Commissariat
à la protection de
la vie privée du Canada

Examen dirigé de la documentation :

Systèmes de gestion de l'identité

jennifer barrigar

Ce rapport a été commandé par le Commissariat à la protection de la vie privée du Canada

Février 2011

Table des matières

Contexte

De façon générale, on peut considérer qu'un système de paiement, et plus précisément le système de paiement du Canada, est une structure globale au sein de laquelle les consommateurs, les entreprises, les marchants, les institutions financières, les réseaux de paiements, les responsables de la réglementation, les transformateurs, les nouveaux arrivants et les fournisseurs de services se croisent au moment d'entreprendre, de traiter, de recevoir ou de réglementer des transferts de valeur dans le système.

Le Groupe de travail [canadien] sur l'examen du système de paiement a été créé en juin 2010 par le ministère des Finances du Canada. Son objectif est d'examiner le système de paiement canadien et de fournir des recommandations au ministère des Finances. On a estimé qu'un tel examen était nécessaire compte tenu des changements technologiques et technosociaux et de leurs répercussions potentielles sur l'utilisation et la portée du système de paiement. Par conséquent, on a demandé au Groupe de travail : (1) de dresser le plan du système de paiement existant au Canada; (2) d'exposer en détail les rôles de tous les joueurs; (3) de nommer les divers régimes de réglementation régissant les participants; (4) d'analyser les tendances et les changements importants des dernières années; (5) d'élucider tout type de paiement nouveau qui n'a pas déjà été traité de façon exhaustive. Dans une certaine mesure, il s'agissait d'un projet préliminaire, première étape d'un processus qui, au bout du compte, devrait mener à une consultation publique et à des recommandations par rapport aux changements jugés nécessaires ou souhaitables.

Avertissement : établissement d'une analogie entre le système de paiement et les systèmes de gestion de l'identité

Il convient de mentionner que le présent examen ne vise pas à soutenir que le système de paiement canadien est en soi un système de gestion de l'identité. Si nous définissons le système de paiement comme étant complexe par nature, comportant de multiples options de paiement et de multiples joueurs ayant parfois des objectifs divergents, des régimes de réglementation inexistants ou se chevauchant et des changements dans les choix offerts aux consommateurs, il devient toutefois évident que le système de paiement canadien doit être compris comme étant le reflet du sujet plus vaste des systèmes de gestion de l'identité ou, à tout le moins, comme étant analogues à ceux-ci.

Le CPVP a cerné la gestion de l'identité comme étant l'une de ses priorités pour cette année, et j'ai cru comprendre qu'il espère élaborer certains types de pratiques exemplaires et de documents de sensibilisation du public en matière de systèmes de gestion de l'identité. Afin d'assurer la constance de la position et de l'analyse, le CPVP a demandé que l'examen de la documentation soit axé sur les systèmes de gestion de l'identité en général plutôt qu'uniquement sur le système de paiement.

Mandat

Le Commissariat à la protection de la vie privée (CPVP) a l'intention de participer au processus d'examen. Je crois comprendre que la commissaire à la protection de la vie privée a déjà fait des présentations à l'intention du Groupe de travail au sujet du rôle important que la protection de la vie privée doit jouer dans un tel examen, et qu'elle a l'intention de fournir d'autres commentaires par écrit. À cette fin, elle a demandé qu'on prépare un examen quasi-dirigé de la documentation axé sur les questions de gestion de l'identité.

À la fin de l'examen, il y avait deux produits livrables : (1) un examen dirigé écrit de la documentation sur les systèmes de gestion de l'identité, et (2) une analyse de suivi avec l'effectif du CPVP dans le but d'examiner le document et les positions éventuelles du CPVP à l'égard de la gestion de l'identité.

En conséquence, le présent document porte sur : (1) les documents mentionnés par le CPVP comme étant essentiels dans le cadre de ce type de projet et (2) d'autres documents pertinents.

Introduction

À la lumière des données choisies au sujet des systèmes fédérés de gestion de l'identité, il devient rapidement clair que cette technologie a une qualité qui nous ramène presque à la théorie de Schrödinger[1], — c'est-à-dire que la gestion de l'identité en ligne, qui peut éventuellement mener à un état ou à un autre, peut être considérée simultanément comme étant incroyablement profitable et terriblement préjudiciable.

En théorie, un système fédéré de gestion de l'identité bien conçu et mis en œuvre peut améliorer la protection de la vie privée, favoriser un anonymat important et renverser la surveillance des comportements. Toutefois, il existe un risque tout aussi réel qu'un système fédéré de gestion de l'identité mal conçu et mis en œuvre exacerbe les problèmes existants et, en créant un nouvel inventaire de données et un nouveau processus d'échange, crée de nouveaux problèmes.

Contexte : systèmes de gestion de l'identité

Même si l'analyse récente de la gestion de l'identité se concentrait généralement sur les problèmes menant à la création de systèmes ou de protocoles en ligne de gestion de l'identité et sur les avantages éventuels de ceux-ci, dans les faits, il est important de reconnaître que la confirmation de l'identité et la confiance ne sont pas des questions propres aux environnements en ligne.

Dans le passé, les collectivités étaient petites et locales. Cela signifiait que, dans une relation, les participants étaient susceptibles de se connaître et qu'il y avait donc peu d'incertitude. Même quand les participants ne se connaissaient pas directement, les petites collectivités faisaient en sorte que les liens sociaux et de parenté de chaque personne étaient connus dans une certaine mesure et que, même si une personne était techniquement un étranger, elle était tout de même « connue » dans une certaine mesure, ce qui réduisait l'incertitude. En effet, non seulement la personne était « connue », mais, comme elle était membre d'une collectivité donnée, on pouvait s'attendre à ce qu'elle respecte un ensemble de normes reconnaissables. Cela, en retour, suscitait la confiance.

[1] Le chat de Schrödinger : un chat, une bouteille contenant un poison et une source radioactive sont placés dans une boîte scellée protégée de la décohérence quantique provoquée par l'environnement. Si un compteur Geiger interne détecte une radiation, la bouteille vole en éclats, relâchant le poison qui tue le chat. En mécanique quantique, l'école de Copenhague soutient que, après un certain temps, le chat est *simultanément* en vie *et* mort. Malgré cela, quand nous regardons dans la boîte, nous voyons le chat *non pas* mort *et* vivant, mais bien mort *ou* vivant.

Le terme « confiance » lui-même est extrêmement nuancé et peut être défini de nombreuses façons. Aux fins de notre examen, la définition la plus pertinente est la suivante : « Fait de croire, espérance ferme (en qqch.), foi (en qqn) assurance qui en découle[2] ». Essentiellement, la confiance nous permet de croire en la fiabilité de l'autre et, par conséquent, de croire que le résultat souhaité sera obtenu.

Toutefois, au fur et à mesure que les sociétés ont évolué et sont devenues plus complexes et plus dispersées, il est devenu plus difficile de se fier à des relations prolongées et à une coprésence, ce qui fait que la confiance est devenue plus difficile. L'absence de coprésence n'a pas réduit en conséquence la nécessité de procéder à de telles évaluations — elle l'a peut-être même augmentée. Au fur et à mesure que les sociétés deviennent de plus en plus complexes et dispersées, il est toutefois devenu moins possible de s'appuyer sur une coprésence pour en tirer des évaluations, ce qui fait que la coprésence a commencé à faire place à d'autres marqueurs de confiance.

> Les modes d'interaction ont commencé à changer radicalement dans les temps modernes, au moment où les transports et les communications ont permis aux gens d'être plus mobiles et où les institutions sociales ont contribué à modifier leurs relations. Cela a fait en sorte que la signature, par exemple, est devenue plus importante comme garantie d'identité légitime et a été acceptée par des organisations comme les banques. Ces organisations ont élargi la portée des actions humaines ou, de la même façon que des objets fabriqués comme le téléphone, nous ont permis de faire de plus en plus de choses à distance, sans la coprésence des parties de la relation. Une marque de confiance, comme un numéro d'identification personnel, est devenue le moyen permettant le type de confiance qui découle d'une relation suivie de personnes coprésentes[3].

La coprésence n'est que la moitié de l'équation. Si la coprésence crée une confiance parce qu'elle permet aux gens de se fier à leur propre évaluation de l'autre, un moyen de confirmer l'identité d'une personne ne répond pas pour autant à la question de savoir comment évaluer la mesure dans laquelle la personne dont l'identité a été confirmée est digne de confiance. Stephen Nock a écrit ce qui suit :

> Quand nous faisons un achat, par exemple, nous le faisons auprès d'étrangers, qui ont besoin d'une marque qui montre que nous sommes dignes de confiance et que nous avons les ressources pour payer. Mais cela soulève pleinement la question de savoir qui est digne de confiance si l'étranger — ou l'institution — n'a pas eu personnellement la possibilité de vérifier la réputation, les références et la crédibilité des personnes avec lesquelles il doit néanmoins interagir tous les jours[4].

Au moment où la diminution de la coprésence a exigé la création de moyens de vérification, la culture technologique urbaine de plus en plus anonyme (et rendue anonyme) exige de nouvelles formes d'identification et de reconnaissance.

Comme David Lyon le fait remarquer :

> Depuis les années 1960, les corps disparaissent à un rythme de plus en plus rapide. La communication et les technologies de l'information permettent non seulement des communications par télécopieur et par téléphone fixes, mais également des courriels, des transactions par carte de crédit, des cellulaires et Internet. Cela signifie que de nombreuses autres relations deviennent possibles sans coprésence. Les

---

[2] Confiance. *Le Grand Robert en cd-rom*, version 2.0, 2005.
[3] Extrait traduit de David Lyon, « Surveillance Society: Monitoring Everyday Life » (Open University Press, 2001), p. 15.
[4] Extrait traduit de Stephen Nock cité dans Lyon, « Surveillance Society », p. 21.

corps et l'expérience personnelle ne vont plus ensemble, et une part importante de cette expérience personnelle est sociale. Les liens qui nous lient ne sont pas les câbles électroniques ni les signaux satellites eux-mêmes, mais passent de plus en plus par l'intermédiaire des moyens électroniques. Au moment où ce genre de relations deviennent de plus en plus fréquentes, la quête de substituts aux modes d'intégration du passé s'accélère elle aussi[5].

Dans ces circonstances, il est peut-être compréhensible, compte tenu du fait que la simple dispersion géographique a nécessité la création de pièces d'identité comme moyens d'identification et d'authentification et a fait en sorte qu'on s'y fie, que la participation et la confiance accrues à l'égard des interactions en ligne pour des raisons personnelles, commerciales et même de gouvernance créent elles aussi le besoin d'un système de déclaration, d'authentification et d'autorisation d'identité. Par conséquent, quand nous parlons de gestion de l'identité (GID), nous parlons de ce genre de système[6], où « identité » signifie « une allégation ou un ensemble d'allégations au sujet de l'utilisateur[7] », l'authentification est le processus par lequel un certain niveau de confiance peut être établi au sujet de l'allégation faite[8] et l'autorisation est l'octroi de permissions ou de privilèges à l'identité confirmée[9]. Un système fédéré de gestion de l'identité est simplement un système où les fournisseurs de services peuvent se fier à des tiers de confiance choisis par l'utilisateur pour confirmer les services en son nom[10].

Dans le passé, cela se faisait face à face, c'est-à-dire entre un fournisseur de services et un utilisateur. Même si, provisoirement, cela suffisait peut-être, avec l'expansion du nombre d'utilisateurs, de fournisseurs de services et de demandes d'information et de renseignements fournis, le nombre de profils d'utilisateurs s'est multiplié, créant des désavantages pour les utilisateurs et les organisations. Pour les utilisateurs, les multiples écrans d'ouverture de séance, mots de passe et codes d'identification à mémoriser et les demandes de renseignements de divers niveaux et renseignements fournis pour chaque accès ne sont pas pratiques et prennent beaucoup de temps. Les organisations, elles, s'efforcent de limiter les coûts de la gestion et du stockage de ces profils[11] de même que la redondance des profils eux-mêmes[12].

Même s'il peut y avoir de nombreux joueurs, il y a au moins quatre (4) entités essentielles au sein d'un système fédéré de gestion de l'information :

UTILISATEUR : l'utilisateur final qui souhaite interagir avec un service en ligne.

AGENT DE L'UTILISATEUR : généralement un navigateur, c'est le moyen par lequel l'utilisateur interagit.

---

[5] Extrait traduit de Lyon, « Surveillance Society », p. 16.
[6] Center for Democracy & Technology, « Issues for Responsible User-Centric Identity », novembre 2009, version 1.0, http://www.cdt.org/files/pdfs/Issues_for_Responsible_UCI.pdf, p. 1 [en anglais seulement].
[7] Extrait traduit, CDT, p. 2.
[8] Clarke : Sufficently Rich Model of (id)Entity, Authentication and Authorization http://www.rogerclarke.com/ID/IdModel-1002.html#MAc [en anglais seulement].
[9] Clarke.
[10] CDT, p. 2.
[11] Surtout dans les administrations où il y a des lois sur la protection des données ou de la vie privée qui imposent des obligations à l'organisation à l'égard de cette information.
[12] G.-J. Ahn et J. Lam, « Managing Privacy Preferences for Federated Identity Management », dans V. Atluri, P. Samarati et A. Goto, *Chairs*, (2005) *Digital Identity Management '05: Proceedings of the 2005 ACM Workshop on Digital Identity Management* 28, <http://portal.acm.org/citation.cfm?id=1102492>, p. 28 [en anglais seulement].

FOURNISSEUR DE SERVICES OU PARTIE UTILISATRICE (FS/PU) : l'application ou le service en ligne avec lequel l'utilisateur souhaite interagir et qui exige une certaine assurance au sujet de l'utilisateur avant l'interaction.

FOURNISSEUR D'IDENTITÉ (FID) : une entité en ligne qui gère le processus d'authentification ou entrepose l'information sur l'utilisateur. Cette information peut être communiquée de diverses façons à différentes PU. Certains systèmes fédérés de gestion de l'information permettent l'existence de nombreux FID au sein d'un « cercle de confiance[13] ».

De la même façon qu'il peut y avoir de nombreux FID, il existe divers mécanismes reconnus dans la documentation pour structurer un système fédéré de gestion de l'identité : trois (3) qui sont universellement reconnus, et un quatrième (4e) qui est de plus en plus souvent ajouté à la liste.

1. Un système de gestion de l'identité intégré à un système d'exploitation, comme Cardspace de Microsoft[14];
2. Un système omni-directionnel et modulable, comme OpenID, qui s'appuie sur une source ouverte[15];
3. Le Security Assertion Markup Language (SAML) utilisé par les protocoles de la Liberty Alliance fournissent peut-être le métasystème de gestion de l'identité le plus diversifié et complet[16];
4. Les sites de réseaux sociaux, qui exercent de plus en plus une fonction (surtout dans le cas de Facebook et Twitter) de fournisseurs d'identité de fait pour de multiples PU[17].

Examen de la documentation : thèmes

En essayant de préparer un aperçu de la documentation examinée, on a cerné quatre principaux sujets :

1. Interroger l'utilisateur
    a. Conception axée sur l'utilisateur
    b. Anonymat, pseudonyme et dépersonnalisation
2. Sécurité et protections
3. Mondialisation et souveraineté des données
4. Réglementation

---

[13] S. Landau, H. Le Van Gong et R. Wilton, « Achieving Privacy in a Federated Identity Management System », dans R. Dingledine et P. Golle, *Eds.* (2009) 5628 FC LNCS 51, http://www.springerlink.com/content/b149n4u255u3n378/fulltext.pdf, p. 64 [en anglais seulement].
[14] E. Maler et D. Reed, « The Venn of Identity: Options and Issues in Federated Identity Management », (2008) mars/avril *IEEE Security & Privacy* 16, <http://www.xmlgrrl.com/publications/IEEESecPriv-MarApr2008-MalerReed-Venn.pdf>, p. 22 [en anglais seulement].
[15] Maler et Reed p. 21.
[16] Landau et coll.
[17] M. Melanson, « Facebook Wants to be Your One True Login », ReadWriteWeb.com, le 10 février 2010, en ligne : <http://www.readwriteweb.com/archives/facebook_wants_to_be_your_one_true_login.php>. Voir aussi CIPPIC Comments on OPC Draft Report on the 2010 Consultations on Online Tracking, Profiling and Cloud Computing, p. 12 [en anglais seulement].

L'examen dirigé de la documentation fait en sorte qu'il est évident que les documents au sujet de la GID et des systèmes fédérés de gestion de l'identité ne fournissent aucune solution facile à mettre en œuvre. En effet, les points de vue semblent inévitablement dichotomiques au sujet de chacun des thèmes cernés.

Interroger l'utilisateur

Conception axée sur l'utilisateur

Lorsque l'avantage du système fédéré de gestion de l'identité pour les utilisateurs individuels est expliqué, l'interface et l'affirmation de la détermination de l'utilisateur en matière d'information sont souvent mises de l'avant. La conception ou l'identité axée sur l'utilisateur dans un système permet à l'utilisateur de contrôler (l'accès à) ses pièces d'identité comme nous le faisons dans la vraie vie, conservant nos propres marques d'identité et choisissant celles que nous présentons et à qui[18].

Au niveau de l'interface, on s'attend à ce que cela entraîne des améliorations importantes de l'efficacité et de la convivialité à l'utilisateur. Celui-ci peut demander et attendre des solutions qui sont facilement comprises et accessibles, et le processus est simplifié en réduisant au minimum ou en éliminant l'exigence pour les utilisateurs de gérer de multiples noms d'utilisateur et mots de passe pour les divers services souhaités.

En abordant le système fédéré de gestion de l'identité du point de vue de l'utilisateur, les personnes ont (théoriquement) le pouvoir d'effectuer des transactions en ligne sans sacrifier leur vie privée, qu'ils effectuent des transactions avec un ou avec de nombreux fournisseurs de services. Non seulement l'utilisateur est en mesure de traiter avec de nombreux fournisseurs de services, mais, idéalement, il n'y a pas de fournisseur d'identité central unique, mais plutôt un éventail de fournisseurs offrant divers services, ce qui permet aux personnes de choisir le ou les nombreux fournisseurs qui répondent le mieux à leurs besoins. On soutient qu'une telle concurrence a pour effet non seulement de faciliter le choix de l'utilisateur, mais également d'améliorer la sécurité et la sensibilisation à la protection de la vie privée chez les fournisseurs d'identité, la compétition sur le marché encourageant et améliorant ces protections. Au sein des relations avec les fournisseurs d'identité individuels, le choix de l'utilisateur demeure plus facile, puisque celui-ci peut choisir les pièces d'identité qu'il présentera à un fournisseur de services donné sans craindre de s'identifier précisément lui-même à moins qu'il choisisse de le faire.

Au-delà du micro-niveau du choix de l'utilisateur, ses promoteurs soutiennent que la conception axée sur l'utilisateur continue d'être avantageuse pour l'utilisateur. Le système favorise la sécurité grâce à une identification et une authentification solides pour les transactions tout en offrant un stockage sécurisé des renseignements personnels des utilisateurs.

La protection des renseignements personnels de l'utilisateur est également plus facile, parce que la conservation des renseignements de l'utilisateur en lieu sûr protège la vie privée de l'utilisateur en empêchant les fournisseurs de services de recueillir, d'utiliser ou de communiquer des renseignements personnels autres que ceux requis, tout en s'assurant que l'information n'est pas liée ni liable à diverses sources à moins que l'utilisateur veuille ce qu'elle le soit.

[18] CDT, p. 2.

Malheureusement, l'analogie avec les pièces d'identité hors ligne se transposent de façon positive et négative. Le concept axé sur l'utilisateur peut faciliter le contrôle de l'utilisateur mais, ce faisant, peut aussi avoir des répercussions négatives sur les utilisateurs et être un fardeau.

D'abord, l'interface elle-même doit être utilisable et accessible. Reconnaissant que certains systèmes actuels exigent de l'utilisateur qu'il quitte la page Web pour ouvrir une séance ailleurs, on a suggéré qu'une approche axée sur l'utilisateur inclurait une interface constante pour en faciliter l'utilisation[19] et réduire les tentatives d'hameçonnage[20]. La constance ne devrait toutefois pas être un synonyme de simplification extrême faisant en sorte que les utilisateurs ne prennent pas des décisions rigoureuses[21].

Pour que l'autodétermination de l'information par les utilisateurs soit importante, ceux-ci doivent être en mesure non seulement de faire des choix, mais également de faire des choix éclairés et d'avoir les connaissances nécessaires pour le faire[22]. Comme diverses études l'ont montré, ce n'est pas toujours le cas. D'abord, les paramètres par défaut d'une interface seront très déterminants dans les choix des utilisateurs. Ceux-ci sont beaucoup moins susceptibles de refuser un paramètre par défaut que d'accepter quelque chose de différent. Par conséquent, quand les paramètres par défaut protègent les renseignements personnels et la sécurité, les utilisateurs seront plus susceptibles de demeurer à ce niveau ou même d'adapter les niveaux pour s'assurer des niveaux plus élevés de sécurité et de protection des renseignements personnels. L'expérience avec les sites des réseaux sociaux et diverses autres entités en ligne porte toutefois à croire qu'il ne faut pas nécessairement s'attendre à ce que les paramètres par défaut protègent les renseignements personnels. D'autres études ont permis d'examiner la compréhension qu'ont les utilisateurs des politiques de protection des renseignements personnels et des conditions d'utilisation et ont démontré que de nombreux utilisateurs ne lisent pas ces documents et que, même parmi ceux qui les lisent, le libellé leur est souvent inaccessible, ce qui laisse une compréhension confuse ou inexacte des paramètres de l'accord. Enfin, l'utilisateur doit avoir accès aux procédures et politiques de gestion fédérée de l'identité de même qu'à ses renseignements pour bien comprendre le sens de son consentement[23].

Même quand la compréhension ne pose pas problème, d'autres ont signalé que, même si, en théorie, ce type de micro-contrôle de l'utilisateur sur les renseignements est un élément positif, dans les faits, il peut entraîner une incapacité de faire des choix, une situation où l'utilisateur est submergé par les choix qui s'offrent à lui et devient incapable de prendre une décision. Même quand cela n'entraîne pas une paralysie, loin de faciliter l'auto-détermination de l'information, l'existence de nombreux choix et la responsabilité à leur égard peuvent faire en sorte que l'utilisateur revienne à son point de départ et se sente accablé par le système qui était censé simplifier ses relations en ligne[24].

---

[19] Maler et Reed, p. 21.
[20] R. Dhamija et L. Dusseault, « The Seven Flaws of Identity Management: Usability and Security Challenges », (2008) mars/avril *IEEE Security & Privacy* 24, <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4489846> p. 27 [en anglais seulement].
[21] Dhamija et Dussault, p. 26.
[22] Landau et coll., p. 64.
[23] K. Cameron, « The Laws of Identity », 12 mai 2005, Kim Cameron's Identity Weblog, <http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>, p. 6 [en anglais seulement].

[24] B. Masiello et A. Whitten « Engineering Privacy in an Age of Information Abundance », Intelligent Privacy Management Symposium, 2010, p. 122.

Anonymat, vie privée et dépersonnalisation

L'opposition binaire peut aussi être observée dans les documents concernant le rôle de l'anonymat, de la vie privée et de la dépersonnalisation. Fait intéressant, cette opposition semble s'appuyer non pas sur une critique des systèmes fédérés de gestion de l'identité eux-mêmes, mais plutôt sur des conceptions essentielles d'Internet. Autrement dit, là où Cameron soutient que le caractère identifiable est un élément essentiel qui a malheureusement été oublié par les architectes d'Internet et qui doit donc y être intégré de façon latérale[25], d'autres perçoivent l'absence de mécanisme d'identification comme étant essentiellement une libération[26] et peut-être même comme étant un élément essentiel de ce que Zittrain a appelé un « système génératif[27] ».

Cette différence à un niveau aussi essentiel ne peut que contribuer à former les différentes approches relatives aux questions entourant l'anonymat, la vie privée et la dépersonnalisation. Fait intéressant, toutefois, cette influence prend une forme assez différente de celle à laquelle on s'attendrait. En effet, ceux qui sont favorables aux systèmes fédérés de gestion de l'identité sont, dans les faits, ceux qui estiment que l'utilisation d'un pseudonyme est un élément positif facilité par les systèmes fédérés de gestion de l'identité et qui soutiennent que ceux-ci deviennent un outil important pour protéger la vie privée et contrer l'exploration et l'interception de données de même que l'établissement de lien entre les données[28]. Cependant, pour rendre cela significatif, les contrôles de chaque pseudonyme doivent être suffisamment précis pour permettre à l'utilisateur de choisir différents niveaux de suivi, de protection, etc. De la même façon, certains auteurs continuent de présenter les technologies et les stratégies d'anonymisation ou de dépersonnalisation comme étant une étape légitime dans la gestion de l'information[29].

À l'inverse, d'autres soutiennent qu'une hypothèse concernant les effets immunisateurs de l'anonymisation et de la dépersonnalisation a eu une incidence négative sur la protection des renseignements personnels, ce qui a entraîné des approches réglementaires axées sur le caractère identifiable et qui exclut de leur portée des renseignements dont le caractère identifiable a présumément été supprimé[30]. Même quand l'efficacité présumée du recours à l'anonymisation ou à la dépersonnalisation n'a pas eu de répercussion sur la portée du droit relatif à la protection des renseignements personnels, certains soutiennent que le langage de l'anonymisation et de la dépersonnalisation crée des dangers qui lui sont propres à de multiples niveaux, semblant décharger les organisations de leur responsabilité de protéger et de bien traiter l'information tout en encourageant, à tout le moins potentiellement, les personnes à abaisser leur garde à l'égard de leurs renseignements, présumant qu'ils sont à l'abri de la dépersonnalisation et de l'établissement de liens. Cela signifie que les organisations et les personnes sont plus susceptibles d'échanger des renseignements ou de

---

[25] Cameron, p. 1.
[26] *CPVP « L'identité, la protection de la vie privée et le besoin d'autrui de savoir qui vous êtes* », p. 4.
[27] Zittrain, « Future of the Internet and How to Stop It », cité dans L. Church et A. Whitten, « Generative Usability: Security and User Centered Design Beyond the Appliance » NSPW '09 Débat des ateliers de 2009 sur les nouveaux paradigmes de sécurité, p. 2 [en anglais seulement].
[28] Maler et Reed, p. 18.
[29] Privacy Analytics, « De-Identification: Reduce Privacy Risks When Sharing Personally Identifiable Information », 2009, Privacy Analytics Inc., <http://www.ehealthinformation.ca/documents/deidwhitepaper.pdf>, p. 9 [en anglais seulement].
[30] K. El-Emam et P. Kosseim, « Privacy Interests in Prescription Data, Part 2: Patient Data », dans E.M. Powers et R.L. Trope, *Eds.*, *Privacy Interests*, mars/avril 2009, <http://www.ruor.uottawa.ca/fr/bitstream/handle/10393/12985/El_Emam_Khaled_2009_Privacy_interests_in_prescription_data_2.pdf>, p. 75 [en anglais seulement].

consentir à leur communication avec la fausse impression qu'ils n'ont pas à s'en inquiéter. Comme Ohm l'explique en détail, la « sécurité » putative accordée par l'anonymisation ou la dépersonnalisation est non seulement illusoire, mais dangereuse. La repersonnalisation est de plus en plus possible, non pas seulement parce que de plus en plus de données sont publiquement accessibles et parce que nous travaillons avec des ordinateurs de plus en plus puissants, mais également parce que les techniques de repersonnalisation ne sont pas aussi complexes que les utilisateurs aimeraient le croire et parce que la repersonnalisation et l'établissement de liens sont associés à d'importants incitatifs financiers[31].

Sécurité et protections

Là encore, au chapitre de la sécurité et des protections, le système fédéré de gestion de l'identité semble susciter différentes réactions.

Au niveau de l'infrastructure pure et simple, il faudrait admettre qu'il y a des difficultés technologiques et procédurales inhérentes à la mise en place d'un tel système, surtout un système qui est, par définition, inter-opérationnel et modulaire. De la même façon, il y a des enjeux économiques liés aux coûts du déploiement, de la coordination et de l'utilisation des systèmes fédérés de gestion de l'identité. Ces préoccupations doivent être admises au moment de prendre en considération les questions liées à la sécurité et à la protection pour la simple raison que ces deux facteurs exerceront une pression supplémentaire sur ceux qui cherchent à concevoir et à mettre en œuvre (ou même à joindre) un système fédéré de gestion de l'identité. Ce qui accentue cette pression, c'est le fait que, même après que l'infrastructure a été payée et créée, cela accroît plutôt que de régler les questions relatives à la sécurité et à la protection qui sont soulevées.

Avant tout, même si le système fédéré de gestion de l'identité est présenté avec insistance comme étant un système qui protège la vie privée et qui offre une sécurité accrue, il faut admettre qu'il s'agit en fait d'un modèle s'appuyant sur la collecte, l'entreposage, l'utilisation et la transmission d'information et que, par conséquent, il y a des risques inhérents pour l'utilisateur, le fournisseur d'identité et le fournisseur de services. De plus, le fournisseur d'identité et le fournisseur de services ont peut-être besoin eux aussi de connaître les normes de réglementation pour la protection et la conservation en lieu sûr de l'information.

La négociation de ces différents intérêts et risques peut être angoissante. Toutefois, il est également possible de voir cette situation comme étant analogue au nuage et à la circulation transfrontalière des données et, par conséquent, qu'elle est idéale pour négocier un ensemble clair de règles, d'obligations, d'attentes et de permissions contractuelles afin de protéger toutes les parties et de fournir un cadre clair pour gérer l'information de façon appropriée.

Une fois la gestion des renseignements de base abordée, le processus d'authentification qui est la clé du système fédéré de gestion de l'identité doit être vu comme comportant des risques qui lui sont propres. L'efficacité du système fédéré de gestion de l'identité est mesurée, au bout du compte, en fonction de l'efficacité et de la fiabilité de l'authentification. Là encore, à ce niveau, nous pouvons voir que toutes les principales parties sont concernées : l'utilisateur et le fournisseur de services souhaitent une authentification appropriée et efficace, et le fournisseur de services et le fournisseur d'identité doivent trouver un équilibre entre le besoin de garantir que l'information échangée est exacte et pertinente et leur tentative de structurer leur utilisation et leur stockage de l'information de façon à limiter leur responsabilité.

[31] P. Ohm, « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization », 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 [en anglais seulement].

Là encore, cela ne doit pas être une préoccupation rendant automatiquement le système fédéré de gestion de l'identité irréalisable — au contraire, il peut aussi être négocié par les parties et, comme nous le verrons dans une autre section, il peut éventuellement être formé par des approches de réglementation et de gouvernance.

Tel qu'il a été mentionné précédemment, le fournisseur de services et le fournisseur d'identité doivent aussi faire des efforts pour se protéger et protéger leurs processus de la responsabilité qui pourrait découler d'une identification ou d'une authentification frauduleuse, de procédures ou d'une sécurité inadéquates pour protéger l'information et son utilisation ou même contre la mauvaise utilisation ou utilisation abusive de l'information qui leur a été confiée. En plus de rendre le fournisseur de services ou d'identité responsable, ces situations rendent aussi l'utilisateur vulnérable à un éventail de conséquences, comme le vol d'identité, la communication inappropriée ou même le refus d'accès aux services souhaités.

Enfin, surtout à la lumière de l'investissement économique dans l'infrastructure, les parties doivent aussi être conscientes d'un devoir de protéger davantage que l'information — à un certain niveau, il y a une obligation de protéger le système fédéré de gestion de l'identité lui-même. Le système doit avoir une vaste distribution pour être efficace, et toutes les parties du système doivent pouvoir faire confiance aux autres parties pour que le processus soit efficace. Par conséquent, la question des protections et de la sécurité doit être comprise à l'échelle du système, et chaque acteur doit être préoccupé non seulement par la protection de ses propres intérêts, mais également par le maintien de l'intégrité de l'ensemble[32].

Fait intéressant, c'est aussi une situation où, loin d'invalider le système fédéré de gestion de l'identité, l'attention appropriée accordée à ces problèmes pourrait non seulement les régler, mais également, par le fait même, renforcer le système fédéré de gestion de l'identité et contribuer à la création des avantages que ses partisans lui attribuent. L'utilisation appropriée de certaines formes d'analyse des répercussions sur la vie privée pour confirmer tous les risques possibles associés à l'information, par exemple, mène naturellement à l'application des principes de conception visant à protéger les renseignements personnels[33] pour veiller à ce que la conception de l'infrastructure, qui, sur les plans des composantes et du modèle dynamique plus vaste, vise à aborder ces risques, peut offrir une bonne protection contre ceux-ci ou les atténuer.

Mondialisation et souveraineté des données

La portée et l'incidence mondiale des systèmes fédérés de gestion de l'identité démontrent une fois de plus la double nature qui est constamment présente dans la documentation concernant la gestion de l'identité. Si l'on tient compte du fait que la confiance par authentification du marqueur d'identité est endémique aux systèmes diversifiés sur le plan géographique, il n'est pas surprenant que de nombreuses personnes présentent avec insistance la gestion de l'identité comme étant un élément qui contribuera à la mondialisation du commerce, qui facilitera l'accès à l'information et le commerce et qui simplifiera les interactions en ligne. Si un grand nombre de ces recommandations semblent bien connues, c'est parce que les termes dans lesquels la gestion de l'identité est analysée dans ce contexte rappellent la documentation concernant l'infonuagique.

---

[32] T.J. Smedinghoff, Federated Identity Management: Balancing Privacy Rights, Liability Risks, and the Duty to Authenticate (21 août 2009). Accessible à SSRN : http://ssrn.com/abstract=1471599, p. 15-24 [en anglais seulement].
[33] Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario, Submission of the Information & Privacy Commissioner, Ontario, Canada — Response to the FTC *Framework for Protecting Consumer Privacy in an Era of Rapid Change, p.* 2.

L'établissement d'un lien entre la rhétorique relative à la mondialisation et l'infonuagique ne devrait pas être considéré comme étant un rejet de l'importance de la gestion de l'identité. En effet, le « Plan pour un Canada numérique[34] » de juin 2010 établit un certain nombre de thèmes clés[35], qui sont tous, sans doute, en accord avec la création et le soutien des systèmes fédérés de gestion de l'identité au Canada. Pour faire cela, il faut reconnaître que la technologie atténue les frontières géographiques et réduit leur signification, de nombreuses nations numériques et économies de l'information convergeant vers les espaces en ligne.

Compte tenu de ce reflet, il n'est pas surprenant qu'un grand nombre des préoccupations que nous connaissons dans le domaine de l'infonuagique soient soulevées relativement à la gestion de l'identité. Tel qu'il a été mentionné précédemment, la base d'un système fédéré de gestion de l'identité est en fait la collecte, l'entreposage, l'utilisation et l'échange d'informations dans des réseaux. Cela, en retour, soulève de nombreuses préoccupations. La nature de plus en plus mondiale d'Internet, par exemple, soulève des préoccupations concernant les instances responsables, pour ce qui est de la réglementation de l'espace et de l'accès à la justice. Comme il a été mentionné dans la section concernant la sécurité et les protections, les différentes méthodes de stockage de l'information suscitent aussi des préoccupations concernant la protection des renseignements eux-mêmes à l'aide des bonnes mesures de protection, limites d'utilisation et méthodes de conservation de même que la nécessité de droits d'accès et de mesures correctives. Enfin, de la même façon qu'on s'en préoccupe de plus en plus au moment de gérer la sous-traitance du stockage de l'information, l'éventualité qu'un tiers ait accès à l'information suscite des préoccupations, tout comme la nécessité de s'assurer que les protections appropriées sont en place pour que l'information soit non seulement en sécurité pendant sa transmission aux fournisseurs d'identité et par celui-ci, mais qu'elle soit entreposée par l'organisation du fournisseur d'identité d'une façon qui ne permette pas la manipulation ou l'exploration des données à la recherche de liens ou de nouveaux renseignements.

La souveraineté des données suscite des préoccupations semblables à celles relatives à la mondialisation, qui sont parfois soulevées relativement au système fédéré de gestion de l'identité. Ces préoccupations ont aussi une double fonction — les préoccupations relatives à l'influence d'états étrangers sur les données canadiennes liée au fait qu'elles se trouvent dans un espace virtuel et la préoccupation de plus en plus importante concernant l'appartenance des télécommunications à des intérêts étrangers pour ce qui est de conserver la propriété canadienne, de filtrer et d'inspecter la circulation des données au Canada[36].

Gouvernance et réglementation

Fait intéressant, l'un des seuls domaines dans lesquels la documentation semble homogène est l'accord au sujet de la nécessité d'une gouvernance des systèmes fédérés de gestion de l'identité qui va au-delà de la simple technologie de même que les suggestions concernant l'approche qui serait la plus efficace.

---

[34] Comité sénatorial permanent des transports et des communications. Plan pour un Canada numérique, juin 2010, à http://planforadigitalcanada.ca/index.php?option=com_content&view=article&id=4&Itemid=13&lang=fr .
[35] Encourager l'innovation, mettre en place une infrastructure de classe mondiale, développer le secteur de la technologie et faire en sorte que le Canada soit en position pour réussir sur le plan numérique maintenant et dans l'avenir. Plan pour un Canada numérique, p. 14.
[36] M. Moll, « Trading Sovereignty for Surveillance » Centre canadien de politiques alternatives (décembre 2010) http://www.policyalternatives.ca/publications/monitor/trading-sovereignty-surveillance [en anglais seulement].

Premièrement, l'aspect mondial d'un système fédéré de gestion de l'identité (à l'échelle internationale et nationale) garantit que ces systèmes, s'ils sont réglementés, seront probablement régis (couverts) par un ensemble de politiques organisationnelles concernant la protection des renseignements personnels, une situation qui peut créer de l'incertitude pour toutes les parties visées. En conséquence, dans la documentation, il existe un accord clair concernant la nécessité d'une méthode homogène de gouvernance et de réglementation de ces systèmes pour assurer la confiance et la convergence entre les participants au système à tous les niveaux[37].

Ce besoin de faire régner la gouvernance n'est pas simplement le produit d'un désir de fiabilité. Cela nous ramène plutôt à la reconnaissance du fait que tous les membres du système ont le devoir non seulement de protéger leurs intérêts, mais également de soutenir le système dans son ensemble. Dans le cas d'un système fédéré de gestion de l'identité, nous comprenons intuitivement que la gouvernance visant à soutenir ou à protéger un seul des intérêts (qu'il s'agisse de l'utilisateur, du fournisseur de services ou du fournisseur d'identité) ne serait pas viable et ne fournirait pas l'expansion nécessaire à la réussite du système fédéré de gestion de l'identité. Les préoccupations et les intérêts légitimes de toutes les parties doivent être reconnus et abordés de façon appropriée dans un système de gouvernance[38]. En conséquence, on a entendu l'appel à l'élaboration d'un cadre de gouvernance qui préserverait les intérêts de tous et constituerait une base de protections auxquelles un utilisateur d'un système fédéré de gestion de l'identité, ou le système lui-même, pourrait raisonnablement présumer qu'il a droit et qu'il pourrait présumer qu'il les reçoit[39]. À cette fin, de nombreuses personnes ont laissé entendre qu'un projet de gouvernance approprié doit commencer avec quelque chose qui ressemble à une évaluation des facteurs relatifs à la vie privée → à une analyse minutieuse des intérêts de toutes les parties à l'égard du système afin de commencer à structurer un cadre pouvant satisfaire ces intérêts et trouver un équilibre entre ceux-ci. Cette approche comporte de nombreux avantages : non seulement elle garantit une approche minutieuse et équilibrée, mais elle facilite aussi la mise en place d'un système fédéré de gestion de l'identité qui est équilibré et responsable de façon ascendante, au lieu de continuer à se fier à des méthodes ou technologies dépassées simplement parce qu'on les connaît bien[40].

La documentation révèle certains principes de conception qui méritent d'être pris en considération pour inclusion dans un tel cadre. Par exemple :

- les systèmes fédérés de gestion de l'identité devraient être conçus pour communiquer uniquement les renseignements qui sont absolument nécessaires et devraient avoir l'anonymat comme paramètre par défaut[41];
- les systèmes devraient pouvoir héberger de multiples marqueurs d'identité unique dans différents services afin d'empêcher l'établissement de liens et la réidentification involontaires chez les fournisseurs de services[42];

---

[37] Ahn et Lam, p. 32.
[38] Smedinghoff, p. 24.
[39] Smedinghoff, p. 27; CDT, p. 7.
[40] « Document de travail sur l'identité et les questions qu'elle soulève », p. 34.
[41] The Public Voice, « Civil Society Background Paper », Recommendations and Contributions to the OECD Ministerial Meeting of 17-18 June 2008 from Civil Society Participants in the Public Voice Coalition, <http://www.oecd.org/dataoecd/45/47/44686738.pdf>, p. 30 [en anglais seulement]; Document de travail sur l'identité et les questions qu'elle soulève, p. 32 et CIPPIC, commentaires sur l'ébauche du rapport du CPVP, p. 15.
[42] Voir par exemple : Civil Society Backgrounder; Ahn et Lam, p. 30; Maler et Reed, p. 18; Clark et coll. « Exit Node Repudiation for Anonymity Networks ».

- reconnaître que, même si le système fédéré de gestion de l'identité peut faire un suivi de l'activité de l'utilisateur ou de l'ensemble des renseignements sur l'utilisateur, ce n'est pas acceptable et, de fait, c'est contraire au but du projet[43];
- il faut conserver le modèle axé sur l'utilisateur pour faciliter l'auto-détermination de l'information et (ce qui est le plus important) le consentement significatif à la collecte, l'utilisation, la conservation et la communication d'information[44];
- les utilisations secondaires d'information au sein des systèmes fédérés de gestion de l'identité doivent être mentionnées à l'utilisateur, qui doit pouvoir y consentir explicitement au préalable avant que cela soit acceptable.

Au moment où on envisage de bâtir un tel cadre, il faut se demander si ce cadre serait appliqué dans la pratique et de quelle façon. Diverses suggestions ont été faites, allant d'une approche axée sur le libre marché qui permettrait aux fournisseurs d'identité de mettre en place et de faire appliquer leurs propres normes grâce à la possibilité de gérer les relations par contrat, comme cela se fait avec la transmission transfrontalière des données et la sous-traitance en général. La dernière suggestion consiste à adopter une véritable approche de réglementation[45].

Là encore, il y a un consensus remarquable chez les observateurs concernant la meilleure façon d'aborder la réglementation. Il y a deux possibilités : soit une réglementation qui essaie d'exposer clairement et de contrôler tous les aspects du système existant, ou une approche réglementaire axée sur une flexibilité de principe[46]. Les voix disparates sont unies dans le rejet d'une tentative d'adoption de mesures législatives très précises visant à contrôler le processus tout en s'efforçant de réconcilier une flexibilité par principe avec la reconnaissance de l'importance du contexte, sous l'influence de Nissenbaum, dans la gestion et la comparaison des risques associés à toute communication donnée de l'information[47].

Systèmes fédérés de gestion de l'identité au Canada

Les liens entre les conclusions au sujet de la gouvernance et de la réglementation et le cadre de protection de la vie privée existant au Canada peuvent être intéressants pour le CPVP. Les théoriciens et les observateurs semblent d'accord pour dire que la meilleure approche pour réglementer les systèmes fédérés de gestion de l'identité en serait une qui soit flexible et capable d'évaluer la proportionnalité. À cette fin, les termes utilisés doivent mettre l'accent sur la nécessité d'une approche neutre sur le plan technologique accordant aussi la flexibilité nécessaire pour aborder la force du contexte dans la mise en place d'une collecte, d'une utilisation, d'une conservation et d'une communication appropriée de l'information.

Le cadre canadien de protection de la vie privée est actuellement composé de la *Loi sur la protection des renseignements personnels* et de la *Loi sur l'accès à l'information* de 1983 de même que de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) de 2000. La LPRPDE intègre le *Code type* de l'Association canadienne de normalisation, qui a été élaboré pour

[43] CDT, p. 4.
[44] Civil Society Backgrounder; Dhamija et Dusseault, p. 26.
[45] Smedinghoff, p. 28.
[46] Ohm, p. 35.
[47] Ohm, p. 50.

l'autoréglementation du secteur. Le Code lui-même s'appuyait sur les Lignes directrices (de l'OCDE) régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de 1980, le premier accord international concernant des principes de protection des ensembles de données et visant à soutenir l'objectif de protection des renseignements personnels tout en évitant les obstacles indus à la libre circulation des données. À ce titre, la LPRPDE s'appuie sur une reconnaissance de l'importance de trouver un équilibre entre des intérêts (potentiellement) divergents et d'être neutre sur le plan technologique, plutôt qu'axé sur une technologie ou un secteur, se concentrant sur la circulation de l'information plutôt que sur les moyens de transmission de celle-ci[48]. La LPRPDE a été reconnue comme étant neutre sur le plan technologique, qualité qui a permis au CPVP d'appliquer ses dispositions aux nouvelles technologies et aux nouveaux modèles opérationnels[49], chose qui n'aurait peut-être pas été possible avec une loi plus ciblée[50].

Conclusion

Dans tout l'examen de la documentation, il était évident que les systèmes fédérés de gestion de l'identité sont remplis de contradictions éventuelles. L'authentification d'un tiers et les marqueurs d'identité fiables en ligne peuvent réduire le risque de vol d'identité et de fraude et, ce faisant, améliorer la confiance des gens à l'égard du commerce électronique. Quoi qu'il en soit, il faut reconnaître que ces mêmes caractéristiques, mal mises en œuvre, pourraient avoir l'effet opposé et faciliter plutôt que de prévenir l'accès criminel à l'information. De la même façon, le fait d'avoir un seul inventaire de données et un seul mot de passe ou jeton d'accès peut accroître la sécurité, mais les lacunes dans la mise en œuvre de la sécurité pourraient permettre à n'importe qui d'avoir accès à un ensemble de données sans précédent.

En conséquence, il faut reconnaître qu'un système fédéré de gestion de l'identité ne peut pas être auto-réglementé ni facilement réglementé sur le plan technologique. Il est plutôt essentiel que tous les utilisateurs de l'infrastructure connaissent bien tout le processus et participent pleinement à la production du système. À cette fin, il est important d'avoir un règlement flexible axé sur l'information plutôt que sur la technologie, tout comme il est important qu'un tel système soit entièrement axé sur le savoir et le consentement.

À la fin du présent examen dirigé de la documentation, il n'est donc pas possible de formuler des recommandations concrètes quant au fait de savoir si un système fédéré de gestion de l'identité est profitable ou nuisible ni même sur la façon de veiller à ce qu'il soit profitable plutôt que nuisible. Il demeure plutôt possible qu'il soit simultanément bon et mauvais, jusqu'à ce que la conception et la mise en œuvre du système soit entièrement terminée. En conséquence, c'est aux premières étapes de la conception que la protection des renseignements personnels et la sécurité doivent être évaluées et prises en considération pour soutenir la protection des renseignements personnels qui seront conservés et communiqués à l'aide du système plutôt que de l'attaquer.

[48] CPVP « Vie privée, confiance et innovation » juillet 2010, p. 5.
[49] Ébauche du rapport du CPVP sur la consultation, p. 34.
[50] Voir, par exemple, la *US Video Privacy Protection Act*, 18 U.S.C. § 2710 (2002).

Annexe A

Une partie de la documentation fournit des suggestions concrètes pour cerner les problèmes et mettre en place un cadre approprié de réglementation.

Au méta-niveau le plus élevé, Masiello et Whitten cernent quatre (4) concepts qui, d'après eux, sont des points de départ importants pour la conceptualisation de la vie privée dans ces circonstances : réputation; caractère éphémère; secret et intégrité du contexte[51].

Plus précisément, Smedinghoff mentionne cinq objectifs qui doivent être présents selon lui dans un cadre juridique efficace afin d'offrir un bon équilibre entre les besoins et les objectifs de tous les participants :

- il doit clairement définir les droits et les responsabilités associés à tous les rôles des participants, de façon à ce que le processus fonctionne bien et soit efficace et fiable pour établir le niveau de confiance requis;
- il doit fonctionner conformément à toutes les lois en vigueur régissant la protection de la vie privée et la sécurité des renseignements personnels et aux exigences d'authentification des personnes au moment de transactions en ligne;
- il doit répartir équitablement entre les rôles des participants les principaux risques sur le plan juridique;
- il doit fournir une certaine base permettant de garantir, avant le fait, que tous les rôles (en particulier les fournisseurs d'identité) ont les processus et les technologies nécessaires en place pour bien s'acquitter de leurs obligations et les mettre actuellement en œuvre de façon appropriée (p. ex. par le truchement d'une vérification appropriée);
- il doit fournir un mécanisme d'application réaliste et un recours dans l'éventualité où un participant n'agit pas de façon appropriée (p. ex. mettre fin à sa participation, prévoir la réparation des dommages, etc.)[52].

Dans son rapport de juillet 2007, le Groupe de travail intergouvernemental sur la gestion de l'identité et l'authentification a lui-même cerné trois principales difficultés qui doivent être abordées pour mettre en place un cadre pancanadien de gestion de l'identité et d'authentification : (1) les difficultés relatives à la capacité des administrations d'entreprendre des activités de gestion de l'identité et d'authentification au niveau pancanadien et la participation de base (2) les difficultés relatives à l'identification précise et à l'authentification des clients au niveau d'assurance requis, en particulier par télé-interrogation, et (3) les relations entre les administrations et la confiance[53].

Enfin, au niveau le plus précis des sources de la collecte, le CDT suggère la création d'un cadre de confiance qui, selon ses représentants, « imposerait certaines conditions minimales de participation qui régirait les interactions entre les trois parties — le fournisseur d'identité, la partie utilisatrice et l'utilisateur »

---

[51] Masiello et Whitten, p. 121.
[52] Smedinghoff, p. 28.
[53] Groupe de travail intergouvernemental (pancanadien) sur la gestion de l'identité et l'authentification — rapport final, juillet 2007, résumé, p. 6.

[traduction][54]. En outre, pendant la conception d'un tel cadre, les représentants du CDT présentent quatre (4) groupes de questions ou préoccupations qui doivent être abordées afin de mettre en œuvre le système de façon approprié. Les points sont les suivants :

Confiance à l'égard des fournisseurs de cadre

- *Admission des fournisseurs d'identité :* Dans quelle mesure le cadre de confiance certifiera-t-il que les fournisseurs d'identité satisfont à une norme minimale? Est-ce qu'on croira les affirmations faites par le fournisseur d'identité ou est-ce qu'on procédera à une vérification de ses pratiques? Pour quel motif un cadre de confiance pourrait-il refuser d'admettre un nouveau membre?
- *Vérification des fournisseurs d'identité :* Si les fournisseurs d'identité doivent se soumettre à une vérification, qui procédera à celle-ci, quels seront les critères d'indépendance à appliquer et à qui le vérificateur devra-t-il rendre des comptes?
- *Démonstration de la conformité :* Est-ce que le cadre donnera aux fournisseurs d'identité une façon de démontrer leur conformité avec le cadre, comme une marque ou un sceau? À l'aide de quelles ressources et de quelle façon surveillera-t-on la conformité?
- *Mise en place des politiques relatives au cadre :* De quelle façon la politique relative au cadre de confiance sera-t-elle adoptée et par qui? De quelle façon les utilisateurs intéressés seront-ils pris en considération, et comment les politiques seront-elles communiquées aux utilisateurs? Comment les politiques évolueront-elles?
- *Manquement en matière de service :* Si un fournisseur d'identité devait manquer à ses obligations au sein d'un cadre de confiance, quelles en seraient les conséquences?

Règles minimales pour les fournisseurs d'identité

- *Exigences relatives au cadre de confiance :* Est-ce que le cadre de confiance exigera un contrat minimal avec le fournisseur d'identité afin de limiter les conditions que celui-ci peut fournir à l'utilisateur?
- *Lien avec le cadre de confiance :* Quelle sera la relation entre le fournisseur d'identité et le fournisseur du cadre de confiance? Sera-t-elle contractuelle? Exigera-t-elle également la participation de l'utilisateur et de la partie utilisatrice?
- *Lien avec la partie utilisatrice :* Est-ce que les fournisseurs d'identité exerceront un pouvoir discrétionnaire concernant les parties utilisatrices avec lesquelles ils feront affaire? Est-ce que le fait de fournir de l'information authentifiée aux parties utilisatrices entraînera une obligation ou responsabilité éventuelle pour les parties utilisatrices ou les fournisseurs d'identité (autre que l'obligation de fournir des renseignements qu'ils croient de bonne foi être exacts)?
- *Lien avec l'utilisateur :* Est-ce que les fournisseurs d'identité seront soumis à de nouvelles exigences minimales concernant la protection de la vie privée et la sécurité des renseignements personnels concernant les utilisateurs? Y aura-t-il des politiques sur la conservation ou les limites d'utilisation des données?
- *Obligations relatives à la transmission d'information :* Est-ce que les parties utilisatrices devront assumer certaines obligations comme condition d'accès à l'information au sujet de l'utilisateur?

[54] Extrait traduit de CDT, p. 6.

Recours et responsabilité

- *Responsabilité et obligations à l'égard de l'utilisateur :* Si un fournisseur d'identité ne fournit pas les services attendus ou ne respecte pas ses obligations en vertu du cadre de confiance et que les utilisateurs subissent des dommages, y aura-t-il des recours pour eux? Si l'information de l'utilisateur est mal utilisée ou communiquée sans autorisation, quels sont les droits de l'utilisateur? Est-ce que l'utilisateur est responsable s'il fournit de faux renseignements d'identité?
- *Responsabilité du fournisseur d'identité :* Quelle est la responsabilité du fournisseur d'identité à l'égard d'une mauvaise identification ou authentification? S'il omet de protéger adéquatement les renseignements de l'utilisateur contre une utilisation ou une communication non autorisées?
- *Responsabilité de la partie utilisatrice :* Quelle est la responsabilité de la partie utilisatrice si elle s'est fiée à une mauvaise authentification (par exemple, dans le cas d'un vol d'identité) ou rejette une pièce d'identité valide en croyant à tort qu'elle est compromise? S'il omet de protéger adéquatement les renseignements de l'utilisateur contre une utilisation ou une communication non autorisées?
- *Obligations à l'égard du cadre de confiance :* Si le cadre de confiance impose des obligations contractuelles minimales, qui pourra faire appliquer le contrat? Y aura-t-il une obligation d'application du contrat?
- *Procédure de règlement des conflits :* Quelles procédures seraient utilisées pour régler les conflits entre les fournisseurs d'identité et le fournisseur de cadre de confiance? Entre le fournisseur d'identité et le cadre de confiance? Pour l'utilisateur, avec n'importe quelle des parties?
- *Exactitude :* Y a-t-il une méthode permettant de déterminer l'exactitude de l'information? Y a-t-il une façon pour l'utilisateur de corriger le dossier?

Vie privée et sécurité

- *Réduction au minimum de la quantité de données :* Y a-t-il une limite à la portée de l'information qui peut être recueillie (par une partie ou une autre) au sujet de l'utilisateur? Y a-t-il une limite quant à la période pendant laquelle ces données sont conservées et sur la façon de les éliminer?
- *Définition des objectifs et limites d'utilisation :* Y a-t-il des limites à l'utilisation qui peut être faite par une partie ou une autre de l'information recueillie?
- *Autorisation relative aux transactions :* Est-ce que les services d'identité offriront à l'utilisateur la possibilité d'approuver ou de refuser la présentation d'information authentifiée à une partie utilisatrice dans chaque cas? Est-ce que l'utilisation de certains renseignements est interdite à des utilisateurs en particulier?
- *Sécurité :* Est-ce que les fournisseurs d'identité ou les parties utilisatrices devront respecter des exigences minimales relatives à la sécurité des données? Quels mécanismes de gouvernance seront imposés pour prévenir l'utilisation ou la communication non autorisées?

Tribunaux : Quelles normes s'appliquent à l'accès à l'application de la loi ou à la communication associée aux litiges civils[55]?

[55] CDT, p. 7-8.