souvent par conséquent les activités liées à l'identité de manière inadéquate ou inappropriée. Ainsi, la législation existante ne dit souvent rien au sujet de l'obligation de vigilance qu'une personne évaluant l'authenticité de justificatifs d'identité doit observer, ni au sujet de l'étendue de l'obligation de divulgation d'un fournisseur d'identité à l'égard d'un sujet;

b) Incertitude/ambiguïté juridique: Certaines questions liées à la gestion de l'identité sont traitées par les lois et réglementations existantes, mais l'applicabilité de ces dernières est souvent incertaine ou ambiguë, si bien que les participants à des systèmes d'identité sont confrontés à une grande incertitude juridique qui risque d'entraver la croissance, l'innovation et l'investissement. C'est pourquoi, même lorsqu'une loi existante s'applique à la gestion de l'identité, la manière dont elle s'applique à une question spécifique ou à une approche proposée dans un système d'identité n'est pas toujours claire. C'est surtout le cas de lois qui mettent l'accent sur une technologie spécifique. Cela peut limiter la capacité de parties cherchant à effectuer une transaction liée à l'identité à évaluer et à gérer les risques qu'elles prennent ce faisant;

---

[42] Federal Financial Institutions Examination Council ("FFIEC"), "Authentication in an Internet Banking Environment," 12 octobre 2005, p. 1; disponible à l'adresse www.ffiec.gov/pdf/authentication_guidance.pdf.

[43] Autorité monétaire de Singapour, circulaire n° SRD TR 02/2005, 25 novembre 2005.

[44] Directive 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, articles 6 à 8 et annexes I et II, disponible à l'adresse http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:FR:HTML.

[45] Article 8 de la Directive 1999/93/CE.

c) Questions de confidentialité: De par sa nature, la gestion de l'identité implique qu'un fournisseur d'identité réunisse des données personnelles sur un sujet et les divulgue à une partie en confiance. Pour participer à un système d'identité, les sujets doivent divulguer des informations personnelles et s'exposer ainsi au risque qu'il en soit fait un usage non autorisé ou inapproprié. En outre, dès lors que des sujets traitent avec de nombreuses parties en confiance, le fournisseur d'identité peut, en transmettant ou en vérifiant les informations les concernant, surveiller les activités de chacun d'entre eux, ce qui peut susciter des craintes quant à la collecte et à l'utilisation des données relatives à leurs transactions. La confidentialité est par conséquent un élément clef de tout système d'identité. Elle impose de se poser les questions suivantes: i) Quelles sont les informations qui peuvent être réunies par le fournisseur d'identité? ii) Quelles sont les informations qui peuvent être divulguées aux parties en confiance? iii) Quel contrôle le sujet peut-il exercer sur la divulgation des informations? iv) Quel doit être le niveau de sécurité requis pour les données gérées par les parties? et v) Quelles limites faut-il imposer à l'utilisation des informations par le fournisseur d'identité et les parties en confiance? Ces questions sont souvent traitées dans les lois existantes, qui peuvent par ailleurs être complétées par des règles de fonctionnement contractuelles;

d) Questions de responsabilité: Tout participant à un système d'identité se posera la question essentielle de savoir qui assumera la responsabilité liée aux risques visés au paragraphe 24 ci-avant. De nombreuses théories fondées sur le droit législatif, civil ou contractuel ont été avancées pour identifier, définir et préciser la source et l'étendue de ces responsabilités potentielles[46]. Ces risques juridiques restent toutefois souvent mal définis et incertains. Cette question de la responsabilité constitue un obstacle majeur à l'adoption, par le secteur privé, de solutions interopérables en matière d'identité. Dans bien des cas, la meilleure solution consiste à traiter cette question en élaborant des règles de fonctionnement ou un autre type d'accord contractuel entre les participants, solution qui permet en outre d'adapter le contrat en fonction des risques, qui varient selon le cas d'espèce;

e) Différences et conflits entre les pays: Il existe certains points essentiels sur lesquels les lois et réglementations existantes en matière d'activités liées à l'identité varient considérablement d'un pays à l'autre. C'est souvent le cas des lois régissant la responsabilité des participants et des lois de protection des données régissant la confidentialité des informations personnelles. De plus, dans certains cas, les modalités d'autorisation et de réglementation des activités liées aux systèmes d'identité posent des obstacles additionnels au fonctionnement de systèmes d'identité par-delà les frontières. Pour ce type de systèmes, la difficulté consistant à élaborer des règles de fonctionnement appropriées est encore aggravée par le fait que les lois et réglementations existantes varient (souvent sensiblement) d'un pays à l'autre;

f) Besoin d'interopérabilité juridique: Le fonctionnement des systèmes d'identité est compliqué par le fait que les lois applicables peuvent différer d'un pays à l'autre. On cherche souvent à remédier à ce problème en élaborant des règles

---

[46] Voir l'étude intitulée "*Certification Authority Liability Analysis*", établie pour le compte de l'American Bankers Association, qui examine les risques de responsabilité d'un fournisseur d'identité opérant en qualité d'autorité de certification. Elle peut être consultée à l'adresse http://64.78.35.30/article/ca-liability-analysis.pdf.

de fonctionnement qui prévoient l'interopérabilité juridique des systèmes. Or l'élaboration des règles ou des contrats requis pour uniformiser le rôle des participants entre les différents systèmes en ligne est rendue difficile par l'existence de différences entre les lois et réglementations des différents pays;

g) Restrictions à la capacité de modifier des dispositions par contrat: Certaines lois et réglementations existantes peuvent être modifiées par contrat. Ainsi, de nombreux textes législatifs incorporent des principes du droit des contrats ou du droit commercial tendant à définir des "règles par défaut", c'est-à-dire s'appliquant en l'absence d'un choix exprès des parties, qui peuvent être modifiées par accord entre les parties à la transaction. Dans un tel cas, les parties à un système d'identité sont libres de modifier les règles par défaut en les remplaçant par les règles de fonctionnement contractuelles appropriées. Dans d'autres cas, toutefois, les règles contraignantes prévues par la loi ne peuvent être ignorées par simple accord entre les parties, car elles répondent à des objectifs de politique publique, comme la protection des consommateurs ou des tiers.

34. Par conséquent, il arrive que les lois existantes créent des obstacles à la mise en place de systèmes d'identité efficaces, interopérables et fiables, capables d'opérer par-delà les frontières. Pour tenir compte de ces difficultés juridiques et réduire l'incertitude des participants, la meilleure méthode consiste à élaborer des règles de fonctionnement contractuelles régissant le système d'identité concerné. Cette méthode permet aussi d'expérimenter divers systèmes et approches pendant que le marché s'efforce, de son côté, de résoudre la question de la gestion de l'identité.

35. Tous les participants à un système de fédération d'identité ont intérêt à répartir justement, au préalable, les risques de responsabilité liés à la participation au processus, et à les limiter autant que possible. Tant que l'on n'examine pas la question de savoir comment répartir les responsabilités, et à qui faire porter les risques, les incertitudes juridiques constituent un obstacle majeur à la mise en place d'un système d'identité digne de confiance. Lorsqu'il s'agit de transactions plus importantes, entraînant des risques plus élevés pour les parties, il apparaît clairement que l'application de règles de fonctionnement appropriées, qui répartissent d'emblée les risques et les limitent dans la mesure du possible en attribuant des obligations à chaque participant, est avantageuse pour toutes les parties.

36. Le prochain défi consiste à mettre en place des systèmes d'identité du secteur privé qui soient interopérables et permettent d'effectuer des transactions commerciales par-delà les frontières. Il est probable que les règles de fonctionnement relatives à ces systèmes, tout comme celles relatives aux systèmes de carte de crédit ou de paiement électronique, seront de nature contractuelle, d'autant plus qu'ils sont destinés à être déployés sur Internet, au-delà des frontières nationales. Il pourrait être utile d'envisager une législation visant à éliminer les obstacles à ce type de systèmes, plutôt qu'à les réglementer.

* * *

DÉFINITIONS

[*Note: Les définitions suivantes sont générales et visent uniquement à faciliter la compréhension des pages qui précèdent*]

Attribut: Qualité ou caractéristique inhérente ou attribuée à un sujet, telle que nom, adresse, âge, sexe, titre, salaire, fortune, numéro de permis de conduire, numéro de sécurité sociale, etc. (pour un être humain), marque et modèle, numéro de série, emplacement, capacité, etc. (pour un appareil), etc. Synonyme: attribut d'identité.

Authentifiant: Élément servant à établir la relation entre un sujet et un justificatif. Il s'agit généralement d'un objet, d'une connaissance, ou d'une caractéristique de la personne qui permet de l'associer à un justificatif. Par exemple, un mot de passe constitue l'authentifiant d'un identifiant informatique, et une photo constitue l'authentifiant d'un passeport ou d'un permis de conduire.

Authentification: Processus consistant à vérifier l'identité déclarée par un sujet en confirmant son association avec un justificatif. Par exemple, la saisie d'un mot de passe en combinaison avec un nom d'utilisateur est réputée suffire à établir que l'utilisateur est bien la personne pour le compte de laquelle le nom d'utilisateur a été émis. De même, comparer la personne produisant un passeport à la photo qui y figure permet de vérifier ou de confirmer qu'elle est bien la personne décrite dans le passeport.

Autorisation: Processus consistant à octroyer des droits et privilèges à des sujets authentifiés sur la base de critères déterminés par la partie en confiance. Il vise à contrôler l'accès aux informations ou aux ressources de manière à ce que seules les personnes expressément autorisées puissent y accéder.

Fournisseur d'attributs: Entité de référence pour un ou plusieurs attributs de l'identité d'un sujet, qui est responsable des processus associés à la collecte et à la gestion de ces attributs. Un fournisseur d'attribut répond aux requêtes formulées par des fournisseurs d'identité ou des parties en confiance en confirmant des attributs fiables et validés. Il peut s'agir notamment d'un registre de la propriété, d'un bureau de crédit ou d'une base de données commerciale.

Fournisseur d'identité: Entité chargée d'identifier des personnes, entités juridiques, appareils et/ou objets numériques, d'émettre les justificatifs d'identité correspondants et de gérer ces informations pour le compte des sujets. (Synonymes: prestataire de service de certification, autorité de certification, fournisseur d'attributs (lorsque l'on ne dispose que de données limitées sur les attributs))

Gestion de l'identité: Processus, fonctions et capacités visant à réunir, vérifier, recouper et communiquer des informations sur l'identité d'un sujet à une partie en confiance, pour permettre à cette dernière de vérifier que ces informations correspondent à un sujet donné.

Identification: Processus consistant à réunir, vérifier et valider des informations suffisantes sur un sujet donné pour définir et confirmer son identité dans un contexte particulier. (Synonymes: inscription; confirmation de l'identité)

Identité: Informations relatives à un sujet donné, qui prennent la forme d'un ou plusieurs attributs permettant au sujet d'être identifié de manière suffisante dans un contexte particulier. Série d'attributs permettant à une personne d'être distinguée parmi d'autres dans un contexte donné.

Justificatif: Donnée présentée comme preuve de l'identité déclarée par un sujet. Les justificatifs papier comprennent les passeports, les actes de naissance, les permis de conduire et les cartes d'employé. Les justificatifs numériques comprennent les noms d'utilisateur, les cartes à puce et les certificats numériques.

Partie en confiance: Personne ou entité juridique qui se fie à un justificatif ou à une déclaration d'identité pour décider des mesures à prendre dans un contexte donné, qu'il s'agisse par exemple de traiter une transaction ou d'accorder un accès à des informations ou à un système. (Synonyme: prestataire de service)

Règles de fonctionnement: Procédures opérationnelles, spécifications techniques et règles juridiques contractuelles régissant le fonctionnement d'un système d'identité donné. Elles sont généralement élaborées par une entité privée (par exemple par l'opérateur du système d'identité) et rendues contraignantes pour les participants par voie contractuelle. (Synonymes: cadre général de confiance; règles du système; règles de fonctionnement communes; règlement de fonctionnement)

Sujet: Personne, entité juridique, appareil ou objet numérique identifié dans un justificatif donné, qui peut être authentifié par un fournisseur d'identité et dont ce dernier peut se porter garant. (Synonyme: utilisateur)

Système d'identité: Environnement en ligne servant à la gestion de l'identité régi par une série de règles de fonctionnement, dans lequel particuliers, organisations, services et appareils peuvent se faire mutuellement confiance parce que des entités de référence ont établi et authentifié leur identité respective.

Système de fédération d'identité: Système d'identité qui permet à un sujet d'utiliser le justificatif émis par l'un des multiples fournisseurs d'identité pour s'authentifier face à plusieurs parties en confiance non liées entre elles, dans différents systèmes.