# GUIDE D'ENCADREMENT SÉCURITAIRE DE L'IDENTITÉ NUMÉRIQUE

**VERSION DU 25 MARS 2022**

GRIC

UDS Université de Sherbrooke

# TABLE DES MATIÈRES

# REMERCIEMENTS

Ce guide a été financé par le Commissariat à la protection de la vie privée du Canada en vertu du Programme des contributions 2021-2022. Les opinions exprimées dans ce rapport ne sont ni celles du Commissariat ni celles gouvernement du Canada.

LES PERSONNES SUIVANTES ONT PARTICIPÉ À LA RÉDACTION DE CE GUIDE :

- M. Benjamin Ali Aboudou
- Mme Samiha Abounouar
- Mme Marylise Caron
- Pr Daniel Chamberland-Tremblay
- M. Félix Gariépy
- Pre Manon Ghislaine Guillemette
- Pr Hugo Loiseau
- M. Moumouni Krissiamba Ouiminga
- Pr Arthur Oulaï
- Me Claudiu Popa
- M. Aboubakar Séhéna Soro
- Pr Pierre-Martin Tardif

LES PERSONNES SUIVANTES ONT PARTICIPÉ À L'AMÉLIORATION, À LA CORRECTION, À LA MISE EN PAGE ET À LA TRADUCTION DE CE GUIDE :

- Mme Pascale Beausoleil
- M. Mohammed Sbaï El Idrissi

# 1. MISE EN CONTEXTE

Sans contredit, l'identité numérique est un sujet complexe qui demande à être vulgarisé. L'identité numérique, ses cadres légaux et ses systèmes de gestion interrogent. L'objectif de ce guide vise à fournir des réponses à des questions à propos des nombreux aspects entourant l'identité numérique au Canada. Les dirigeants et les conseils d'administration sont responsables de l'identité numérique de leurs clients, de leurs employés et de leurs fournisseurs. Encadré par plusieurs lois et règlements, l'écosystème de cette identité recouvre la protection des renseignements personnels qui, elle-même, fait partie d'une réalité plus grande, celle de la cybersécurité. C'est pour dire que les défis sont grands pour les organisations du secteur privé!

Or, ce Guide débute, en section 2, en exposant ce qu'est l'identité numérique et les multiples approches qui la commandent. La section 3 indique comment et pourquoi l'identité numérique impacte l'organisation. Ensuite, en section 4, le Guide énonce en quoi la protection de l'identité numérique est devenue un facteur important pour la réussite d'une organisation au Canada. La section 5 décrit comment gérer l'écosystème de l'identité numérique pour une organisation du secteur privé au Canada. Enfin, la section 6 du Guide envisage les bénéfices et les occasions d'affaires que peut engendrer la bonne gestion de l'identité numérique pour une organisation.

## 1.1. UNE HISTOIRE COURTE

Le développement d'Internet ainsi que l'avènement de la société de l'information au début des années 2000 amenèrent certes, leurs lots d'opportunités, mais également plusieurs défis. Parmi ceux-ci, la nécessité, notamment pour les organisations, de pouvoir identifier et authentifier en ligne avec confiance les entités avec lesquelles elles font des transactions. C'est dans l'objectif de répondre à cet impératif que se développa le concept d'identité numérique (que nous définissons à la section 2.1 du document). L'identité numérique occupe une place de plus en plus importante au sein de notre société tel que le démontre l'annonce du gouvernement québécois en 2019 de la création et de la mise en place du Service québécois d'identité numérique (SQIN) visant à doter chaque membre de la population québécoise d'une identité numérique. La pandémie a mis en relief les besoins criants de notre société pour une identité numérique forte considérant la nécessité pour la population d'obtenir des services même lorsqu'elle ne pouvait se présenter en personne pour s'identifier lors de la prestation de services. L'identité numérique comporte, certes, un volet technique important, mais elle va beaucoup plus loin en impliquant également des aspects légaux, sociaux, de gestion et de gouvernance.

## 1.2. À QUI S'ADRESSE CE DOCUMENT ?

Ce document vise à informer les propriétaires et l'équipe de direction de chaque organisation canadienne de tout ce qui a trait à l'encadrement de l'identité numérique des personnes physiques. Il est écrit dans un langage vulgarisé et neutre. Il est construit sous la forme de questions et réponses, de façon à faciliter sa consultation. Il est suggéré de lire les sections qui d'intérêt, minimalement les sections 2.3, 3.1, 3.3, 3.4, 4.1, 4.2, 4.3, 5.2, 5.3, 5.4, 6.1 et 7.Malgré le soin apporté par les auteurs pour fournir une information fiable et aussi à jour que possible en date du 29 mars 2022, les enjeux et les règles applicables à l'identité numérique évoluent rapidement. Le document ne constitue pas un avis juridique et ne saurait se substituer à une analyse personnalisée du processus d'affaires envisagé par un professionnel. Le lecteur est invité à demeurer vigilant puisque le cadre juridique applicable, notamment en matière de protection des renseignements personnels, peut différer d'un territoire à l'autre et selon le type d'organisation.

## 1.3. POURQUOI EN PARLER MAINTENANT ?

Les technologies de l'information (TI) sont omniprésentes dans les organisations, peu importe leur taille et leur domaine d'affaires. Elles permettent d'acquérir, de stocker, de traiter et de transmettre une grande quantité d'informations dans un laps de temps très court. Parmi les informations traitées par une organisation, il y a les renseignements personnels qui permettent d'identifier les personnes avec lesquelles elle transige. Ces informations d'identité (voir section 3.6) peuvent être des renseignements personnels sensibles. En tant qu'organisation responsable, il est impératif de les protéger adéquatement, sous peine de perdre sa réputation et d'être victime de poursuites judiciaires.

Le contexte actuel est plus que propice pour s'intéresser à l'identité numérique. D'une part, plusieurs lois ont été récemment adoptées ou sont sur le point de l'être un peu partout au Canada. Ces lois visent à inciter les organisations à adopter des comportements responsables en gestion des données sensibles comme les renseignements personnels, qui comprennent notamment les identités numériques de chaque citoyen. D'autre part, la gestion des identités numériques est au cœur des actions de transformation numérique de plusieurs gouvernements à travers le monde. Cette nouvelle approche touche donc tous les citoyens, mais également toutes les organisations qui font des affaires avec les gouvernements, leurs employés et leurs partenaires. C'est donc tout un écosystème qui se met en place et auquel les organisations canadiennes sont ou seront exposées à très court terme.

Enfin, il va sans dire que la cybersécurité des données est au cœur de l'actualité et des préoccupations des citoyens et des organisations. Même si la cybersécurité va bien au-delà de la protection des données, celles-ci sont de plus en plus visées par les attaques et sont à la base d'un

modèle d'affaires très lucratif. S'il y a quelques années les vols de données visaient essentiellement les renseignements personnels, on voit apparaître une nouvelle tendance où le vol des renseignements personnels s'accompagne également de celui des données d'affaires très convoitées. Les identités numériques doivent donc être gérées sécuritairement par les organisations canadiennes.

# 2. L'IDENTITÉ NUMÉRIQUE

## 2.1. QU'EST-CE QUE L'IDENTITÉ NUMÉRIQUE?

L'identité numérique est l'ensemble des données d'identification d'une personne physique ou morale et constituée notamment d'identifiants numériques permettant de la représenter de manière univoque. Cette définition est inspirée de l'article 2 de la Loi n° 1.483 du 17 décembre 2019 relative à l'identité numérique de la Principauté de Monaco (voir p. 3870, Journal de Monaco du 27 déc. 2019). Cependant, il n'existe pas de consensus, ni en recherche et ni juridiquement, sur la nature exacte de l'identité numérique.

## 2.2. UN CONSENSUS SUR LA DÉFINITION DE L'IDENTITÉ NUMÉRIQUE EST-IL POSSIBLE?

La définition de l'identité numérique peut varier selon la discipline en cause, et même à l'intérieur de la même discipline.

La Recommandation UIT-T X.1252[1] témoigne toutefois de la nécessité de converger vers un relatif consensus dans le domaine de la gestion de l'identité, du moins au niveau terminologique. En proposant près de 99 définitions pour des concepts liés à l'identité numérique, la plus récente version de la Recommandation qui date d'avril 2021 vise à dissiper la confusion.

L'identité numérique y est présentée comme le produit d'attributs, un peu à l'instar du monde réel qui s'appuie sur les caractéristiques physiques ou sociales d'une personne pour la distinguer. On en profite toutefois pour clarifier que la gestion de l'identité numérique ne consiste pas seulement à singulariser des personnes physiques ou morales, elle s'étend aussi aux objets inanimés qui outre un dispositif, une application logicielle ou un service, peut s'avérer être dans le contexte des télécommunications un point d'accès, un abonné, des éléments de réseaux et plusieurs autres choses. Pour cette raison, le recours à l'identité numérique permet de démontrer qu'une entité – c'est le terme générique retenu – a une existence "séparée et distincte" lui permettant d'être "identifié[e] dans un contexte [donné]".

1 L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations unies et contribue au développement de normes (aussi connues comme étant des "Recommandations") pour assurer le développement et le bon fonctionnement des technologies de l'information et de la communication.

Plusieurs concepts de la norme ISO/IEC 24760-1 : 2019 Sécurité TI et confidentialité – Cadre pour la gestion de l'identité – Partie 1 : Terminologie et concepts ont été repris dans la Recommandation UIT-T X.1252. Cela vaut pour celui d'identification qui se veut être le "processus de reconnaissance d'une entité dans un domaine particulier, par opposition à d'autres entités". Dans les deux cas, on s'accorde pour reconnaître qu'il est possible qu'une entité puisse avoir plus d'une identité tout comme il se peut que plusieurs entités partagent la même identité dans certaines circonstances[2]. Cela dépendra toujours du contexte[3].

## 2.3. QU'EST-CE QUI LES COMPOSE?

Les identités numériques sont composées de différents types d'information susceptibles de révéler une caractéristique de la personne concernée. La première catégorie touche l'identité propre d'une personne incluant son profil sur le Web, alors que la seconde catégorie touche l'identité transactionnelle. Une troisième catégorie quant à elle touche des informations qu'on peut récupérer ou inférer à partir d'une identité de base et qu'on ajoute à cette identité numérique.

À la base, les identités numériques regroupent des informations qui sont associées directement à une personne. On peut penser par exemple à des informations nominatives comme le nom d'une personne physique, son adresse, son numéro de téléphone, sa date de naissance, ses identifiants uniques délivrés par un gouvernement comme un numéro d'assurance sociale ou un numéro d'assurance maladie, mais également à des éléments d'identification biométriques. Certaines de ces informations nominatives peuvent être uniques à une organisation, par exemple un numéro de dossier. Dans le cas d'une identité numérique recourant à un nom fictif utilisé sur le Web par exemple, l'identité numérique prendra alors la forme du pseudonyme et des caractéristiques qui auraient été fournies lors de l'enregistrement (comme les préférences ou intérêts par exemple). Ces données sont relativement stables dans le temps.

**2** ISO/IEC 24760-1, art. 3.1.2 s.v. "identité". Voir les notes 1 et 2.
**3** La Recommandation UIT-T X.1252 préconise l'expression "contexte" alors que la norme ISO 24760-1 y préfère le terme "domaine".

Ensuite, les identités numériques regroupent des informations touchant aux interactions qu'un sujet a eues dans un contexte numérique. Pour une organisation par exemple, les identités numériques des clients incluront des historiques d'achats, des historiques de navigation sur le Web, alors que les identités numériques des employés incluront des données salariales ou des évaluations de rendement par exemple. Dans un domaine médical, on pensera à l'historique médical, dans une banque on pensera plutôt aux transactions bancaires, dans une compagnie d'assurances on pensera aux données servant à évaluer l'admissibilité des personnes, les primes, les réclamations, etc. Sur les réseaux sociaux, il y aura des commentaires, des photos, des mentions (j'aime, je suis ici, etc.) qui permettent de suivre l'activité d'une personne. Ces données varient donc grandement d'une organisation à une autre et il est impossible de dresser une liste qui serait complète. Ces données sont beaucoup plus dynamiques que les données du premier groupe et elles changent constamment.

Enfin, le troisième type d'information qui compose les identités numériques concerne les données que l'on peut inférer à partir de l'analyse d'un profil, qu'on associe à ce profil et qu'on utilise dans les interactions subséquentes. Par exemple, les informations secondaires que l'on peut récupérer et associer à une identité numérique font partie des informations qui viennent s'ajouter à l'identité numérique. Un autre exemple vient des activités d'analyses des profils (souvent d'un client) et qui permettraient, par exemple, de lui associer un statut particulier (classifier un client dans une catégorie Or ou Platine par exemple) ou encore de lui attribuer une cote de propension à réagir positivement à une offre particulière. Ces données relèvent de techniques d'analytique et d'analytique avancées qui sont de plus en plus utilisées dans les organisations. Cette utilisation secondaire des données mène très souvent à la création de nouvelles informations qui viennent s'ajouter aux identités numériques déjà existantes. Ces données peuvent être plus ou moins dynamiques en fonction de la fréquence des analyses qui sont réalisées par les organisations et de la mise à jour des identités numériques.

## 2.4. À QUOI SERT L'IDENTITÉ NUMÉRIQUE?

L'identité numérique permet d'établir la confiance entre deux parties. Elle est au cœur de la gestion des identités et des accès qui s'articule autour de 4 étapes fondamentales : l'identification, l'authentification, l'autorisation et la journalisation. Ce guide se concentre sur l'étape de l'identification.

L'identification associe un ensemble d'attributs à une personne afin de la distinguer de façon univoque. Un identifiant unique est un attribut qui permet d'assurer cette distinction. Il faudra vérifier que les attributs soient authentiques. L'authentification consiste à demander au sujet de fournir une ou des preuves corroborant l'identité revendiquée. Il existe quatre preuves usuelles : ce qu'il sait – tel sa date de naissance, ce qu'il possède – tel un permis de conduire, ce qu'il est –

tel un trait physique et où il est – tel une adresse IP. L'autorisation fournit les accès correspondant au niveau d'habilitation du sujet, d'une façon discrétionnaire, en se basant sur son rôle ou encore par une combinaison d'attributs. Enfin, la journalisation permet de tracer les actions des sujets afin d'identifier les menaces sur la gestion de l'identité et des accès. La journalisation permet de détecter, d'enquêter ou de prouver certaines actions basées sur l'identité du sujet.

En termes simples, l'identité numérique est au cœur du processus qui permet d'identifier une personne et de l'authentifier comme étant bel et bien qui elle prétend être. Elle permet d'autoriser l'accès d'une personne à un système informatique dans la limite de ce qu'elle est autorisée à faire (ses droits d'accès) et conserve une trace de l'ensemble de ses actions qu'elle associe à son identité.

Illustrons le tout à l'aide d'un exemple. Imaginons un client qui veut interagir avec une institution financière. La banque voudra d'abord s'assurer que son client, appelons-le Marc Tardif, est bien celui qu'il prétend être. Elle lui demandera donc de fournir des informations qui sont associées à sa personne, dans notre exemple son identifiant. Elle voudra ensuite l'authentifier avec une information connue de lui seul, comme son mot de passe. Si l'information ainsi reçue correspond à celle qui est connue par la Banque, alors elle conclura que c'est bien Marc Tardif qui a fait la requête. Elle lui donnera accès à son compte et l'autorisera à poser certaines actions en lien avec son identité, par exemple en lui donnant accès uniquement aux comptes bancaires pour lesquels il est autorisé, acceptera seulement les transactions qu'il a le droit de faire, et le laissera consulter uniquement les informations qui le concernent. Enfin, la banque gardera une trace de tout ce que Marc aura fait comme transaction dans le système informatique et rattachera ces actions à son identité.

## 2.5. COMMENT EST-CE QUE JE PEUX RECONNAÎTRE LES IDENTITÉS NUMÉRIQUES?

Toute information détenue sur une personne physique qui peut servir à l'identifier compose l'identité numérique. Cette information peut être de nature confidentielle. Cette information confidentielle peut contenir des renseignements personnels ou non. Les identités numériques des personnes physiques peuvent être détenues par l'organisation. Dans le cas contraire, une organisation tierce conservera des informations concernant l'identité de la personne et pourra les communiquer en tout ou en partie. Dès qu'une organisation reçoit ces informations, elle en devient détentrice. Cependant, l'organisation tierce demeure responsable de communiquer cette information seulement si elle a reçu un consentement valide de la personne.

**LES RENSEIGNEMENTS PERSONNELS COMPOSANT L'IDENTITÉ NUMÉRIQUE SONT PARTICULIÈREMENT SENSIBLES. ILS INCLUENT LES :**

- noms et prénoms;
- adresses, telles l'adresse du domicile et l'adresse IP d'un appareil[4];
- attributs physiques, tels le poids et la taille;
- codes d'identification, tels les mots de passe, le numéro de client, le numéro d'assurance sociale, le numéro de passeport et le numéro du permis de conduire;
- croyances, telle la religion;
- dates liées à une personne, telles la date de naissance, la date d'obtention d'un diplôme;
- descriptions de biens possédés par la personne, telle une voiture;
- informations biométriques, telles que des mesures sur la topologie du visage ou sur les formes d'une empreinte digitale;
- informations de santé physique ou mentale;
- informations sociodémographiques, tels l'âge, l'état matrimonial, l'identification sexuelle et les langues parlées;
- données de localisation;
- numéros de téléphone;
- statuts accordés à la personne, tels un niveau élite et une marge de crédit;
- transactions effectuées par une personne, tels les achats, les requêtes et les ventes.

## 2.6. QU'EST-CE QU'UN JUSTIFICATIF D'IDENTITÉ NUMÉRIQUE?

Les justificatifs mieux connus comme étant les credentials servent de preuve pour établir "une partie ou (...) la totalité des attributs d'une identité" dans un contexte précis. Tant la norme ISO 29115 :2013 – Technologies de l'information – Techniques de sécurité – Cadre d'assurance de l'authentification d'entité que la Recommandation UIT-T X.1252 s'accordent sur la définition et le rôle du justificatif en matière d'identité numérique.

4 Commissariat à la protection de la vie privée du Canada, Ce qu'une adresse IP peut révéler à votre sujet – *Rapport préparé par la Direction de l'analyse des technologies – Mai 2013* <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/ip_201305/ > : Le Commissariat à la vie privée du Canada a conclu que l'adresse IP pouvait être un renseignement personnel particulièrement quand elle est considérée en fonction d'autres activités effectuées en ligne par un utilisateur.

Le justificatif remplit deux fonctions qui peuvent coexister ou non selon les objectifs mis de l'avant par celui qui décide d'inclure une démarche d'identité numérique dans son modèle d'affaires. Il y a, d'une part, le justificatif générateur de confiance dont la vocation est de venir confirmer les attributs déclarés par une entité. D'une autre, on retrouve aussi le justificatif servant à démontrer la capacité d'exercer un droit, et ce, sans obligation que l'identité réelle de l'entité soit divulguée. La Recommandation UIT-T X.1252 donne comme exemple de ce deuxième type de justificatif le cas du billet pour une rencontre sportive ou un événement musical. Le titre d'entrée rend possible la présence sur les lieux sans qu'il y ait de besoin d'y rattacher d'autres renseignements sur l'entité. Dans les deux scénarios, l'idée de l'identification par la voie du numérique est présente.

Dans l'élaboration d'une identité numérique, une analyse approfondie des relations et des dépendances entre l'entité, l'identité et les attributs se veut réconciliatrice avec le principe juridique de minimalisation de collecte de renseignements personnels (lorsqu'applicable) et la prudence qui s'impose du point de vue de la cybersécurité.

# 3. L'IDENTITÉ NUMÉRIQUE ET MON ORGANISATION

## 3.1. EST-CE QUE MON ORGANISATION DOIT ABSOLUMENT GÉRER DES IDENTITÉS NUMÉRIQUES?

L'organisation n'est pas tenue de gérer elle-même les identités numériques. Elle peut en externaliser la gestion en la confiant, par exemple, à un sous-traitant sur la base d'un contrat de service. Toutefois, l'organisation demeure toujours responsable de la protection des renseignements personnels qu'elle détient, ce qui inclut les informations soutenant l'identité numérique. Cela devrait l'amener à s'assurer que ses pratiques internes et celles du prestataire de services, s'il y a lieu, s'alignent sur de bonnes pratiques en matière de protection des renseignements personnels (voir les sections 5.7 et 5.8).

Puisqu'aucune organisation n'est à l'abri d'un dommage sous sa responsabilité, il importe de s'assurer que les pratiques de gestion de l'identité numérique permettent d'établir avec une grande fiabilité l'identification de la personne concernée. Qui plus est, l'engagement de l'organisation envers ces bonnes pratiques de gestion de l'identité numérique devrait être connu de la clientèle et des autres parties prenantes concernées[5].

**5** Le Bulletin d'interprétation portant sur la forme de consentement du Commissariat à la vie privée du Canada (mars 2014) est en cours de révision : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations_07_consent/

## 3.2. POURQUOI DOIS-JE M'EN PRÉOCCUPER DANS MON ORGANISATION?

Les identités numériques sont un actif important pour les organisations. Les renseignements personnels qui la composent doivent être adéquatement protégés. Une mauvaise gestion des identités numériques peut avoir des conséquences diverses dont certaines sont légales, d'autres touchent à la réputation, et certaines peuvent également entraver la compétitivité de l'organisation. Ces conséquences peuvent perdurer suffisamment longtemps pour créer des dommages irréparables qui mettent en péril l'organisation.

Un gestionnaire avisé pensera probablement ici à des scandales liés à des vols de données qui ont eu lieu ces dernières années comme la fuite de données déclarée par Capital One (106 millions de personnes nord-américaines, dont 6 millions au Canada) et celle de Desjardins (8 millions de personnes). Ces événements, très médiatisés, ont eu un effet important de conscientisation auprès des populations. Ces fuites ou vols de données ont entraîné des réactions vives chez les personnes touchées. Certains clients et partenaires ont immédiatement quitté l'organisation, ils l'ont inondé d'appels pour obtenir des réponses à leurs questions, et en bout de piste ils recevront des dédommagements substantiels. Dans tous les cas, les conséquences sont importantes, coûteuses et difficiles à renverser. Ces vols de données sont parfois le résultat d'une cyberattaque provenant d'un attaquant externe et, plus souvent encore, ils sont commis par des employés de l'organisation que ce soit de façon intentionnelle ou non. Dans le cas des incidents commis par des employés, ils sont surtout le résultat de mauvaises pratiques de gouvernance des données qui, si elles avaient été mises en place et suivies rigoureusement, auraient souvent pu réduire une partie des conséquences, voire empêcher l'événement de se produire.

Cela étant dit, malgré la visibilité accordée à ces fuites de données et l'importance des conséquences pour les organisations, un impact beaucoup plus fréquent et persistant de la mauvaise gestion des identités numériques se reflète dans les pratiques d'affaires courantes des organisations. Par exemple, avoir plusieurs systèmes de gestion de la relation client (GRC) peut amener différentes façons de représenter les clients, dont l'identifiant unique (voir section 2.1). Ceci peut entraîner des problèmes de qualité du service à la clientèle, d'efficience des processus d'affaires, et réduit la proposition de valeur de l'organisation. Ces effets, persistants et non épisodiques, diminuent la compétitivité des organisations, que ce soit à cause d'une attrition continue des clients, des difficultés à recruter la main-d'œuvre de qualité ou une augmentation des coûts d'exploitation. En fin de compte, tout ceci se reflète sur la santé financière de l'organisation et met en péril sa pérennité.

Bref, la gestion des identités numériques est essentielle pour assurer la compétitivité des organisations.

## 3.3. QUI DANS MON ORGANISATION DEVRAIT S'EN OCCUPER?

L'identité numérique d'une personne physique comporte des renseignements personnels, c'est-à-dire des informations concernant une personne physique identifiée ou identifiable. De ce point de vue, l'exécutif de l'organisation en est responsable et peut désigner une personne responsable de la protection des renseignements personnels. Cette personne aura notamment les responsabilités suivantes :

- **Élaborer des politiques de l'entreprise en la matière ;**
- **Informer et sensibiliser le personnel aux meilleures pratiques;**
- **Informer les parties prenantes externes sur les politiques et pratiques de l'entreprise;**
- **Veiller à la conformité légale et réglementaire;**
- **Informer l'organisation, notamment lorsque les données changent de juridiction légale;**
- **Informer les autorités de tout incident de confidentialité;**
- **Créer, mettre en place, surveiller et auditer le suivi des politiques et procédures;**
- **S'assurer de l'évaluation de facteurs relatifs à la vie privée (EFVP) lorsque pertinente;**
- **Établir et maintenir des registres relatifs à la cueillette, au traitement, à la communication et à la destruction des données;**
- **Recevoir et traiter les plaintes des personnes concernées;**
- **Être le point de contact de l'organisation au niveau des personnes et des autorités.**

### Il n'est pas exigé que le responsable de la protection des renseignements personnels ait des compétences techniques particulières, si ce n'est de :

- **Connaître les lois, les règlements et les normes de l'industrie en matière de protection des renseignements personnels ;**
- **Être attentif aux détails;**
- **Être irréprochable au niveau de la gestion des renseignements personnels;**
- **Exercer un jugement sûr en lien avec les risques liés à la confidentialité;**
- **Exercer un leadership favorisant le changement;**
- **Savoir communiquer dans un langage clair et concis;**
- **Savoir travailler en équipe, notamment avec des experts juridiques ou technologiques.**

Un point important à souligner est que cette personne relève, selon les bonnes pratiques, du conseil d'administration ou de l'administration de l'organisation. Ceci lui assure l'autorité et l'indépendance nécessaires pour accomplir sa mission.

La personne responsable des renseignements personnels doit collaborer avec différents intervenants de l'organisation pour protéger les données composant l'identité numérique. En premier lieu, il faut reconnaître le rôle de la personne ou des personnes responsables des technologies de l'information qui assurent le fonctionnement adéquat et sécuritaire des systèmes stockant les données d'affaires, dont les données de l'identité numérique, et l'architecture technologique globale assurant l'interaction entre ces systèmes. La fonction de gestion des systèmes intègre tant les systèmes exploités localement que ceux hébergés dans l'infonuagique. On reconnaîtra aussi le rôle des intendants de données qui sont chargés de la saine gestion des données d'affaires, incluant les données de l'identité numérique. Le rôle de l'intendant de données inclut la gestion de la qualité et de la sécurité des données, ainsi que la compréhension et l'utilisation de saines pratiques de gestion des données par l'ensemble des personnes dans une organisation. Cette coordination multipartite peut être formalisée au moyen de structures et de pratiques formalisées de gouvernance des données d'affaires.

## 3.4. OÙ DEVRAIS-JE CHERCHER DE TELLES DONNÉES ?

Les organisations gèrent un volume important de données numériques et papier, dont les données spécifiques à l'identité numérique, pour l'ensemble de ses activités. Ces données peuvent se retrouver dans différents systèmes informatiques ou d'archivage d'une organisation, voire apparaitre en multiples copies dans plusieurs de ces systèmes.

Il est irréaliste de prétendre produire une liste exhaustive de toutes les technologies ou pratiques pouvant servir à stocker des données liées à l'identité numérique. Toutefois, le cadre de référence de la gestion de l'information MIKE2.0[6] permet de structurer la recherche et l'identification des sources potentielles de ces données. Ainsi, le cadre MIKE2.0 reconnaît cinq catégories de systèmes qui peuvent exister sous une forme numérique ou physique :

- **Les systèmes d'accès, de recherche et de livraison d'information, incluant les outils de communication comme le courriel, les applications mobiles ou les portails d'entreprise;**
- **Les systèmes de gestion des contenus d'affaires, incluant les suites collaboratives, les espaces de stockage sur disque ou dans le nuage, les systèmes d'entreprise de type PGI (progiciels de gestion intégrés) et GRC (gestion de la relation client) ou les gestionnaires de contenu Web;**
- **Les systèmes de gestion des actifs informationnels, incluant les outils de contrôle et de suivi des accès ou les systèmes de gestion des flux d'information (workflow systems);**
- **Les systèmes de gestion des données d'entreprise, incluant les comptoirs et les entrepôts de données ou les systèmes de gestion des données maître;**
- **Les systèmes d'intelligence d'affaires, incluant les systèmes de gestion de la performance et les outils soutenant l'analyse, l'analytique et l'intelligence artificielle.**

6 http://mike2.openmethodology.org/

Lors de la recherche et de l'identification des données relevant de l'identité numérique, la vigilance est de mise. En effet, selon les pratiques en vigueur dans une organisation, les données peuvent se retrouver, par négligence, par erreur ou par choix, en dehors des systèmes officiels et répertoriés. C'est le cas si des données se retrouvent dans des courriels personnels d'employés ou sur un support de stockage gratuit dans l'infonuagique.

Enfin, il est important de souligner que les données relatives à l'identité numérique peuvent être fragmentées et éparpillées. Cette situation engendre un niveau de complexité accru lors de la recherche et l'identification. Prises individuellement, certaines données peuvent passer inaperçues, alors que combinées elles peuvent révéler l'identité d'une personne physique.

Il faut donc sensibiliser et former le personnel aux pratiques et aux systèmes appropriés pour la gestion de ces données et s'assurer de leur utilisation adéquate.

## 3.5. QUAND EST-CE QUE JE DOIS FAIRE QUELQUE CHOSE AVEC CES DONNÉES ?

La vigilance est de mise, afin d'assumer pleinement la responsabilité de l'organisation. Il y a six principales situations où il faut réagir : (1) lorsque des données d'identité sont acquises ou colligées sans qu'il n'y ait nécessité, (2) lorsque des données d'identité sont colligées à l'insu de la personne, (3) lorsque les données d'identités sont conservées sans directives, (4) lorsque des données d'identité sont perdues ou volées, (5) lorsque des données d'identité sont partagées avec un tiers sans obligation légale ou consentement des personnes concernées, (6) lorsque l'endroit où sont conservées les données d'identité change. Elles sont décrites dans le tableau qui suit :

**TABLEAU 1** PRÉSENTATION DES SIX SITUATIONS PROBLÉMATIQUES, DE LEURS CAUSES ET DE SOLUTIONS POTENTIELLES

| # | SITUATIONS | CAUSE(S) POTENTIELLE(S) | SOLUTION(S) |
|---|---|---|---|
| 1 | Absence de nécessité | Gouvernance déficiente | **Détruire** les données ainsi colligées<br><br>**Sensibiliser** le personnel aux exigences légales concernant la collecte des renseignements personnels et l'identité numérique<br><br>**Établir** et **mettre en place** des politiques et des pratiques internes visant les exigences légales concernant la collecte de renseignements personnels |
| 2 | Manque de transparence | • Acte illégal<br>• Erreur ou omission | **Établir** et **mettre en œuvre** des politiques et des pratiques conformes aux lois et règlements, pour encadrer la gouvernance des renseignements personnels Rendre accessibles les politiques sur le site Internet de l'organisation<br><br>**Créer** une politique Rendre accessibles les politiques sur le site Internet de l'organisationconcernant la collecte et la gestion des renseignements personnels et l'identité numérique<br><br>**Enquêter** lors d'un doute raisonnable |
| 3 | Aucun calendrier de conservation | Aucune gestion du cycle de vie des données | **Instaurer** la gestion (politiques, cartographie, etc.) des données d'identité numérique au regard des exigences légales et réglementaires |

| # | SITUATIONS | CAUSE(S) POTENTIELLE(S) | SOLUTION(S) |
|---|---|---|---|
| **4** | Incident de confidentialité, incluant la fuite de données | Protection des données inadéquates (technologie et gouvernance) | **GESTION DE L'INCIDENT**<br><br>**Informer** promptement le responsable de la protection des renseignements personnels de l'organisation et déclarer la fuite aux autorités compétentes<br><br>**Gérer** activement la crise (médias, technologie)<br><br>**Demander** de l'aide à une firme spécialisée en cybersécurité pour gérer l'incident actif<br><br>**MESURES CORRECTIVES POST-CRISE**<br><br>**Établir** et mettre en œuvre une politique de gestion de crise en prenant des mesures raisonnables pour diminuer le risque de préjudice<br><br>**Demander** de l'aide à une firme spécialisée en cybersécurité pour réaliser un audit de l'incident, identifier la cause racine de la fuite et mettre en place des mesures correctives et préventives<br><br>**Améliorer** la posture de sécurité de l'organisation, notamment par la sensibilisation du personnel aux exigences légales concernant les renseignements personnels, l'identité numérique et la sécurité de l'information<br><br>**Tenir** un registre des incidents de confidentialité |
| **5** | Partage illégal | • Gouvernance déficiente<br>• Absence d'expertise juridique | **Cesser** le partage et exiger que l' organisation tierce détruise les informations reçues<br><br>**Consulter** une firme juridique avant de partager des données avec une organisation tierce<br><br>**Interdire** aux personnes de l'organisation de partager l'identité des personnes sans l'autorisation explicite du responsable de la protection des renseignements personnels<br><br>**Demander** le consentement explicite des personnes avant de partager des identités numériques |
| **6** | Stockage hors juridiction | Ne pas gérer les contrats avec les fournisseurs de services TI | **Vérifier** la juridiction de stockage du fournisseur visé ou une nouvelle plateforme infonuagique<br><br>**Vérifier** les politiques de confidentialité et les conditions d'utilisation du fournisseur visé ou toute une nouvelle plateforme infonuagique<br><br>**Éviter** les plateformes « gratuites »<br><br>**Utiliser** des clauses contractuelles légitimes pour l'ensemble des contrats, incluant des clauses de résiliation du contrat assurant une gestion sécuritaire et appropriée des identités numériques |

Il convient de souligner que le critère de “nécessité” est celui qui guide la portée de l’acquisition ou de la cueillette de renseignements personnels. Il suppose qu’une évaluation du contexte se doit d’être faite pour déterminer si le renseignement est requis. Ce qui est nécessaire s’apprécie avec plus de sévérité que ce qui est utile ou pratique d’autant plus quand il est possible de s’en remettre à la collecte d’autres renseignements, généralement moins sensibles, qui peuvent permettre de rencontrer la même finalité.

# 4. LA PROTECTION DE L’IDENTITÉ NUMÉRIQUE AU CANADA

## 4.1. EST-CE QUE LA PRÉSENCE D’IDENTITÉS NUMÉRIQUES DANS MON ORGANISATION A UN IMPACT SUR MES PRATIQUES D’AFFAIRES?

L’organisation qui souhaite recourir à des solutions d’identification numérique doit forcément clarifier ses intentions et surtout ses obligations. Il est parfois indésirable de rattacher automatiquement certaines actions et transactions à une personne[7]. Pour s’en prémunir, il est possible de recourir à l’anonymat ou d’utiliser un identifiant non significatif.

Force est de constater que la portée de la collecte d’informations susceptibles de constituer des renseignements personnels variera en fonction du besoin d’établir un lien fort avec une personne physique. De plus, l’association entre un identifiant unique et une personne peut être requise. Par exemple, si on veut éviter d’accorder un privilège deux fois à une même personne, tel un vote électronique.

L’organisation peut être soumise à des exigences plus strictes face à l’usurpation d’identité, notamment pour lutter contre le blanchiment d’argent et le financement des activités terroristes. Par exemple, la partie 3 du Règlement sur le recyclage des produits de la criminalité et le financement des activités terroristes[8] énonce les moyens pouvant être utilisés pour vérifier l’identité d’une personne. Dans la mesure où les gouvernements fédéral, provinciaux et étrangers délivrent pas ou peu de document d’identité numérique, la personne tenue de satisfaire aux exigences de vérification est placée dans une position où elle doit faire le pont entre le monde physique et virtuel. Par conséquent, la Directive du Centre d’analyse des opérations et déclarations financières du Canada (CANAFE) sur les méthodes pour vérifier l’identité de personnes et d’entités[9] prévoit quelques alternatives comme :

**7** Paul A. Grassi et als., National Institute of Standards and Technology Special Publication 800-63-3A, Enrollment and Identity Proofing (2017), 2, < https://doi.org/10.6028/NIST.SP.800-63a>.
**8** DORS/2002-184.
**9** Gouvernement du Canada, Méthodes pour vérifier l'identité de personnes et d'entités (fintrac-canafe.gc.ca), Novembre 2021.

- **participer à une séance de clavardage vidéo en direct avec la personne, pour comparer le nom et les particularités des images vidéo avec le nom et la photo figurant sur le document d'identité délivré par un gouvernement; ou**
- **demander à la personne de prendre un égoportrait, puis, au moyen d'une application de reconnaissance faciale, comparer les particularités de l'égoportrait à la photo du document d'identité vérifié délivré par un gouvernement et comparer le nom fourni avec celui figurant sur le document d'identité.**

Ainsi, l'organisation devrait toujours voir à la mise en place de politiques et de procédures permettant de vérifier l'authenticité d'un document d'identité.

## 4.2. EST-CE QUE MON ORGANISATION A DES OBLIGATIONS LÉGALES ENVERS LA GESTION DES IDENTITÉS NUMÉRIQUES?

La cueillette, la détention, la gestion, l'exploitation ou toute autre forme d'utilisation d'informations relevant notamment de l'identité numérique d'une personne physique créent des obligations légales à l'égard de l'organisation.

Les obligations indicatives, ci-après énumérées sont inspirées des meilleures pratiques juridiques, notamment canadiennes, pour un encadrement sécuritaire de l'identité numérique. L'observation de ces meilleures pratiques permet aux entreprises de se conformer notamment au cadre juridique canadien en la matière.

Désigner une personne responsable de la protection ou de la sécurisation de l'identité numérique au sein de l'organisation (voir section 3.3).

Établir un inventaire des données d'identité numérique détenues par l'organisation, afin d'en faciliter la gouvernance et la gestion (voir sections 3.5 et 4.4) puis déterminer si chaque système impliqué assure le niveau de confidentialité et de protection qui est nécessaire.

Mettre en œuvre des politiques et procédures conformes aux exigences légales soutenant la gouvernance et la gestion des données d'identité numérique. On peut noter :

- **Des politiques établissant les principes relatifs à la collecte, à la gestion, à la communication ou à toute autre forme d'utilisation des données d'identité numérique;**
- **Des politiques relatives à la réception, au traitement des plaintes et de réclamation des citoyens souhaitant exercer leurs droits;**
- **Des politiques relatives à la sécurité des données;**
- **Des politiques de signalement et de gestion des incidents de confidentialité;**

- **Des politiques particulières sur l'utilisation de systèmes biométriques appliqués à l'identité numérique, l'utilisation d'informations d'identité numérique pour la recherche et l'intelligence artificielle, etc.;**
- **Des politiques de protection par défaut pour tous les systèmes de l'organisation;**
- **Des politiques d'évaluation des facteurs relatifs à la vie privée (EFVP) préalablement à tout projet impliquant des données d'identité numérique. Définir les critères déclenchant l'obligation d'effectuer une EFVP.**

## 4.3. QUELS PRINCIPES MON ORGANISATION DOIT-ELLE RESPECTER POUR ÊTRE CONFORME À LA LOI?

Toute cueillette, détention, gestion, exploitation, etc. d'informations relevant notamment de l'identité numérique d'une personne physique doit obéir à des principes directeurs[10]. Que retenir succinctement de l'essentiel des principes ?

### 4.3.1. L'IDENTIFICATION D'UNE FINALITÉ

L'organisation doit déterminer à l'avance les fins pour lesquelles les données d'identité numérique sont collectées pour traitement. Ces fins doivent être précises, explicites, légitimes et licites. En clair, chaque collecte de données d'identification doit correspondre à une finalité déterminée à l'avance qui soit précise, explicite, légitime et licite. Par exemple, il faut recueillir l'adresse de la clientèle afin d'être en mesure de livrer les produits commandés.

### 4.3.2. LA MINIMISATION DES DONNÉES

L'organisation doit recueillir uniquement les données d'identité numérique adéquates et pertinentes pour la réalisation de la finalité de l'opération. Une donnée est pertinente ou adéquate si elle a un lien direct avec la finalité du traitement. Les données identifiantes collectées doivent être exactes et, si nécessaire, mises à jour. Par exemple, en évitant de demander le numéro de permis de conduire à la clientèle même si cela aurait pu diminuer les cas de fraude.

### 4.3.3. LA SÉCURISATION ET LA CONFIDENTIALITÉ

L'organisation doit prendre toutes les mesures techniques, logicielles et organisationnelles nécessaires et pertinentes au regard de la finalité de chaque traitement et de la nature des données d'identité numérique, pour prévenir leur communication, leur accès non autorisé ou leur perte, afin de garantir un niveau élevé de sécurité. Par exemple, une organisation chiffre les bases de données clientèles afin d'éviter qu'un cyberattaquant puisse voler l'information qu'elles contiennent.

**10** Principes relatifs à l'équité dans le traitement de l'information de la LPRPDE, Commissariat à la protection de la vie privée du Canada, https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/p_principle/

### 4.3.4. LE PRINCIPE DE RESPONSABILITÉ

L'organisation doit avoir à l'esprit qu'elle est responsable de la protection des informations d'identité numérique qu'elle recueille ou détient et, doit en conséquence, être toujours en mesure de démontrer et de documenter que chaque utilisation est conforme au cadre juridique en la matière. En d'autres termes, il faut respecter toutes les obligations légales qui incombent dans la collecte, l'exploitation, la gestion ou toute autre forme d'utilisation des informations d'identité numérique dans le cadre de leur organisation. Ceci implique la mise en œuvre de mécanismes et de procédures internes permettant d'en démontrer le respect. Par exemple, lorsqu'un système d'information clientèle est modifié, il faut évaluer les facteurs relatifs à la vie privée (EVFP) et agir proactivement lorsque le risque est trop grand.

### 4.3.5. LE PRINCIPE DE TRANSPARENCE

L'organisation doit informer la personne concernée lorsqu'elle recueille son identité numérique. Par exemple, une personne qui a fourni ses informations de paiement doit cocher une case de consentement pour conserver ces informations pour un paiement futur.

## 4.4. QU'EST-CE QUI ARRIVE SI MON ORGANISATION NE LE FAIT PAS?

Le non-respect des principes et obligations énoncées à la section 4 peut exposer les organisations à des sanctions administratives pécuniaires ou à une poursuite pénale, mais aussi au paiement de dommages-intérêts issus des lois en matière de protection de renseignements personnels nationales et internationales.

Au Canada la violation des dispositions du cadre juridique peut entraîner des sanctions importantes, pouvant aller jusqu'à 25 millions de dollars ou 4 % du chiffre d'affaires mondial de l'exercice financier précédent, si ce dernier montant est plus élevé

Dans l'Union européenne, le Règlement général de protection des données (RGPD), qui peut s'appliquer au Canada, prévoit que la violation des principes peut entraîner une amende administrative pouvant aller jusqu'à 20 millions d'euros ou, dans le cas d'une organisation, jusqu'à 4 % du chiffre d'affaires mondial de l'exercice financier précédent, si ce montant est plus élevé.

À ces sanctions provenant des lois spécifiques en matière de protection de renseignements personnels, s'ajoute le risque de non-respect des principes constitutionnels et quasi constitutionnels de protection de la vie privée du client, ouvrant la porte au risque de contraventions à des lois provenant d'autres domaines du droit, relevant notamment du droit criminel canadien, des règles de la responsabilité civile et des protections fondamentales prévues par la Charte des droits et libertés de la personne, exposant une organisation au dépôt d'accusations criminelles

ou au paiement de dommages-intérêts ainsi que de dommages-intérêts exemplaires (punitifs). Dans la protection des données de l'identité numérique, une organisation doit également prendre en compte les risques liés aux affaires comme l'atteinte à sa réputation ou à son image de marque, les coûts engendrés pour la mitigation de problèmes découlant d'un non-respect des lois ou d'un vol de ces données et la perte de clients ou d'employés actuels ou potentiels qui ne voudraient plus être associés à l'organisation.

## 4.5. EN TANT QUE PROPRIÉTAIRE DE MON ORGANISATION, EST-CE QUE JE SUIS PERSONNELLEMENT RESPONSABLE DU RESPECT DE CES OBLIGATIONS LÉGALES?

Toute personne qui exploite une organisation est responsable de la protection des informations relevant de l'identité numérique des citoyens qu'elle détient et la personne ayant la plus haute autorité doit veiller à assurer le respect et la mise en œuvre du cadre juridique de protection en la matière. Elle peut cependant déléguer cette fonction par écrit, en tout ou en partie, à un membre du personnel.

Cependant, devant la variété de modèles et la diversité des opérations, il n'est pas facile de faire un portrait de toutes les conséquences indésirables[11] pouvant résulter d'une mauvaise gestion de l'identité. Certaines situations vont requérir un niveau d'assurance[12] élevé et d'autres moins, d'où l'importance de mener une analyse rigoureuse à intervalle donné. Une politique de gestion de l'identité[13] demeure un outil incontournable.

Par ailleurs, le seul fait d'être le propriétaire d'une organisation qui collecte ou traite des éléments composant l'identité numérique d'un utilisateur ne rend pas le propriétaire personnellement responsable du non-respect des obligations légales par l'organisation. Il y a toutefois certaines situations dans lesquelles la responsabilité de l'entrepreneur serait engagée. Ainsi, le propriétaire peut devenir personnellement responsable lorsqu'il (1) agit à titre d'administrateur ou de dirigeant ou de représentant de l'organisation et (2) qu'il a prescrit ou autorisé ou consenti à l'accomplissement de l'acte ou de l'omission qui constitue une infraction au regard de la loi. De plus, lorsqu'il s'agit d'une entreprise individuelle ou d'une entreprise à propriétaire unique, l'entrepreneur propriétaire conserve la responsabilité à l'égard des obligations de son entreprise. Il est tenu de respecter les obligations légales susmentionnées.

**11** Pour un aperçu d'exemples de préjudice, voir l'annexe B de la Ligne directrice sur la définition des exigences en matière d'authentification : Ligne directrice sur la définition des exigences en matière d'authentification- Canada.ca (tbs-sct.gc.ca)

**12** Pour un aperçu, voir la Ligne directrice sur l'assurance de l'identité : Ligne directrice sur l'assurance de l'identité- Canada.ca (tbs-sct.gc.ca)

**13** Voir la Directive sur la gestion de l'identité du gouvernement du Canada dont la dernière modification remonte au 1er juillet 2019 : Directive sur la gestion de l'identité- Canada.ca (tbs-sct.gc.ca)

À défaut, il s'expose aux sanctions pécuniaires administratives, pénales ou aux dommages-intérêts qui en découlent. Dans le cas d'un co-propriétaire d'une société en nom collectif, chaque associé est personnellement responsable des dettes de la société lorsque ses actifs sont insuffisants pour payer ses dettes découlant des sanctions administratives, pénales ou des dommages-intérêts en raison du non-respect des obligations légales de la société.

# 5. LA GESTION DE L'ÉCOSYSTÈME DE L'IDENTITÉ NUMÉRIQUE

## 5.1. COMMENT EST-CE QUE JE PEUX ÊTRE UNE ORGANISATION RESPONSABLE AU NIVEAU DE LA GESTION DE L'IDENTITÉ NUMÉRIQUE?

Une organisation responsable s'assure de gérer les effets sociaux, environnementaux et économiques de ses activités d'une manière responsable et conforme aux attentes du public. Elle veille à utiliser des pratiques éthiques, inclusives, environnementalement soutenables et socialement acceptables. Parmi les pratiques éthiques d'intérêt concernant l'identité numérique, notons le respect des principes légaux (voir section 4.3), la gestion sécuritaire (voir sections 5.6 et 5.7) et la transparence. Les pratiques inclusives permettent d'avoir une représentation conforme à la réalité de la personne, autant au niveau de son identité que de ses préférences. Le respect de l'environnement peut proscrire l'utilisation de technologies énergivores. Enfin, l'acceptabilité des systèmes permet d'obtenir l'accord des parties concernées à l'égard d'un projet (voir section 5.2).

Il faut porter une attention à l'équilibre entre les intérêts d'une organisation, de ses clients et de ses partenaires. Une économie de coûts ne devrait pas se faire au détriment de la sécurité de l'identité numérique, incluant les relations avec les fournisseurs de services infonuagiques. De plus, les mœurs et les préoccupations de sécurité des données évoluent rapidement et l'organisation doit rester en éveil. Enfin, on peut souligner qu'une approche proactive est souvent préférable à une approche réactive, évitant du même fait des correctifs coûteux.

## 5.2. COMMENT TENIR COMPTE DE L'ACCEPTABILITÉ SOCIALE DES APPROCHES D'IDENTITÉ NUMÉRIQUE PRÉCONISÉES PAR MON ENTREPRISE ?

Dans le but d'assurer le succès d'un système d'identité numérique et plus largement, de la transformation numérique d'une organisation, il importe de ne pas ignorer la question de l'acceptabilité sociale, soit le degré d'accord des parties concernées à l'égard d'un projet.

En effet, une absence d'acceptabilité sociale peut se traduire par une faible utilisation du système d'identités numériques jusqu'à une vive opposition des parties concernées à l'égard de ce système ou de la gestion des identités les comprenant, et ce, en dépit d'investissements importants dans la mise en place et la gestion de celle-ci. Au-delà de la perte d'argent, une faible acceptabilité sociale peut entraîner en une faible confiance de la clientèle envers l'organisation, culminant par une mauvaise réputation. Par ailleurs, une absence d'acceptabilité sociale pourrait engendrer des coûts financiers supplémentaires pour l'organisation, dont l'abandon de projets, en plus d'exposer à des contestations tant sociales que judiciaires.

Dans cette optique, il convient d'aborder rapidement les éléments influençant le risque qu'un des projets de l'organisation ne jouisse pas d'une acceptabilité sociale. Parmi les éléments exerçant une influence sur l'acceptabilité sociale, on remarque l'adéquation entre le milieu et le projet, ce qui se traduit notamment par un respect des valeurs (ex. préoccupations relatives à la vie privée). Ensuite, il importe de considérer la perception de la clientèle de la présence et de l'ampleur des bénéfices/dommages, le niveau de risque, de nouveauté et d'incertitude à l'égard du projet (ex. risques perçus d'intrusions dans la vie privée ou de fuites des renseignements personnels). Aussi, la confiance de la clientèle envers l'organisation et la gestion des identités numériques n'est pas à négliger si l'on souhaite s'assurer d'une bonne acceptabilité sociale. Ultimement, ces éléments sont influencés par la qualité du processus de consultation avec les parties prenantes. Souvent prise pour acquise, l'acceptabilité sociale n'est pas à négliger vu les conséquences possibles de son absence d'autant plus qu'elle n'est jamais acquise et qu'elle peut être perdue à tout moment.

## 5.3. QUE FAIRE AVEC MES FOURNISSEURS ET SOUS-TRAITANTS ?

Les fournisseurs et les sous-traitants qui gèrent des identités numériques en partenariat, ou pour le compte d'une organisation, doivent respecter les mêmes lois, droits et obligations que l'organisation principale. Puisque la responsabilité finale revient à l'organisation principale, celle-ci se doit d'en faire une étroite surveillance. Celle-ci doit être planifiée dès le début du partenariat et clarifiée par écrit entre les parties qui s'échangent les informations, car l'information sur l'identité numérique peut être rendue vulnérable du fait d'une gestion inadaptée de la sécurité. Il convient d'identifier et d'appliquer des mesures pour gérer l'accès des tiers aux moyens de traitement de l'information à la base de l'identité numérique.

Il est primordial de bien définir les responsabilités et les obligations respectives. Il devient alors nécessaire de s'assurer de l'exhaustivité des clauses contractuelles. Ainsi, en plus des clauses standards, il faut s'assurer de bien définir :

- **la mise en place de mesures de sécurité appropriées;**
- **le respect de certaines politiques et procédures de l'organisation;**

- **le droit à l'audit ou de recevoir un document d'attestation de conformité, tel un rapport System and Organisation Controls 2 de type 2 (SOC 2, type 2);**
- **les obligations mutuelles de confidentialité, incluant tout ce qui a trait à l'identité numérique et les renseignements personnels. Ces obligations limitent au strict nécessaire l'accès aux informations confidentielles, interdisent toute divulgation à des tiers, proscrivent toute utilisation secondaire, forcent l'effacement sécuritaire des informations confidentielles à la fin du contrat, affirment que toute fuite causera un préjudice à l'autre organisation, s'assurent de gérer un engagement de confidentialité à son personnel devant avoir accès aux informations confidentielles, etc.;**
- **la gestion des incidents de confidentialité, notamment le délai de notification qui doit être court (moins de 48 heures si possible), la collaboration nécessaire entre les organisations, l'escalade nécessaire selon la sévérité de l'incident, etc.;**
- **la prescription de pénalités;**
- **la notification préalable à tout changement au niveau du lieu de conservation des informations confidentielles;**
- **la limitation de responsabilité non abusive;**
- **la présence d'assurances adéquates en cybersécurité, en erreur et omission, en responsabilité civile ou autre.**

Il peut être opportun de valider les expériences antérieures du fournisseur pour évaluer son niveau de maturité organisationnelle en matière de gestion des identités numériques.

## 5.4. QUELLES SONT LES IMPLICATIONS SI JE VEUX COMMUNIQUER LES DONNÉES D'IDENTITÉ DE MON ORGANISATION ?

Les implications sont notamment d'ordre juridique et économique. En effet, la communication ou toute autre forme de mise à disposition des données en général et des renseignements personnels formant l'identité numérique des citoyens est une question sensible et parfois complexe. Les meilleures pratiques en la matière, quelle que soit la forme de traitement envisagée, prescrivent la protection stricte des libertés et droits fondamentaux des personnes physiques à l'égard de leurs renseignements personnels.

En clair, si l'organisation projette ou entreprend de communiquer ou de mettre à disposition des données relevant de l'identité numérique, elle doit rigoureusement s'assurer que tous les droits des personnes concernées en matière de traitement des renseignements personnels sont respectés et qu'elle se conforme à ses strictes obligations en (sa) qualité de responsable de la protection des renseignements personnels.

Le non-respect de ces exigences en matière de protection des renseignements personnels instaure un climat d'insécurité juridique au sein de l'organisation et l'expose à différentes sortes de sanctions (voir sections 4.4 , 5.6 et 5.8); toute chose pouvant impacter négativement son image et entraîner une perte de gains financiers.

Dans le contexte du marché unique du numérique, l'intensification de la circulation et de la valorisation économique du capital informationnel sont récurrentes au point où, l'on assiste souvent à des cas de fusion, de partenariats ou d'acquisition d'entreprises avec leur capital informationnel. La question de la revente des données détenues par l'entreprise pourrait alors se poser.

S'agissant particulièrement de la revente en pareil cas, l'organisation doit être consciente du risque que certaines informations révèlent des renseignements personnels, notamment d'identité numérique. Dès lors, les meilleures pratiques susmentionnées devraient être adoptées par prudence, y compris le recours aux techniques d'anonymisation en fonction de la sensibilité des données.

## 5.5. QU'EST-CE QU'UN CONSENTEMENT ADÉQUAT LORSQUE JE COMMUNIQUE DES INFORMATIONS LIÉES À L'IDENTITÉ NUMÉRIQUE ?

Dans la mesure où des renseignements personnels sont en cause, la communication de ceux-ci à l'insu de la personne concernée ou avec son consentement est limitée aux exceptions prévues par la législation. Une organisation voulant revendre de tels renseignements serait avisée de s'assurer que les personnes concernées soient en mesure d'y consentir en employant un langage simple.

Pour y voir plus clair et mesurer la portée des attentes en matière de consentement, il pourrait être sage de prendre connaissance des conclusions du Commissariat à la protection de la vie privée du Canada dans l'enquête conjointe au sujet de Facebook inc. :

> "71. Afin que le consentement soit considéré comme étant valable, les organisations doivent informer les personnes de leurs pratiques en matière de confidentialité de manière claire, détaillée et compréhensible. La communication de ces renseignements devrait être indiquée en temps opportun, afin que les utilisateurs disposent d'une information et d'un contexte pertinents pour prendre une décision éclairée avant que leurs renseignements personnels ne soient recueillis, utilisés ou communiqués. Depuis juin 2015, la Loi sur la protection des renseignements personnels et les documents électroniques prévoit également que le consentement d'un intéressé n'est valable que s'il est raisonnable de s'attendre à ce qu'il comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti."[14]

**14** Commissariat à la protection de la vie privée du Canada, Enquête conjointe du Commissariat à la protection de la vie privée du Canada et du Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique au sujet de Facebook, Inc., rapport de conclusions n°2019-002 du 25 avril 2019.

## 5.6. LA PROTECTION DES DONNÉES COÛTE-T-ELLE CHER?

Dans le cadre de traitement de données, les organisations ont accès à de plus en plus de moyens de se protéger, et par le même fait, protéger leur clientèle. La logique est simple : sans sécurité des données, l'organisation devra affronter des réactions vives de la part de sa clientèle, des poursuites et une baisse rapide de ses revenus. La question n'est pas de savoir si les organisations seront victimes d'un incident de confidentialité, mais plutôt quand? Et, si nous nous fions aux sondages récents concernant les entreprises canadiennes, les cyberattaques touchent annuellement plus d'une entreprise sur quatre[15].

Plusieurs mesures requièrent peu ou pas de technologies et demeurent économiques. Ainsi, les politiques liées à la confidentialité des données sont à la base des mesures à mettre en place. (voir sections 4.2 et 4.3). Il faut également s'assurer d'avoir informé et formé le personnel de l'organisation à la confidentialité des données (causes, comportements à risques, impacts). Enfin, dans le cadre de la relation avec les fournisseurs, les organisations doivent s'assurer que les obligations contractuelles soient adéquates (section 5.3). Ces mesures permettent d'augmenter rapidement la maturité organisationnelle en matière de protection des identités numériques.

Par exemple, une plateforme Web a été créée par l'entreprise X et vendue au client Y. Le visiteur se rend sur la plateforme et saisie des données d'identité. Ces données vont transiter par la plateforme de l'entreprise X pour aller s'entreposer au sein des bases de données du client Y. L'entreprise X doit donc signifier dans les politiques de confidentialités, les conditions d'utilisations de la plateforme, la façon dont le traitement des données est effectué.

Enfin, une firme spécialisée en cybersécurité conseillera judicieusement les dirigeants sur les mesures les plus appropriées au regard de leurs obligations, de leur structure organisationnelle, des systèmes d'information et du marché.

## 5.7. QUELLES SONT LES MESURES DE SÉCURITÉ MINIMALES QUE MON ORGANISATION DOIT METTRE EN PLACE POUR ASSURER ADÉQUATEMENT LA PROTECTION DE L'IDENTITÉ NUMÉRIQUE?

Les mesures de protection de sécurité touchent différents aspects, notamment :

- **La documentation des principes, rôles, responsabilités, obligations, pénalités et dérogations dans des politiques;**
- **Le développement des procédures assurant une répétabilité des activités sensibles;**

**15** Voir IT.Rends sur https://info.novipro.com/en/it-trends

- **La gestion des accès aux systèmes gérant l'identité numérique;**
- **La protection des appareils et des réseaux de l'organisation, notamment par des antivirus et des pare-feux;**
- **Les systèmes de surveillance des systèmes et la détection proactive de situations anormales;**
- **Le maintien des mises à jour des actifs informationnels, notamment pour ceux contenant des informations confidentielles.**

Ces mesures doivent être adaptées à la réalité de chaque organisation et de son environnement. Elles évoluent au rythme des technologies, des meilleures pratiques, des menaces, etc. En ce sens, il est important de suivre minimalement les recommandations gouvernementales[16].

## 5.8. EST-CE QUE MON ORGANISATION DEMEURE RESPONSABLE DU RESPECT DES OBLIGATIONS CONCERNANT LA PROTECTION DES IDENTITÉS NUMÉRIQUES LORSQU'ELLE UTILISE L'INFONUAGIQUE?

Les organisations demeurent toujours responsables de la protection de ses identités numériques, peu importe si celles-ci sont conservées à l'intérieur ou à l'extérieur de ses murs, si elles sont gérées par ses employés, des contractants ou par une ou des firmes externes. Cette responsabilité est fondamentale, notamment pour les personnes qui font affaire avec l'organisation ou qui y travaillent. De plus, les dirigeants de l'organisation demeurent responsables de la proportionnalité et de l'adéquation des mesures de protection qui sont mises en place.

Ainsi, une organisation est tenue d'agir au mieux des intérêts de ses clients, avec prudence et diligence, et ce, même en cas de sous-traitance de la gestion de renseignements personnels de ses clients. L'organisation est également tenue d'agir conformément aux meilleures pratiques en la matière. Le droit de l'Union européenne est plus précis encore sur ce point : un contrat de sous-traitance doit être conclu entre l'organisation et le prestataire à qui le traitement de renseignements personnels est délégué.

Dès lors, toute personne qui subit un dommage, du fait d'un traitement illégal, inadéquat ou déraisonnable des informations relevant de l'identité numérique, a le droit d'obtenir de l'organisation ainsi que de ses sous-traitants, réparation du préjudice subi. Notons que le sous-traitant n'est tenu pour responsable du dommage causé par le traitement illégal, que s'il n'a pas respecté ses obligations spécifiques prévues dans le contrat de sous-traitance ou, qu'il a agi en dehors des instructions autorisées de l'organisation ou contrairement à celles-ci.

**16** Basic Cybersecurity Controls for Small and Medium Organizations, Canadian Centre for Cybersecurity, https://cyber.gc.ca/fr/orientation/controles-de-cybersecurite-de-base-pour-les-petites-et-moyennes-organisations

# 6. LES BÉNÉFICES POUR MON ORGANISATION

## 6.1. À QUOI PUIS-JE M'ATTENDRE COMME BÉNÉFICES POUR MON ORGANISATION?

Toute action d'amélioration de la gestion des données d'identité numérique est aussi une occasion d'augmenter la maturité numérique de l'organisation et, lorsque bien exécutée, peut engendrer des retombées positives. C'est le cas notamment pour les organisations transigeant en ligne, en réduisant le temps, les coûts et les erreurs liés à l'identification des personnes. De plus, un système d'identité numérique facilite la vérification de l'identité numérique de vos clients en reconnaissant les faux et les usages frauduleux. Par exemple, l'organisation pourrait détecter les personnes faisant usage de ses services en utilisant les données d'identité d'une autre personne, comme l'usage d'un abonnement à un service numérique en ligne ou à une salle d'entraînement.

La mise en place de pratiques reconnues peut également améliorer l'image de marque et la confiance de la clientèle. Avec une conscientisation croissante de la population, les organisations démontrant une capacité supérieure à protéger et gérer adéquatement l'identité numérique gagneront la confiance du public et réduiront les obstacles à l'utilisation de leurs services numériques.

Enfin, une gestion formelle de l'identité numérique peut prémunir l'organisation contre la fraude en ligne alors que l'économie numérique est en plein essor ou réduire le risque d'incidents et donc les pertes économiques associées.

## 6.2. ET POUR MA CLIENTÈLE?

On note trois grandes catégories de bénéfices que peut représenter la mise en place d'un système d'identité numérique à grande échelle pour la clientèle et la population. D'une part, elle pourrait permettre d'offrir à la clientèle une expérience plus fluide et simple que ne le permettent plusieurs identités numériques actuelles. À titre d'exemple, cela pourrait se traduire par une réduction du volume de mots de passe à retenir, ainsi que par l'utilisation d'une même identité numérique pour divers services, qu'ils soient en ligne ou hors-ligne. D'autre part, elle dispose également du potentiel d'accroître l'inclusion financière de la population. En d'autres termes, cela se traduit par une plus grande facilité à obtenir des documents permettant de s'identifier en ligne pour les gens ne disposant pas de documents d'identification traditionnels (ex. permis de conduire) et donc, d'intégrer davantage l'économie numérique et devenir des clients potentiels. Finalement, cette identité numérique pourrait offrir un environnement numérique dans lequel la clientèle a davantage confiance.

### 6.3. ET POUR MON PERSONNEL?

La mise en place d'un système d'identité se traduit par une utilisation plus fluide, donc plus efficace, des systèmes de l'organisation. L'information sera mieux gérée et facilitera donc la création de valeur. Un sentiment de fierté, voire d'appartenance, du personnel devrait émerger. Dans un contexte où le recrutement de la main-d'œuvre est de plus en plus difficile, la gestion responsable des identités numériques du personnel peut constituer un atout pour recruter des personnes sensibles à ces considérations éthiques et légales. Un personnel dédié et sensible ne peut que constituer un atout pour une organisation qui gère les identités numériques, en favorisant le développement des bons comportements par les employés, et réduisant ainsi les risques d'incidents de confidentialité.

## 7. EN RÉSUMÉ

### 7.1. ÇA FAIT BEAUCOUP! EN RÉSUMÉ, SUR UNE PAGE, QU'EST-CE QU'IL FAUT QUE JE RETIENNE?

L'identité numérique est formée par l'ensemble des données permettant d'identifier une personne. Les gouvernements fédéral et provinciaux comprennent l'importance et la sensibilité de ces données et promulguent rapidement de nouvelles lois et règlements pour encadrer sa gestion. De nouvelles législations amènent des obligations de protection de ces données pour l'ensemble des organisations canadiennes, peu importe leur secteur d'activité ou leur taille.

Les identités numériques touchent tous les groupes de l'écosystème d'une organisation : les clients, les employés, les partenaires. Elles concernent les renseignements personnels, leurs interactions et le résultat d'analyses secondaires de celles-ci. Elles servent à établir la confiance entre les parties et se doivent d'être gérées activement.

La gestion des identités numériques se fait en s'appuyant sur différentes lois et règlements qui touchent l'ensemble de ses activités d'affaires, mais également à travers des principes de gouvernance généraux appliqués à la gestion responsable des technologies de l'information. Un gestionnaire avisé se doit de les connaître, de les intégrer au sein de ses activités quotidiennes et d'en surveiller le respect et la conformité à travers le temps.

Les dirigeants des organisations et les conseils d'administration sont responsables d'une saine gouvernance au niveau de la gestion des données liées à l'identité numérique. Ils doivent en superviser le risque et contribuer à en exploiter les bénéfices.

Un manquement à la protection des données liées à l'identité numérique peut entraîner de nombreuses conséquences qui touchent directement à la prospérité de l'organisation, notamment des amendes, des pertes financières, une incapacité temporaire à poursuivre ses activités d'affaires, et une perte réputationnelle. Pour réduire ce risque, une organisation doit sensibiliser l'ensemble de ses employés à adopter des comportements sécuritaires et avisés, à identifier les données faisant partie de l'identité numérique et les protéger en se dotant de pratiques adaptées à leur contexte et conformes aux lois et règlements en vigueur ou à venir.

Une conformité à la protection des données liées à l'identité numérique permettra à une organisation d'œuvrer au sein de l'écosystème d'affaires canadien et international de façon compétitive et pérenne. Elle contribuera à la faire reconnaître comme une organisation responsable, respectueuse et de confiance. À terme les avantages économiques, sociaux et environnementaux seront importants pour les organisations et l'ensemble de la société canadienne.

## 7.2. JE VEUX EN APPRENDRE DAVANTAGE, AVEZ-VOUS DES RESSOURCES À ME PARTAGER?

La gestion des données de l'identité numérique se développe rapidement au Canada. Il peut être utile d'exercer une veille sur les différents aspects du domaine. On offre ici quelques ressources qui peuvent être utiles pour les organisations œuvrant au pays et à l'international. Un recensement beaucoup plus détaillé de sources d'information est présenté à la fin de cet ouvrage pour les organisations souhaitant développer une compréhension détaillée du domaine.

### DÉMYSTIFIER L'IDENTITÉ NUMÉRIQUE

- **Puis-je voir votre pièce d'identité (numérique)? [Gouvernement du Canada]**
- **Identité numérique des citoyens [Deloitte]**
- **Service québécois d'identité numérique (en conception) [Gouvernement du Québec]**

### RESSOURCES SUR LA RÉGLEMENTATION

- **Règlement général sur la protection des données (RGPD) de l'Union européenne [Gouvernement du Canada]**
- **Projet de loi C-11 [Gouvernement du Canada]**

### GESTION DES DONNÉES DE L'IDENTITÉ NUMÉRIQUE

- **IDLab le laboratoire d'identité numérique [idlab.org]**
- **Conseil d'identification et d'authentification numériques du Canada [diacc.ca]**
- **Série sur les nouveaux enjeux économiques : L'identité numérique comme nouvelle frontière des politiques [Gouvernement du Canada]**

# BIBLIOGRAPHIE

## ACCEPTABILITÉ SOCIALE DE L'IDENTITÉ NUMÉRIQUE


[1] Dhamija, Rachna et Lisa Dusseault, « The Seven Flaws of Identity Management: Usability and Security Challenges », IEEE Security Privacy, vol. 6, no. 2, 2008, 24-29, consulté le 27/11/2021, DOI 10.1109/MSP.2008.49

[2] Adjei, Joseph et Henning Olesen, « Keeping Identity Private », IEEE Vehicular Technology Magazine, vol. 6, no. 3, 2011, 70-79, DOI 10.1109/MVT.2011.941894

[3] Gehman, Joel, Lianne M. Lefsrud et Stewart Fast, « Social license to operate: Legitimacy by another name? », Canadian Public Administration, vol. 60, no. 2, 2017, 293-317, DOI 10.1111/capa.12218

[4] Cespiva, R. B. (2018). Factors Influencing the Decision to Adopt a Digital Identity : A Correlational Study [D.I.T., Capella University]. In ProQuest Dissertations and Theses. https://www.proquest.com/docview/2124445405?pq-origsite=gscholar&fromopenview=true

[5] Digital Identity—Will the New Oil Create Fuel or Fire in Today's Economy? (s. d.). ISACA. Consulté 14 juillet 2021, à l'adresse https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/digital-identitywill-the-new-oil-create-fuel-or-fire-in-todays-economy

[6] Ishmaev, G., & Stokkink, Q. (2020). Identity Management Systems : Singular Identities and Multiple Moral Issues. Frontiers in Blockchain, 3. https://doi.org/10.3389/fbloc.2020.00015

[7] Kalvet, T., Tiits, M., & Laas-Mikko, K. (2018). Public Acceptance of Advanced Identity Documents. Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, 429 432. https://doi.org/10.1145/3209415.3209456

[8] Kim, A.-Y., & Kim, T.-S. (2016). FACTORS INFLUENCING THE INTENTION TO ADOPT IDENTITY THEFT PROTECTION SERVICES : SEVERITY VS VULNERABILITY. PACIS 2016 Proceedings. https://aisel.aisnet.org/pacis2016/68

[9] Klaus, T., Wingreen, S., & Blanton, J. E. (2007). Examining user resistance and management strategies in enterprise system implementations. Proceedings of the 2007 ACM SIGMIS CPR conference on Computer personnel research: The global information technology workforce, 55 62. https://doi.org/10.1145/1235000.1235013

[10] Mathieson, K. (1991). Predicting User Intentions : Comparing the Technology Acceptance Model with the Theory of Planned Behavior. Information Systems Research, 2(3), 173 191. https://doi.org/10.1287/isre.2.3.173

[11] Rocha, M. (2016). Data Privacy and Social Acceptance of Smart Meters. In Smart Grid Handbook (p. 1 9). American Cancer Society. https://doi.org/10.1002/9781118755471.sgd026

[12] Rome, J. D. (s. d.). Understanding Adoption Barriers of Superior Technologies to Authenticate and Protect Users from Ongoing Cyber Threats [Ph.D., Ashford University]. Consulté 14 juillet 2021, à l'adresse https://www.proquest.com/docview/2481091755/abstract/6531302EDF7A4386PQ/1

[13] Sindi, A. F. (s. d.). Adoption Factors of a Blockchain Digital Identity Management System in Higher Education : Diffusing a Disruptive Innovation [Ed.D., California State University, Los Angeles]. Consulté 16 juin 2021, à l'adresse https://www.proquest.com/docview/2359384031/abstract/7AA1753726E44F8EPQ/1

[14] The factors that influence small and medium enterprises' intention to adopt the government credit program | Emerald Insight. (s. d.). Consulté 16 juin 2021, à l'adresse https://www.emerald.com/insight/content/doi/10.1108/JRME-01-2020-0013/full/html#loginreload

[15] Tiits, M., Kalvet, T., & Mikko, K.-L. (2014). Social acceptance of epassports. 2014 International Conference of the Biometrics Special Interest Group (BIOSIG), 1 6.

## CONSENTEMENT

[16] J. Pandit, H., Jesus, V., Ammai, S., Lizar, M., & D'Agostino, S. (2021). Role of Identity, Identification, and Receipts for Consent. Gesellschaft für Informatik e.V. http://dl.gi.de/handle/20.500.12116/36495

## GESTION DES RISQUES

[17] Appendix_1_e1_maturity_model_for_identity_management_intrahealth_international_digital_square_notice_e1.pdf. (s. d.). Consulté 17 juin 2021, à l'adresse https://applications.digitalsquare.io/sites/default/files/notice-e1/1592580188/appendix_1_e1_maturity_model_for_identity_management_intrahealth_international_digital_square_notice_e1.pdf

[18] Approach for selecting the most suitable Automated Personal Identification Mechanism (ASMSA) | Elsevier Enhanced Reader. (s. d.). https://doi.org/10.1016/j.cose.2010.03.002

[19] Bhardwaj, A., & Kumar, V. (2011). Cloud security assessment and identity management. 14th International Conference on Computer and Information Technology (ICCIT 2011), 387 392. https://doi.org/10.1109/ICCITechn.2011.6164819

[20] Campbell-Verduyn, M., & Hütten, M. (2021). The Formal, Financial and Fraught Route to Global Digital Identity Governance. Frontiers in Blockchain, 4. https://doi.org/10.3389/fbloc.2021.627641

[21] Dans l'actualité – Système d'identité numérique solide au Canada | Dans l'actualité – Système d'identité numérique solide au Canada. (s. d.). Consulté 21 juin 2021, à l'adresse https://cba.ca/cba-in-the-news-Canada-needs-a-robust-digital-id-system?l=fr

[22] Farah, B. (2011). A Maturity Model for the Management of Information Technology Risk. The International Journal of Technology, Knowledge, and Society, 7(1), 13 26. https://doi.org/10.18848/1832-3669/CGP/v07i01/56174

[23] PalsonKennedy, R., & Gopal, T. V. (2010). Assessing the risks and opportunities of Cloud Computing—Defining identity management systems and maturity models. Trendz in Information Sciences Computing(TISC2010), 138 142. https://doi.org/10.1109/TISC.2010.5714625

[24] physical, T. authoritative resource for, & Security, C. (s. d.). Identity management best practice planning—Access & Identity Management Handbook 2011—Hi-Tech Security Solutions. Consulté 21 juin 2021, à l'adresse http://www.securitysa.com/regular.aspx?pklregularid=4702

[25] Rapport-transformation-numerique-fr.pdf. (s. d.). Consulté 21 juin 2021, à l'adresse https://lautorite.qc.ca/fileadmin/lautorite/grand_public/publications/professionnels/rapport-transformation-numerique-fr.pdf

[26] Rasouli, H., Valmohammadi, C., Azad, N., & Esfeden, G. A. (s. d.). Proposing a digital identity management framework : A mixed-method approach. Concurrency and Computation: Practice and Experience, n/a(n/a), e6271. https://doi.org/10.1002/cpe.6271

[27] WEF_Digital_Identity_Strategic_Imperative.pdf. (s. d.). Consulté 23 juin 2021, à l'adresse http://www3.weforum.org/docs/WEF_Digital_Identity_Strategic_Imperative.pdf

## GOUVERNANCE DE L'IDENTITÉ NUMÉRIQUE

[28] 6_Rannenberg_framework_for_identity_management.pdf. (s. d.). Consulté 23 juin 2021, à l'adresse https://fg-secmgt.gi.de/fileadmin/FG/SECMGT/2012/6_Rannenberg_framework_for_identity_management.pdf

[29] Bernabe, J. B., David, M., Moreno, R. T., Cordero, J. P., Bahloul, S., & Skarmeta, A. (2020). ARIES : Evaluation of a reliable and privacy-preserving European identity management framework. Future Generation Computer Systems, 102, 409 425. https://doi.org/10.1016/j.future.2019.08.017

[30] Bucík, B. D. F. (2021). Optimisation of user digital identity gathering process. 100.

[31] Huang, J., Wu, M., & Huang, Y. (2020). Research and Application of eID Digital Identity. Proceedings of the 2nd International Conference on Artificial Intelligence and Advanced Manufacture, 266 270. https://doi.org/10.1145/3421766.3421830

[32] Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, Privacy and Risks Within Smart Cities : Literature Review and Development of a Smart City Interaction Framework. Information Systems Frontiers. https://doi.org/10.1007/s10796-020-10044-1

[33] Kabwe, F., & Phiri, J. (2019). A Framework For Digital Identity Management.

[34] Maldonado-Ruiz, D., Torres, J., El Madhoun, N., & Badra, M. (2021). An Innovative and Decentralized Identity Framework Based on Blockchain Technology. 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 1 8. https://doi.org/10.1109/NTMS49979.2021.9432656

[35] NIST Special Publication 800-63-3. (s. d.). Consulté 8 juillet 2021, à l'adresse https://pages.nist.gov/sp800-63-3.html

[36] Rasouli, H., Valmohammadi, C., Azad, N., & Esfeden, G. A. (s. d.). Proposing a digital identity management framework : A mixed-method approach. Concurrency and Computation: Practice and Experience, n/a(n/a), e6271. https://doi.org/10.1002/cpe.6271

[37] Sarmiento, D. L. (2014, février 28). A conceptual framework for an interoperable online identity management system [Info:eu-repo/semantics/masterThesis]. University of Twente. https://essay.utwente.nl/64801/

[38] Staite, C. (2012). Identity management architecture and implementation : Evaluation and improvement [D_ph, University of Birmingham]. https://etheses.bham.ac.uk/id/eprint/3388/

[39] The-Sequoia-Project-Framework-for-Patient-Identity-Management.pdf. (s. d.). Consulté 21 juin 2021, à l'adresse https://sequoiaproject.org/wp-content/uploads/2015/11/The-Sequoia-Project-Framework-for-Patient-Identity-Management.pdf

## GESTION DE L'IDENTITÉ NUMÉRIQUE

[40] D6.1.2-economic_valuation_of_identity_management_enablers-public.pdf. (s. d.). Consulté 8 juillet 2021, à l'adresse http://primelife.ercim.eu/images/stories/deliverables/d6.1.2-economic_valuation_of_identity_management_enablers-public.pdf

[41] Preibusch, S., Kübler, D., & Beresford, A. R. (2013). Price versus privacy : An experiment into the competitive advantage of collecting less personal information. Electronic Commerce Research, 13(4), 423 455. https://doi.org/10.1007/s10660-013-9130-3

[42] Private Sector Economic Impacts from Identification Systems. (s. d.). [Text/HTML]. World Bank. Consulté 3 juin 2021, à l'adresse https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/219201522848336907/Private-Sector-Economic-Impacts-from-Identification-Systems

[43] Understanding Cost Drivers of Identification Systems. (s. d.). [Text/HTML]. World Bank. Consulté 3 juin 2021, à l'adresse https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/702641544730830097/Understanding-Cost-Drivers-of-Identification-Systems

[44] Jackson, P. M., Ligertwood, J., O'Donnell, J., & Shelly, M. (s. d.). Small Business : Issues of Identity Management, Privacy and Security. 15.

## IDENTITÉ NUMÉRIQUE AUTOSOUVERAINE

[45] 200820-Digital-Wallet-Interview-findings-report.pdf. (s. d.). Consulté 8 juillet 2021, à l'adresse https://www.swinburne.edu.au/media/swinburneeduau/research-institutes/smart-cities/200820-Digital-Wallet-Interview-findings-report.pdf

[46] Alsobhi, H., Mirdad, A., Alotaibi, S., Almadani, M., Alanazi, I., Alalyan, M., Alharbi, W., Alhazmi, R., & Hussain, F. K. (2021). Innovative Blockchain-Based Applications—State of the Art and Future Directions. In L. Barolli, I. Woungang, & T. Enokido (Éds.), Advanced Information Networking and Applications (p. 323 335). Springer International Publishing. https://doi.org/10.1007/978-3-030-75078-7_33

[47] Banihashemi, S., Homayounvala, E., Talebpour, A., & Abhari, A. (2016). Identifying and Prioritizing Evaluation Criteria for User-Centric Digital Identity Management Systems. International Journal of Advanced Computer Science and Applications, 7(7). https://doi.org/10.14569/IJACSA.2016.070707

[48] Campbell-Verduyn, M., & Hütten, M. (2021). The Formal, Financial and Fraught Route to Global Digital Identity Governance. Frontiers in Blockchain, 4. https://doi.org/10.3389/fbloc.2021.627641

[49] Coutor, S., Hennebert, C., & Faher, M. (s. d.). BLOCKCHAIN ET IDENTIFICATION NUMERIQUE. 102.

[50] De Filippi, P. (2016). The Interplay between Decentralization and Privacy : The Case of Blockchain Technologies (SSRN Scholarly Paper ID 2852689). Social Science Research Network. https://papers.ssrn.com/abstract=2852689

[51] Digital Identity. (s. d.). Consulté 23 juin 2021, à l'adresse https://learning.oreilly.com/library/view/digital-identity/0596008783/

[52] Gilani, K., Bertin, E., Hatin, J., & Crespi, N. (2020). A Survey on Blockchain-based Identity Management and Decentralized Privacy for Personal Data. 2020 2nd Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS), 97 101. https://doi.org/10.1109/BRAINS49436.2020.9223312

[53] Ishmaev, G., & Stokkink, Q. (2020). Identity Management Systems : Singular Identities and Multiple Moral Issues. Frontiers in Blockchain, 3. https://doi.org/10.3389/fbloc.2020.00015

[54] Kakarlapudi, P. V., & Mahmoud, Q. H. (2021). A Systematic Review of Blockchain for Consent Management. Healthcare, 9(2), 137. https://doi.org/10.3390/healthcare9020137

[55] Lesavre, L., Varin, P., Mell, P., Davidson, M., & Shook, J. (2020). A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems (p. 62 62). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.01142020

[56] Mahula, S., Tan, E., & Crompvoets, J. (2021). With blockchain or not? Opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the Belgian case. DG.O2021: The 22nd Annual International Conference on Digital Government Research, 495 504. https://doi.org/10.1145/3463677.3463705

[57] Maldonado-Ruiz, D., Torres, J., El Madhoun, N., & Badra, M. (2021). An Innovative and Decentralized Identity Framework Based on Blockchain Technology. 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 1 8. https://doi.org/10.1109/NTMS49979.2021.9432656

[58] Meghana, A. R., & Krishna, C. V. R. (2020). Identity Management Using Blockchain Technology. 3(10), 6.

[59] Nchinda, N., Cameron, A., Retzepi, K., & Lippman, A. (2019). MedRec : A Network for Personal Information Distribution. 2019 International Conference on Computing, Networking and Communications (ICNC), 637 641. https://doi.org/10.1109/ICCNC.2019.8685631

[60] Pannifer, S. (2021, juin 17). Digital Identity Wallets are coming. Consult Hyperion. https://chyp.com/2021/06/17/digital-identity-wallets-are-coming/

[61] Rahman, S. M. T. (s. d.). BUSINESS MODEL OF BLOCKCHAIN ENABLED SMART CITY SERVICES. 134.

[62] Rathee, T., & Singh, P. (in press). A systematic literature mapping on secure identity management using blockchain technology. Journal of King Saud University- Computer and Information Sciences.

[63] Ruoti, S., Kaiser, B., Yerukhimovich, A., Clark, J., & Cunningham, R. (2019). SoK : Blockchain Technology and Its Potential Use Cases. arXiv:1909.12454 [cs]. http://arxiv.org/abs/1909.12454

[64] Sahmim, S., Gharsellaoui, H., & Bouamama, S. (2019). Edge Computing : Smart Identity Wallet Based Architecture and User Centric. Procedia Computer Science, 159, 1246 1257. https://doi.org/10.1016/j.procs.2019.09.294

[65] Schanzenbach, M. (s. d.). Towards Self-sovereign, Decentralized Personal Data Sharing and Identity Management. 183.

[66] Schanzenbach, M., Grothoff, C., Wenger, H., & Kaul, M. (2021). Decentralized Identities for Self-sovereign End-users (DISSENS). Schanzenbach, Martin; Grothoff, Christian; Wenger, Hansjürg; Kaul, Maximilian (2021). Decentralized Identities for Self-Sovereign End-Users (DISSENS) In: Open Identity Summit. Gesellschaft Für Informatik. Open Identity Summit, Lyngby, Denmark. https://oid2021.compute.dtu.dk/

[67] Sin, E. S., & Naing, T. T. (2021). Digital Identity Management System Using Blockchain Technology. In D. Gupta, A. Khanna, S. Bhattacharyya, A. E. Hassanien, S. Anand, & A. Jaiswal (Éds.), International Conference on Innovative Computing and Communications (p. 895 906). Springer. https://doi.org/10.1007/978-981-15-5148-2_78

[68] Sindi, A. F. (s. d.). Adoption Factors of a Blockchain Digital Identity Management System in Higher Education : Diffusing a Disruptive Innovation [Ed.D., California State University, Los Angeles]. Consulté 16 juin 2021, à l'adresse https://www.proquest.com/docview/2359384031/abstract/7AA1753726E44F8EPQ/1

[69] Stasis, A., Triantafyllou, N., Georgakopoulos, P., Armitt, R. L., & Kavassalis, P. (s. d.). Designing an academic electronic identity management system for student mobility using eIDAS eID and Self-Sovereign Identity technologies. 12.

[70] The Path to Self-Sovereign Identity. (s. d.). Consulté 23 juin 2021, à l'adresse http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[71] Van Wingerde, M. (2017). BLOCKCHAIN-ENABLED SELF-SOVEREIGN IDENTITY An exploratory study into the concept Self-Sovereign Identity and how blockchain technology can serve the fundamental basis. https://doi.org/10.13140/RG.2.2.17693.82406

## MENACES

[72] Branker, J., Eveleigh, T., Holzer, T. H., & Sarkani, S. (2016). Access control, identity management and the insider threat. Journal of Airport Management, 10(2), 180 199.

[73] EBSCOhost | 93980989 | Online Identity Theft : A Longitudinal Study Of Individual Threat-Response And Coping Behaviors. (s. d.). Consulté 16 juin 2021, à l'adresse https://eds.b.ebscohost.com/abstract?site=eds&scope=site&jrnl=15512002&asa=Y&AN=93980989&h=pDeGe%2bCBIhpfaKiMJ0LHzWrJpo7EMh44ZKaEfoVIJBzTsoJkdxwJzLY7bEQQue8XQI3YXurmqzdkkicBPoeqcQ%3d%3d&crl=c&resultLocal=ErrCrlNoResults&resultNs=Ehost&crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d15512002%26asa%3dY%26AN%3d93980989

[74] Fritsch, L. (2020). Identity Management as a target in cyberwar. Gesellschaft für Informatik e.V. https://doi.org/10.18420/ois2020_05

[75] Zaiss, J., Zaeem, R. N., & Barber, K. S. (2019). Identity Threat Assessment and Prediction. Journal of Consumer Affairs, 53(1), 58 70. https://doi.org/10.1111/joca.12191

## MODÈLES DE CONFIANCE

[76] Castro, P., & Bettencourt, L. (2017). Exploring the predictors and the role of trust and concern in the context of data disclosure to governmental institutions. Behaviour & Information Technology, 36(3), 321 331. https://doi.org/10.1080/0144929X.2016.1234645

[77] Koshy, L. (2018). Identity and trust management in distributed systems – a novel approach. https://uobrep.openrepository.com/handle/10547/624021

[78] Palage, M. (s. d.). Digital Identity and Trust Frameworks. 11.

[79] Seltsikas, P., & O'keefe, R. M. (2010). Expectations and outcomes in electronic identity management : The role of trust and public value. European Journal of Information Systems, 19(1), 93 103. ABI/INFORM Collection. https://doi.org/10.1057/ejis.2009.51

[80] Smedinghoff, T. J. (s. d.). The Duty to Verify Identity : A Critical Component of Privacy and Security Compliance. 22.

[81] Warkentin, M., Gefen, D., Pavlou, P. A., & Rose, G. M. (2002). Encouraging Citizen Adoption of e-Government by Building Trust. Electronic Markets, 12(3), 157 162. https://doi.org/10.1080/101967802320245929

[82] Yanushkevich, S. N., Howells, W. G., Crockett, K. A., O'Shea, J., Oliveira, H. C. R., Guest, R. M., & Shmerko, V. P. (2019). Cognitive Identity Management : Risks, Trust and Decisions using Heterogeneous Sources. 2019 IEEE First International Conference on Cognitive Machine Intelligence (CogMI), 33 42. https://doi.org/10.1109/CogMI48466.2019.00014

[83] Yanushkevich, S., Stoica, A., Shmerko, P., Howells, W., Crockett, K., & Guest, R. (2020). Cognitive Identity Management : Synthetic Data, Risk and Trust. 2020 International Joint Conference on Neural Networks (IJCNN), 1 8. https://doi.org/10.1109/IJCNN48605.2020.9207385

## PRATIQUES INNOVANTES INTERNATIONALES


[84] Abolarin, K. (2021). DATA GOVERNANCE AND DATA QUALITY GUIDELINES FOR NATIONAL IDENTITY MANAGEMENT COMMISION (NIMC).

[85] Argentina ID Case Study. (2020). World Bank. https://doi.org/10.1596/33403

[86] Argentina ID Case Study : The Evolution of Identification. (s. d.). [Text/HTML]. World Bank. Consulté 3 juin 2021, à l'adresse https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/318351582559995027/Argentina-ID-Case-Study-The-Evolution-of-Identification

[87] Boysen, A. (2021). Decentralized, Self-Sovereign, Consortium : The Future of Digital Identity in Canada. Frontiers in Blockchain, 4. https://doi.org/10.3389/fbloc.2021.624258

[88] Gruszka, B. (s. d.). Identity Management in Developing Countries : A SWOT-Analysis. . . INTRODUCTION, 8.

[89] Guidelines-for-ID4D-Diagnostics.pdf. (s. d.). Consulté 3 juin 2021, à l'adresse https://documents1.worldbank.org/curated/en/370121518449921710/Guidelines-for-ID4D-Diagnostics.pdf

[90] ID4D Practitioner's Guide. (s. d.). [Text/HTML]. World Bank. Consulté 3 juin 2021, à l'adresse https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/ID4D-Practitioner-s-Guide

[91] ID-Enrollment-Strategies-Practical-Lessons-From-Around-The-Globe.pdf. (s. d.). Consulté 8 juillet 2021, à l'adresse https://documents1.worldbank.org/curated/en/539361582557916734/pdf/ID-Enrollment-Strategies-Practical-Lessons-From-Around-The-Globe.pdf

[92] Identification for Development (ID4D) 2018 Annual Report. (s. d.). [Text/HTML]. World Bank. Consulté 3 juin 2021, à l'adresse https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/967301587472879585/Identification-for-Development-ID4D-2018-Annual-Report

[93] Jefferson, K. A. (2015). What's in a Name : A Comparative Analysis of the United States Real ID Act and the United Kingdom's National Identity Scheme. NAVAL POSTGRADUATE SCHOOL MONTEREY CA. https://apps.dtic.mil/sti/citations/ADA632277

[94] Makarim, E. (2021). Privacy and Personal Data Protection in Indonesia : The Hybrid Paradigm of the Subjective and Objective Approach. In E. Kiesow Cortez (Éd.), Data Protection Around the World : Privacy Laws in Action (p. 127 164). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-407-5_6

[95] Micky, L., & Peichi, C. (2021). Media Technologies for Work and Play in East Asia : Critical Perspectives on Japan and the Two Koreas. Policy Press.

[96] Mir, U. B., Kar, A. K., Dwivedi, Y. K., Gupta, M. P., & Sharma, R. S. (2020). Realizing digital identity in government : Prioritizing design and implementation objectives for Aadhaar in India. Government Information Quarterly, 37(2), 101442. https://doi.org/10.1016/j.giq.2019.101442

[97] Moldova Mobile ID Case Study. (s. d.). [Text/HTML]. World Bank. Consulté 3 juin 2021, à l'adresse https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/279851545919735993/Moldova-Mobile-ID-Case-Study

[98] Mutung'u, G., & Rutenberg, I. (2020). Digital ID and Risk of Statelessness Critique and Commentary. Statelessness & Citizenship Review, 2(2), 348 354.

[99] Noack, T., & Kubicek, H. (2010). The introduction of online authentication as part of the new electronic national identity card in Germany. Identity in the Information Society, 3(1), 87 110. https://doi.org/10.1007/s12394-010-0051-1

[100] Relying Party Guidance. (s. d.-a). 91.

[101] Relying Party Guidance. (s. d.-b). 91.

[102] Schwabe, D., Laufer, C., & Casanovas, P. (2020). Knowledge Graphs : Trust, Privacy, and Transparency from a Legal Governance Approach. Law in Context. A Socio-legal Journal, 37, 24 41. https://doi.org/10.26826/law-in-context.v37i1.126

[103] South Africa ID Case Study. (s. d.). [Text/HTML]. World Bank. Consulté 3 juin 2021, à l'adresse https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/315081558706143827/South-Africa-ID-Case-Study

[104] Teslya, N., Mikhailov, S., & Ryabchikov, I. (2019). Forming of Smart City Resident Digital Identity Based On the City Sources Analysis. IEEE International Black Sea Conference on Communications and Networking. BlackSeaCom.

[105] The State of identification systems in Africa – a synthesis of country assessments. (s. d.). [Text/HTML]. World Bank. Consulté 3 juin 2021, à l'adresse https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/156111493234231522/The-State-of-identification-systems-in-Africa-a-synthesis-of-country-assessments

[106] The state of identification systems in Africa : Country briefs. (s. d.). [Text/HTML]. World Bank. Consulté 3 juin 2021, à l'adresse https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/298651503551191964/The-state-of-identification-systems-in-Africa-country-briefs

[107] Tupay, P. K. (2020). Estonia, the Digital Nation : Reflections on a Digital Citizen's Rights in the European Union Reports: Estonia. European Data Protection Law Review (EDPL), 6(2), 294 300.

## PRINCIPES DE BASE

[108] Axioms for the Practice of Security Architecture. (s. d.). Consulté 21 septembre 2021, à l'adresse https://publications.opengroup.org/downloadable/download/link/id/MC42MTc5MjcwMCAxNjMyMjM2NzE5MTA5NDQzMjExMTk4MTgxMDY2/

[109] Bazarhanova, A., & Smolander, K. (s. d.). The Review of Non-Technical Assumptions in Digital Identity Architectures. 10.

[110] Beduschi, A. (2019). Digital identity : Contemporary challenges for data protection, privacy and non-discrimination rights. Big Data & Society, 6(2), 2053951719855091. https://doi.org/10.1177/2053951719855091

[111] Bhandari, V., Trikanad, S., & Sinha, A. (2020). Governing ID : Principles of Evaluation (SSRN Scholarly Paper ID 3774917). Social Science Research Network. https://papers.ssrn.com/abstract=3774917

[112] Dhamija, R., & Dusseault, L. (2008). The Seven Flaws of Identity Management : Usability and Security Challenges. IEEE Security Privacy, 6(2), 24 29. https://doi.org/10.1109/MSP.2008.49

[113] Digital identity : Towards shared principles for public and private sector cooperation. (s. d.). [Text/HTML]. World Bank. Consulté 3 juin 2021, à l'adresse https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/600821469220400272/Digital-identity-towards-shared-principles-for-public-and-private-sector-cooperation

[114] Dubois, E., & Martin-Bariteau, F. (2020). Next Steps for a Connected Canada (SSRN Scholarly Paper ID 3620182). Social Science Research Network. https://papers.ssrn.com/abstract=3620182

[115] Ferdous, Md. S., Norman, G., & Poet, R. (2014). Mathematical Modelling of Identity, Identity Management and Other Related Topics. Proceedings of the 7th International Conference on Security of Information and Networks, 9 16. https://doi.org/10.1145/2659651.2659729

[116] Hühnlein, D., Roßnagel, H., & Zibuschka, J. (2010). Diffusion of federated identity management. Gesellschaft für Informatik e.V. http://dl.gi.de/handle/20.500.12116/19795

[117] Jericho Forum Identity Commandments. (s. d.). Consulté 21 septembre 2021, à l'adresse https://publications.opengroup.org/downloadable/download/link/id/MC40MjM1OTQwMCAxNjMyMjM2OTcwMTA5NDQ1MzExMTk4MzkzMTk%2C/

[118] Khatchatourov, A., & Chardel, P.-A. (s. d.). The ethical challenges of digital identity. La Conversation. Consulté 8 juillet 2021, à l'adresse http://theconversation.com/the-ethical-challenges-of-digital-identity-126564

[119] Khatchatourov, A., & Chardel, P.-A. (2019). The ethical challenges of digital identity. The Conversation France. https://hal.archives-ouvertes.fr/hal-03126022

[120] Solove, D. J. (2004). The Digital Person : Technology and Privacy in the Information Age (SSRN Scholarly Paper ID 2899131). Social Science Research Network. https://papers.ssrn.com/abstract=2899131

[121] Sullivan, C. (s. d.). Digital Identity. 182.

[122] Wessels, B. (2012). Identification and the practices of identity and privacy in everyday digital communication. New Media & Society, 14(8), 1251 1268. https://doi.org/10.1177/1461444812450679

## OBLIGATIONS LÉGALES CANADIENNES

[123] Charte des droits et libertés de la personne, RLRQ c. C-12.

[124] Code civil du Québec

[125] Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ c. P-39.1.

[126] Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, L.Q. 2021, c. 25.

[127] Loi concernant le cadre juridique des technologies de l'information, RLRQ c. C-1.1.

[128] Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5.

[129] Loi édictant la Loi sur le ministère de la Cybersécurité et du Numérique et modifiant d'autres dispositions, L.Q. 2021, c. 33.

[130] Règlement (UE) 2016/79 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques, à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[131] Code criminel, L.R.C. (1985), ch. C-46.

[132] Loi n° 1.483 du 17 décembre 2019 relative à l'identité numérique de la Principauté de Monaco, Journal de Monaco du 27 déc. 2019.

## REVUES SYSTÉMATIQUES

[133] Ante, L., Fischer, C., & Strehle, E. (s. d.). A bibliometric review of research on digital identity. 33.

[134] Bazarhanova, A., & Smolander, K. (2020, janvier 7). The Review of Non-Technical Assumptions in Digital Identity Architectures. https://doi.org/10.24251/HICSS.2020.785

[135] Cao, Y., & Yang, L. (2010). A survey of identity management technology. Proceedings 2010 IEEE International Conference on Information Theory and Information Security, 287293.

[136] ID Enrollment Strategies : Practical Lessons From Around The Globe. (s. d.). [Text/HTML]. World Bank. Consulté 3 juin 2021, à l'adresse https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/539361582557916734/ID-Enrollment-Strategies-Practical-Lessons-From-Around-The-Globe

[137] Mburu, Z. G., Nderu, D. L., & Tobias, D. M. (2019). REVIEW OF DIGITAL IDENTITY MANAGEMENT SYSTEM MODELS. International Journal of Technology and Systems, 4(1), 2133.

[138] Pöhn, D., & Hommel, W. (2020). An overview of limitations and approaches in identity management. Proceedings of the 15th International Conference on Availability, Reliability and Security, 110. https://doi.org/10.1145/3407023.3407026

[139] Torres, J., Macedo, R., Nogueira, M., & Pujolle, G. (2012). Identity Management Requirements in Future Internet.

[140] Wessels, B. (2012). Identification and the practices of identity and privacy in everyday digital communication. New Media & Society, 14(8), 12511268. https://doi.org/10.1177/1461444812450679

## UNICITÉ

[141] Duncan, J. D. (s. d.). Birth of identity : Understanding the value and policy considerations of using birth certificates for identity resolution [Ph.D., The University of Utah]. Consulté 8 juillet 2021, à l'adresse https://www.proquest.com/docview/1765692866/abstract/E6AD1EE7E15A4051PQ/1

[142] Edwards, M. J. (s. d.). Data Quality Measures for Identity Resolution [Ph.D., Lancaster University (United Kingdom)]. Consulté 8 juillet 2021, à l'adresse https://www.proquest.com/docview/2083742845/abstract/B84F15BBC077469FPQ/1

[143] Helland, P. (2019). Identity by any other name. Communications of the ACM, 62(4), 8080. https://doi.org/10.1145/3303870

[144] Janssen, J. (s. d.). Identity management within an organization. 96.

[145] Kumaraguru, P. (s. d.). Submitted By Rishabh Kaushal PhD15008. 50.

[146] Lin, T., & Misra, S. (2021). The Identity Fragmentation Bias. arXiv:2008.12849 [econ, stat]. http://arxiv.org/abs/2008.12849

[147] Staite, C., & Bahsoon, R. (2012). Evaluating identity management architectures. Proceedings of the 3rd international ACM SIGSOFT symposium on Architecting Critical Systems. ISARCS, New York.

[148] Wang, G. A., Atabakhsh, H., & Chen, H. (2011). A hierarchical Naïve Bayes model for approximate identity matching. Decision Support Systems, 51(3), 413. ABI/INFORM Collection.

## VIE PRIVÉE

[149] A Novel Methodology for Security and Privacy Protection Issues of Data in Cloud Computing-Indian Journals. (s. d.). Consulté 16 juin 2021, à l'adresse https://www.indianjournals.com/ijor.aspx?target=ijor:ijemr&volume=6&issue=1&article=026

[150] Abdu, N. J., & Lechner, U. (2016). A Threat Analysis Model for Identity and Access Management. Proceedings of the 2nd International Conference on Information Systems Security and Privacy, 498502.

[151] Agre, P. E. (1999). THE ARCHITECTURE OF IDENTITY : Embedding privacy in market institutions. Information, Communication & Society, 2(1), 125. https://doi.org/10.1080/136911899359736

[152] Alnsour, Y., & Jumah, A. (2021). Exploring the Effects of Information Security & Privacy on Blockchain Mobile Applications Rating : Text Analytics Approach. AMCIS 2021 Proceedings. https://aisel.aisnet.org/amcis2021/sig_acctinfosystem_asys/sig_acctinfosystem_asys/3

[153] Aloui, A., Msahli, M., Abdessalem, T., Bressan, S., & Mesnager, S. (2017). Protocol for preserving privacy in distributed system (PPDS). 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), 18851890. https://doi.org/10.1109/IWCMC.2017.7986571

[154] Andreou, A., Goga, O., & Loiseau, P. (2017). Identity vs. Attribute Disclosure Risks for Users with Multiple Social Profiles. Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017, 163170. https://doi.org/10.1145/3110025.3110046

[155] Ben Ayed, G., & Ghernaouti-Hélie, S. (2011). Privacy Requirements Specification for Digital Identity Management Systems Implementation Towards a digital society of privacy. 6th International Conference on Internet Technology and Secured Transactions. ICITST, Abu Dhabi, United Arab Emirates.

[156] Bouras, M. A., Lu, Q., Zhang, F., Wan, Y., Zhang, T., & Ning, H. (2020). Distributed Ledger Technology for eHealth Identity Privacy : State of The Art and Future Perspective. Sensors, 20(2), 483. https://doi.org/10.3390/s20020483

[157] Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. 2012 International Conference on Computer Science and Electronics Engineering, 1, 647651. https://doi.org/10.1109/ICCSEE.2012.193

[158] Clauß, S., & Kesdogan, D. (s. d.). Privacy Enhancing Identity Management : Protection Against Re-identification and Profiling. 10.

[159] Clauß, S., Kesdogan, D., & Kölsch, T. (2005). Privacy enhancing identity management : Protection against re-identification and profiling. Proceedings of the 2005 workshop on Digital identity management, 8493. https://doi.org/10.1145/1102486.1102501

[160] de Andrade, N. N. G. (2011). Data Protection, Privacy and Identity : Distinguishing Concepts and Articulating Rights. In S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, & G. Zhang (Éds.), Privacy and Identity Management for Life (Vol. 352, p. 90107). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-20769-3_8

[161] Dienlin, T., Masur, P. K., & Trepte, S. (2021). A longitudinal analysis of the privacy paradox. New Media & Society, 14614448211016316. https://doi.org/10.1177/14614448211016316

[162] Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates : An empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems, 22(3), 295316. ABI/INFORM Collection. https://doi.org/10.1057/ejis.2012.23

[163] Fragoso Rodriguez, U. (2009). Modèle de respect de la vie privée dans une architecture d'identité fédérée [These de doctorat, Evry, Institut national des télécommunications]. https://www.theses.fr/2009TELE0026

[164] Hahn, H. (2021). Digital identification systems and the right to privacy in the asylum context. https://pub-data.leuphana.de/frontdoor/index/index/year/2021/docId/1124

[165] Hansen, M., Berlich, P., Camenisch, J., Clauß, S., Pfitzmann, A., & Waidner, M. (2004). Privacy-Enhancing Identity Management. Information Security Technical Report, 9, 3544. https://doi.org/10.1016/S1363-4127(04)00014-7

[166] Hörbe, R., & Hötzendorfer, W. (2015). Privacy by Design in Federated Identity Management. 2015 IEEE Security and Privacy Workshops, 167174. https://doi.org/10.1109/SPW.2015.24

[167] Jackson, P. M., Ligertwood, J., O'Donnell, J., & Shelly, M. (s. d.). Small Business : Issues of Identity Management, Privacy and Security. 15.

[168] Kaur, J., & Dhillon, S. (2021). Privacy calculus and intension to share confidential information. AMCIS 2021 Proceedings. https://aisel.aisnet.org/amcis2021/info_security/info_security/11

[169] Kaur, P. C., Ghorpade, T., & Mane, V. (2016). Analysis of data security by using anonymization techniques. 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), 287293. https://doi.org/10.1109/CONFLUENCE.2016.7508130

[170] Nergiz, M. E., Clifton, C., & Nergiz, A. E. (2009). Multirelational k-Anonymity. IEEE Transactions on Knowledge and Data Engineering, 21(8), 11041117. https://doi.org/10.1109/TKDE.2008.210

[171] Prasser, F., Eicher, J., Spengler, H., Bild, R., & Kuhn, K. A. (2020). Flexible data anonymization using ARX—Current status and challenges ahead. Software: Practice and Experience, 50(7), 12771304. https://doi.org/10.1002/spe.2812

[172] Priesnitz Filho, W., Ribeiro, C., & Zefferer, T. (2019). Privacy-preserving attribute aggregation in eID federations. Future Generation Computer Systems, 92, 116. https://doi.org/10.1016/j.future.2018.09.025

[173] Privacy by Design : Current Practices in Estonia, India, and Austria. (s. d.). [Text/HTML]. World Bank. Consulté 3 juin 2021, à l'adresse https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/546691543847931842/Privacy-by-Design-Current-Practices-in-Estonia-India-and-Austria

[174] Rajendran, K., Jayabalan, M., & Rana, M. E. (2017). A Study on k-anonymity, l-diversity, and t-closeness Techniques focusing Medical Data. 17.

[175] Rocha, M. (2016). Data Privacy and Social Acceptance of Smart Meters. In Smart Grid Handbook (p. 19). American Cancer Society. https://doi.org/10.1002/9781118755471.sgd026[176] Rodriguez, U. F. (2009). Privacy model for federated identity architectures [Phdthesis, Institut National des Télécommunications ; Instituto tecnológico autónomo (México)]. https://tel.archives-ouvertes.fr/tel-00541850

[177] Schwartz, A. (2011). Privacy and Security : Identity Management and Privacy : A Rare Opportunity To Get It Right. Association for Computing Machinery. Communications of the ACM, 54(6), 22. ABI/INFORM Collection.

[178] Wood, S. (2020). Adhering to privacy by design with identity-as-a-service. Network Security, 2020(7), 1417. https://doi.org/10.1016/S1353-4858(20)30081-7