UNIVERSITÉ DE MONTRÉAL

L’IDENTITÉ NUMÉRIQUE : LA SOLUTION AU VOL D’IDENTITÉ ?

PAR

SARA YASSINE

MAÎTRISE EN CRIMINOLOGIE

FACULTÉ DES ARTS ET DES SCIENCES

TRAVAIL PRÉSENTÉ À DR. MASARAH PAQUET-CLOUSTON

DANS LE CADRE DU COURS CRI6228

CRIMINALITÉS ÉCONOMIQUES

AVRIL 2022

Table des matières

Résumé exécutif ……. 1

Introduction ……..……...…… 1

L'identité …… 2

L'identité ……..……...…… 2

Le vol d'identité ……..……...…… 3

L'identité numérique ……..……..…… 5

Études de cas ……..……..…… 6

L'Estonie ……..……...…… 7

L'Inde ……..……...…… 8

L'Australie ……...……... 11

L'identité numérique au Québec ……..……... 13

Conclusion ……..……...……..… 16

Bibliographie

L’identité numérique : La solution au vol d’identité ?

Résumé exécutif

Depuis quelques décennies, les taux de vol d’identité sont en hausse et ne font qu’augmenter. Étant donné l’ampleur de cette problématique, plusieurs pays et organisations ont commencé à développer des programmes d’identité numérique dans le but de contrer le vol d’identité. L’Estonie, étant pionnière du numérique, a adopté l’identité numérique en 2002. Le programme semble efficace et, malgré une cyberattaque survenue en 2007, les informations des citoyens semblent bien protégées et ces derniers rapportent être satisfaits. L’Inde a adopté son programme d’identité numérique en 2009 et il existerait des problèmes concernant la vérification par biométrie. Le présent rapport fait également état de la nouvelle initiative australienne, ainsi que l’initiative québécoise en cours de développement.

Introduction

Depuis les années 1990s, les pays occidentaux ont connu une importante diminution des taux de criminalité enregistrés. Bien que ceci semble rassurant, certains experts estiment que cette « baisse » serait plutôt un déplacement de la criminalité vers le monde numérique (Dupont, Amicelle, Boivin, Fortin et Tanner, 2019). L’essor d’Internet et l’avancement des diverses technologies informatiques ont grandement facilité et contribué au développement et à la propagation de la cybercriminalité (Holt, 2018). Le vol d’identité est un exemple de cybercrime qui connait une augmentation importante depuis quelques décennies. En effet, entre 2011 et 2018, le Canada aurait connu un accroissement de 58% dans le nombre de cas de vols d’identité (Normandin, 2019). Vu cette augmentation, certains pays et organisations se sont penchés sur le

problème afin d'y trouver une solution viable. Selon certains de ces pays et organisations, l'identité numérique serait la solution idéale pour contrer le vol d'identité.

Le présent rapport vise à présenter cette solution afin de permettre au lecteur de tirer ses propres conclusions quant à l'utilité de l'identité numérique dans la prévention du vol d'identité. Tout d'abord, quelques termes en lien avec l'identité seront définis. Ensuite, trois études de cas de pays ayant développé un programme d'identité numérique seront présentées. Finalement, l'identité numérique citoyenne, soit le programme d'identité numérique en cours de développement au Québec sera également présenté.

L'identité

L'identité

Qui es-tu ? Une simple question qui pourtant peut engendrer tant de réponses. En effet, l'identité d'une personne est un concept multidimensionnel qui englobe plusieurs sphères de sa vie. L'identité est généralement définie comme étant un ensemble d'attributs qui décrivent, de manière unique, un individu, dans un contexte donné (Access Now, 2018). De ce fait, les attributs identitaires varient dépendamment du contexte dans lequel l'identité de la personne est définie (Access Now, 2018 ; Naudin, 2015). Par exemple, l'identité légale est une des facettes de l'identité : c'est l'identité d'une personne dans un contexte légal. Les attributs de cette identité incluent, entre autres, le nom de la personne, sa date et son lieu de naissance et son numéro d'assurance social (NAS). C'est une identité accompagnée de documents légaux à l'appui tels qu'un passeport ou un certificat de naissance (Access Now, 2018).

L'identité n'est donc pas aussi simple à définir que ce que l'on pourrait croire. C'est un concept multidimensionnel, qui prend de l'expansion (Naudin, 2015). Avec cet élargissement des

facettes qui la constituent, l'identité prend de plus en plus de valeur. C'est pourquoi il existe maintenant une multitude de crimes en lien avec l'identité tels que le vol de données personnelles, la vente de ces données ainsi que l'utilisation de l'identité des victimes pour commettre des activités illégales (Ahmed, 2020, ch. 3).

Le vol d'identité

Les crimes contre l'identité (*identity crime*) sont généralement classer en deux catégories : (1) le « vol d'identité » (*identity theft*) et (2) l'« usurpation d'identité » (*identity fraud*). Même si ce sont en fait deux catégories des crimes contre l'identité, ces deux termes sont souvent utilisés de manière interchangeable (Ahmed, 2020, ch. 1). D'un côté, le vol d'identité consiste à avoir en sa possession les informations identitaires d'une personne, sans son consentement. On fait allusion, par exemple, à un employé dans le domaine bancaire qui profite de son poste pour voler des informations identitaires de clients de la banque. Ça peut également être un tiers qui achète ces informations de l'employé malhonnête. Dans les deux cas, les individus ont commis un vol d'identité vu qu'ils ont en leur possession des informations qui ne leur appartiennent pas (Ahmed, 2020, ch. 1). Concernant l'usurpation d'identité, ce crime consiste à se faire passer pour une autre personne, que cette personne soit en vie ou décédée (Ahmed, 2020, ch. 1). De ce fait, posséder les informations identitaires de Madame X sans son consentement consiste en un vol d'identité, alors que se faire passer pour Madame X en utilisant lesdites informations consiste en une usurpation d'identité. En général, dans plusieurs pays tels que les États-Unis, les termes « vol d'identité » et « usurpation d'identité » sont utilisés de manière interchangeable pour décrire le crime contre l'identité. Au Canada toutefois, les deux termes sont généralement utilisés pour faire référence aux deux phénomènes distincts (Ahmed, 2020, ch. 1). Dans le cadre du présent rapport, l'appellation

« vol d'identité » sera utilisé au sens large du terme et englobera donc l'usurpation d'identité, dans le but d'alléger le texte.

Tout comme la cybercriminalité générale, le vol d'identité est également en expansion. En effet, l'essor d'Internet et l'avancement des diverses technologies informatiques ont grandement facilité et contribué au développement et à la propagation de la cybercriminalité (Holt, 2018). En 2010, on estimait le nombre de cybervictimes aux États-Unis à 300 000 ainsi que des pertes financières d'environ 500 000 millions de dollars américains (Song, Lynch et Cochran, 2016). En ce qui a trait au vol d'identité spécifiquement, il est difficile d'obtenir des statistiques précises puisque cette criminalité est généralement recensée comme faisant partie de la fraude générale. Toutefois, vu que la fraude est en hausse, on estime que le vol d'identité l'est également. Selon le Centre antifraude du Canada, il y aurait eu 106 770 cas de fraude à travers le pays en 2021. Ces crimes auraient engendré des pertes financières de 125 M$ (Centre antifraude du Canada, 2022).

Il est toutefois estimé que ces statistiques ne sont pas représentatives de la réalité. En effet, il subsiste un important problème de sous-déclaration de la cybercriminalité, et par le fait même, du vol d'identité. Il existerait donc un chiffre noir significatif concernant la cybercriminalité qui se traduit en un manque de connaissances quant à ce type de crime et en une sous-estimation de son ampleur réelle. Ce problème de sous-déclaration est d'autant plus important vu la constante et rapide évolution de la technologie et, par le fait même, de la cybercriminalité (Dupont et al., 2019).

Le vol d'identité est donc un problème grandissant. De ce fait, plusieurs pays et organisations se sont penchés sur la problématique afin de trouver une solution. Une solution qui semble satisfaire une grande partie des pays et organisations est l'identité numérique.

L’identité numérique

L’identité numérique est une des facettes de l’identité, généralement considérée comme étant une solution prometteuse au vol d’identité. L’identité numérique implique deux processus : (1) l’authentification de l’identité et (2) la vérification de l’identité (Sullivan, 2018).

L’authentification de l’identité est le processus initial requis au moment de l’inscription de l’identité numérique, au sein du gouvernement. C’est à ce moment que l’identité numérique du citoyen est créée. À cette étape, certaines informations — nommées identifiants — sont enregistrées telles que, entre autres, la biométrie, une signature, une photo ou un mot de passe (Sullivan, 2018). Après avoir été créée, l’identité numérique doit être vérifiée à chaque fois que le citoyen veut en faire usage. De ce fait, l’authentification de l’identité consiste en une procédure ponctuelle, alors que la vérification de l’identité est un processus plus fréquent. Lorsque le citoyen souhaite faire des procédures qui requièrent l’utilisation de l’identité numérique, les informations qu’il fournit sont alors comparées aux identifiants enregistrés lors de l’authentification (Sullivan, 2018). Le but de cette comparaison est de répondre à la question suivante : est-ce que cette personne est réellement qui elle prétend être ?

Au cours des deux dernières décennies principalement, de nombreux programmes internationaux d’identité numérique ont vu le jour, alors que d’autres sont toujours en cours de conception ou de développement. Tel est le cas, entre autres, en Estonie, aux Philippines, en Italie, en France, au Japon, en Turquie, en Inde, en Tunisie, en Australie, et dans bien plus de pays encore (Thales Group, s.d.). Il existe principalement deux types de programmes d’identité numérique : (1) ceux qui se basent sur des cartes physiques et (2) ceux qui se basent sur des applications mobiles (Thales Group, s.d.).

Les avantages de l'identité numérique

Selon la littérature, les programmes d'identité numérique à travers le monde sont en mesure de répondre à un besoin de transparence et de protection de la vie privée des utilisateurs (Toth, K. C. et Anderson-Priddy, A., 2019). De ce fait, les nouveaux programmes d'identité numérique sont conçus sous la forme de portefeuilles numériques (Roy, 2022 ; Thales, s.d.). Cette technologie permettrait aux utilisateurs d'avoir le contrôle sur leurs informations et ainsi assurer la protection de leurs identifiants (Thales, s.d.). De ce fait, les risques de vol d'identité seraient minimisés (Sullivan, 2018).

Les désavantages de l'identité numérique

Bien que l'identité numérique se veut une solution avantageuse pour contrer le vol d'identité, la littérature recense quelques problématiques potentielles avec sa mise en œuvre (Sullivan, 2018). En effet, l'identité numérique ne semble pas être un programme infaillible puisque la précision de la vérification de l'identité dépendrait de trois facteurs principaux. Tout d'abord, cette précision dépend du type d'identifiant enregistré au moment de l'authentification, certains identifiants étant moins fiables que d'autres, telle que la biométrie (Anand, 2021 ; Sullivan, 2018). En fait, Sullivan (2018) va encore plus loin et affirme que tous les types d'identifiants peuvent engendrer de faux positifs ou de faux négatifs. La précision de la vérification de l'identité dépend également de la façon dont l'information est enregistrée, stockée et transmise. De plus, le processus même de vérification peut affecter sa précision (Sullivan, 2018).

Études de cas

Parmi les pays ayant développé — ou qui développent — des programmes d'identité numérique, trois seront présentés dans cette section : l'Estonie, l'Inde et l'Australie. Ces pays ont

été sélectionnés en fonction de leur diversification puisque les trois programmes adoptés sont différents l'un de l'autre et présentent donc chacun des pratiques et des points de vue différents.

L'Estonie

Une description de l'identité numérique estonienne

Depuis son indépendance en 1991, l'Estonie est considérée comme étant une pionnière du numérique (Watts, 2019). En 1996, les banques du pays commençaient déjà à utiliser des cartes à authentification basée sur les numéros d'identification personnels (NIP). Puis, le pays a commencé à développer un programme d'identité numérique basé sur des cartes physiques. Les premières cartes ont été émises en mars 2002 (Parsovs, 2021). Aujourd'hui, tous les citoyens estoniens détiennent une identité numérique (Access Now, 2018) dès leur naissance (Watts, 2019). L'identité numérique estonienne (eID) consiste en une carte à puce (avec une photo du détenteur) ainsi qu'une signature électronique (CNBC International, 2019 ; Parsovs, 2021). De ce fait, la signature est un identifiant utilisé dans le processus de vérification. Grâce à l'identité numérique, les Estoniens peuvent faire une multitude de procédures qui demandaient autrefois une présence physique. Les Estoniens peuvent maintenant accéder à leur compte bancaire et y apporter des changements, renouveler leur passeport, vendre leur voiture (CNBC International, 2019), faire leurs déclarations d'impôts, voter lors des élections, accéder à leur historique médical et même avoir accès au portail du site web scolaire de leur enfant, le tout par le biais l'identité numérique (Watts, 2019). Le gouvernement se vante même que les seules procédures qui ne peuvent être faites à travers eID sont l'achat d'une maison, le mariage ou le divorce (Watts, 2019).

Les arguments en faveur de l'identité numérique estonienne

Les partisans de l'identité numérique estonienne avancent que cette technologie est avantageuse en raison de sa transparence et de sa protection de la vie privée de ses utilisateurs. De

plus, cette technologie pourrait sauver des vies selon certains. En effet, si une personne doit être transportée d'urgence à l'hôpital, les ambulanciers ne devraient avoir aucun problème à récupérer l'historique complet du patient, puisque l'information est centralisée (Watts, 2019). Parallèlement, l'adoption de l'identité numérique aurait engendré des gains financiers au pays, soit des économies de 2% du produit intérieur brut (PIB) par année (CNBC International, 2019). En général, les personnes en faveur de eID estiment que cette technologie facilite leur vie puisque la plupart des transactions et des procédures qu'ils souhaitent mener quotidiennement peuvent être faites en quelques clics seulement, dans le confort de leur chez-soi (Ronzaud, 2020).

Les arguments en défaveur de l'identité numérique estonienne

Bien qu'approuvée par un grand nombre de personnes, l'identité numérique adoptée en Estonie est certainement critiquée par plusieurs. Certains avancent que l'eID serait un outil de surveillance de masse, puisque toutes les informations des citoyens sont centralisées par le gouvernement (Watts, 2019). De plus, certains dénoncent des failles dans le système qui le rendrait plus vulnérable à une cyberattaque. C'est en effet un point important à considérer, surtout après l'avènement d'une cyberattaque en 2007. Bien qu'aucune perte financière ne fût déclarée, des informations ont certainement été compromises (Ronzaud, 2020 ; Watts, 2019). Depuis, l'Estonie a mis en place une sauvegarde des données gouvernementales au Luxembourg, afin de protéger ses données en cas d'une nouvelle cyberattaque (Watts, 2019).

L'Inde

Description de l'identité numérique indienne

L'Inde a implémenté une technologie basée sur l'identité numérique en 2009 (Anand, 2021), connue sous le nom de *Aadhaar* (Access Now, 2018). Le programme *Aadhaar*, tout comme le programme adopté en Estonie, est basé sur des cartes d'identité physiques (Anand, 2021 ; World

Bank, 2016). Le processus de vérification peut généralement se faire de trois manières différentes. Tout d'abord, des informations démographiques peuvent être utilisées pour vérifier l'identité de la personne en comparant lesdites informations au numéro *Aadhaar*. Une deuxième méthode impliquerait la biométrie, soit les empreintes digitales ou la reconnaissance de l'iris. Finalement, la vérification de l'identité peut se faire à travers la technologie d'authentification multifactorielle ou le mécanisme d'authentification à l'aide d'un mot de passe à usage unique (*One-Time Password* – OTP) (Anand, 2021). Il est à noter toutefois que la méthode de vérification de l'identité la plus communément utilisée avec *Aadhaar* est celle de la biométrie (Anand, 2021).

Les arguments en faveur de l'identité numérique indienne

Les personnes en faveur du programme d'identité numérique en Inde évoquent la distribution des rations alimentaires dans le pays, facilitée par l'avènement d'*Aadhaar*. De ce fait, si une personne ne peut recevoir qu'un seul kilo de riz par mois par exemple, il lui serait impossible de se procurer des kilos de riz additionnels en se présentant à plusieurs centres de distribution. En effet, lorsque la personne prend sa ration alimentaire, elle doit s'identifier à l'aide de son identité numérique, soit de sa carte identitaire ainsi que d'identifiants biométriques. Le système enregistre donc que telle personne a déjà reçu sa portion. Il lui sera donc impossible de prendre une deuxième portion dans le même centre distribution ou même dans un autre centre (World Bank, 2016).

Les arguments en défaveur de l'identité numérique indienne

Malgré le support que reçoit *Aadhaar*, nombreux sont ceux qui se montrent en défaveur du programme. Tout d'abord, l'une des raisons pour lesquelles *Aadhaar* aurait été initialement développée est de fournir une identité légale aux personnes qui n'en ont pas, principalement des personnes marginalisées ou issues de milieux défavorisés. Toutefois, il semblerait que la situation ne se soit pas réglée avec l'adoption du programme *Aadhaar*. Cette identité numérique a

principalement été attribuée à des personnes ayant déjà une ou plusieurs pièces d'identité, laissant les personnes qui n'ont pas de pièce d'identité gouvernementale dans le même problème (World Bank, 2016).

De plus, *Aadhaar* reçoit beaucoup de critiques quant à son utilisation de la biométrie comme moyen d'authentification et de vérification. En effet, la biométrie n'est pas une méthode complètement fiable. Les empreintes digitales d'une personne peuvent être affectées par le travail manuel constant, mais également par l'âge ou même par des blessures aux doigts (Anand, 2021). Quant à la reconnaissance de l'iris, sa précision peut être entravée par des cataractes. De ce fait, une personne pourrait présenter les bonnes informations, mais quand même échouer le processus de vérification de l'identité (Anand, 2021). Anand (2021) rapporte également que l'authentification à l'aide d'un mot de passe à usage unique ne pourrait être une solution viable au problème d'identification à l'aide de la biométrie puisque 32% de la population indienne adulte n'a pas accès à la téléphonie mobile par manque de moyens financiers.

D'un autre côté, le programme d'identité numérique indien est critiqué pour sa centralisation des banques de données, le rendant ainsi vulnérable aux cyberattaques. En fait, plusieurs brèches de données ont eu lieu depuis la naissance de *Aadhaar*. Le plus gros problème cependant, avec ces brèches de données, concerne l'unicité de la biométrie. En effet, si les informations biométriques d'une personne sont compromises, il lui serait impossible de les modifier. Une fuite de données biométriques est donc irréversible (Acces Now, 2018). En outre, les personnes en défaveur de *Aadhaar* dénoncent des enjeux en lien avec la vie privée des citoyens. Avec le temps, le gouvernement indien a commencé à exiger l'utilisation de l'identité numérique pour accéder à de plus en plus de services gouvernementaux. Les citoyens ne voulant pas se créer une identité numérique se sont donc trouvés obligés d'adopter cette technologie, faute de ne pas

avoir accès à certains services gouvernementaux (Access Now, 2018). Certains ont même mené ce combat à la cour, et en s'ont sorti vainqueurs. Toutefois, même si le gouvernement propose des alternatives à *Aadhaar* en termes de vérification de l'identité des citoyens, la plupart des programmes gouvernementaux, de par leur conception, utilisent le programme *Aadhaar* comme méthode d'identification par défaut (Anand, 2021).

L'Australie

Il est à noter que le programme de l'identité numérique australien est jeune comparativement aux initiatives estonienne et indienne. De ce fait, la présente section ne sera pas séparée en fonction des avantages et des inconvénients du programme vu que la littérature scientifique est encore pauvre à ce sujet. Toutefois, une description générale dudit programme ainsi que de ses promesses et de ses citriques sera présentée.

Dans le but d'améliorer son agenda numérique, l'Australie a créé une agence du numérique en 2016 : la *Digital Transformation Agency* (DTA) (Hanson, Ott et Krenjova, 2018). Un des buts de cette agence est d'améliorer l'expérience client des citoyens lors de leur utilisation des différents services en ligne fournis par le gouvernement australien. La DTA vise également à augmenter la transparence du gouvernement quant à ses divers projets numériques, l'un d'entre eux étant le *Trusted Digital Identity Framework* (TDIF), soit le programme d'identité numérique australien (Hanson et al., 2018). Il est important de s'attarder sur le mot *Framework,* ou cadre en français. Une des caractéristiques du programme d'identité numérique en Australien est l'utilisation de ce TDIF ou de ce cadre général. Le principe de ce cadre est que les citoyens peuvent choisir d'utiliser un fournisseur de services accrédité dans le but d'accéder aux services gouvernementaux en ligne. De ce fait, il y aurait plusieurs fournisseurs de services permettant de s'identifier à l'aide de son identité numérique (Digital Transformation Agency, 2022).

Le programme australien de l'identité numérique se veut accessible, simple d'utilisation et centré sur l'utilisateur, le but étant de rendre l'expérience client la plus agréable possible. De plus, l'agence du numérique australienne rapporte que le TDIF est volontaire et transparent (Digital Transformation Agency, 2022). De ce fait, il n'est pas obligatoire pour les citoyens de prendre part de ce programme. La sécurité et le respect de la vie privée des utilisateurs sont également un point important que souligne la DTA. Les utilisateurs peuvent ainsi savoir comment leurs informations sont utilisées et ils peuvent révoquer leur consentement à tout moment (Digital Transformation Agency, 2022). L'agence promet également que le TDIF mettra l'accent sur la collaboration entre le secteur public et le secteur privé. Finalement, le TDIF permet de contrôler les risques de fraude et de cyberattaque en vue de protéger les utilisateurs et leurs informations personnelles (Digital Transformation Agency, 2022).

Concernant les critiques du programme australien, Benjamin Frengley, un candidat à la maîtrise en informatique de l'Université de Melbourne ainsi que sa superviseure Vanessa Teague se sont fait entendre (Barbaschow, 2021 ; Frengley, 2020). Dans sa thèse de maîtrise, Frengley (2020) a souligné plusieurs points qu'il considère comme étant défaillants et qui rendraient le TDIF insécure. Basé sur cette thèse, Frengley, en collaboration avec Teague, a écrit un rapport résumant les points jugés défaillants, à l'attention de la DTA et du *Australian Tax Office* (ATO), soit le Bureau fiscal australien (Frengley et Teague, 2020). Frengley et Teague (2020) rapportent plusieurs failles qu'ils estiment exister dans le système TDIF. Ces failles seraient principalement en lien avec la technologie sur laquelle se base TDIF. L'une de ces failles impliquerait *myGovID*, un service d'identité numérique offert par l'ATO. Selon les auteurs, *myGovID* serait à risque d'attaque par le biais de code proxy. Les auteurs avancent que cette faiblesse dans le système aurait déjà été rapportée à l'ATO, mais que le bureau aurait décidé de ne rien y faire (Frengley et Teague,

2020). Dans le but de remédier aux problèmes soulevés, Frengley et Teague (2020) recommandent l'utilisation d'un système basé sur une infrastructure à clé publique (ICP) ainsi que l'utilisation d'un protocole OpenID Connect.

En bref, les prochains mois, voire les prochaines années, mettront en lumière les avantages et les inconvénients réels du programme d'identité numérique en Australie, un État dont les citoyens se rappellent encore les années 1980s et qui redoutent l'arrivée d'une nouvelle version du plan « Austalia card » (Bonyhady, 2022).

L'identité numérique au Québec

Comme plusieurs pays et provinces à travers le globe, le Québec est également intéressé à adopter l'identité numérique au sein de son territoire. La province travaille donc sur son propre programme d'identité numérique : l'identité numérique citoyenne. Pour se faire, le nouveau ministère de la Cybersécurité et du numérique mené par le ministre Éric Caire a vu le jour le 1er janvier 2022 et travaille présentement sur le développement de l'identité numérique citoyenne (Secrétariat du Conseil du trésor, 2021) ainsi que d'un portefeuille numérique (Roy, 2022). Le but premier de ce projet est d'offrir aux citoyens « … un accès simplifié aux services de l'État, en toute sécurité. » (Secrétariat du Conseil du trésor, 2021).

Il est important de noter que, puisque le programme d'identité numérique est encore en cours de développement, il existe très peu de littérature le décrivant. De ce fait, les informations transmises dans le présent rapport proviennent d'une rencontre avec trois représentants du ministère de la Cybersécurité et du numérique. Il se peut donc que des changements aient déjà été apportés ou que des changements soient éventuellement apportés au projet avant que l'identité ou le portefeuille numériques ne voient le jour. Il est également important d'ajouter qu'une partie des

informations présentées dans le présent rapport provient d'un article du journal « Le Quotidien », basé sur une entrevue avec le ministre Éric Caire (Roy, 2022).

Le programme d'identité numérique en cours de développement au Québec se basera sur une application mobile plutôt que sur des cartes physiques tel qu'en Estonie ou en Inde. Ce programme impliquera trois parties : l'émetteur, le détenteur et le consommateur. Tout d'abord, l'émetteur — c'est-à-dire le gouvernement — émet des identifiants au citoyen, soit le détenteur. Ces identifiants — ou attestations — peuvent être, entre autres, un numéro d'assurance sociale, un numéro d'assurance maladie, un passeport, un permis de conduire ou un certificat de naissance. Lorsqu'une attestation est émise, l'émetteur ne peut plus la modifier puisqu'elle appartient au détenteur. Finalement, le consommateur représente la personne ou l'organisation qui demande d'avoir accès à l'identifiant pour une raison donnée. Par exemple, le consommateur peut être un médecin qui demande d'avoir accès à l'historique médical d'un détenteur.

Un grand souci du gouvernement est de protéger la confidentialité et la vie privée des citoyens. De ce fait, l'information ne serait pas centralisée puisque le programme sera basé sur la technologie *blockchain*. De plus, le détenteur n'accèdera qu'à l'attestation qu'il a besoin de vérifier, rien de plus. Par exemple, en ce moment en 2022, si une personne doit démonter qu'elle ait bien l'âge légal pour acheter des produits de la Société des alcools du Québec (SAQ), elle doit présenter, généralement, son permis de conduire ou sa carte d'assurance maladie. Toutefois, ces pièces d'identité contiennent beaucoup plus d'informations que requis par le consommateur, soit la SAQ. Des informations sensibles seront donc partagées au consommateur à l'instar du nom du détenteur, sa date de naissance et son adresse. Avec l'identité numérique citoyenne, le consommateur n'aura accès qu'à l'attestation dont il a besoin ; dans ce cas-ci, l'âge du détenteur. En effet, le détenteur présentera un code QR que le consommateur scannera à l'aide d'un appareil

mobile intelligent. Sur son écran, deux éléments apparaitront : (1) la photo du détenteur afin de vérifier que c'est la bonne personne et (2) une coche si le détenteur est d'âge légal ou un « X » si le détenteur est un mineur. De ce fait, le consommateur n'aura pas accès aux autres identifiants qu'on retrouve normalement sur un permis de conduire ou sur une carte d'assurance maladie.

Cette technologie permettra donc au détenteur d'avoir le contrôle de ses informations. En fait, lors de l'entretien avec les représentants du ministère de la Cybersécurité et du Numérique, la phrase « on redonne le pouvoir au citoyen » a été répétée à maintes reprises. Le détenteur sera donc en contrôle des personnes qui auraient accès à ses différentes attestations. De plus, le détenteur aura le contrôle sur quelle attestation sera partagée et laquelle ne le sera pas. Par exemple, si une personne se présente chez un professionnel de la santé, le médecin lui demandera certainement des informations telles que son nom, son âge, son numéro d'assurance maladie et son historique médical. De ce fait, le patient recevra une demande d'accès à ces attestations et aura l'option d'approuver ou de refuser cette demande. Admettons que le médecin demande accès à l'historique médical du patient ainsi qu'à son numéro de permis de conduire, le patient pourra accepter l'accès à son historique médical, mais refuser l'accès à son numéro de permis de conduire puisque le contexte ne nécessite pas cette information.

En somme, l'identité numérique citoyenne se veut innovante et axée sur le citoyen. D'ici l'année 2025, les Québécois auront non seulement accès à une identité numérique, mais également à un portefeuille numérique (Roy, 2022). Le portefeuille numérique inclura tout ce que contient un portefeuille physique et plus encore. Ceci inclus donc les pièces d'identité standards, mais également, les diplômes du détenteur, son passeport, son certificat de naissance, son certificat de mariage, et plus.

Conclusion

À la lumière de ce qui précède, la cybercriminalité incluant le vol d'identité et en hausse à travers le globe. Une des solutions proposées pour contrer ce problème est l'identité numérique. Les prochaines années s'avèreront cruciales pour déterminer l'effet de l'identité numérique sur le vol d'identité et les taux de cette délinquance. Il serait intéressant de mener une étude ou même un recensement auprès de la population québécoise avant l'avènement de l'identité numérique afin d'enregistrer les taux de vols d'identité dans la province. Ensuite, la même étude pourrait être refaite lorsqu'un nombre suffisant de Québécois auront adopté l'identité numérique. De ce fait, les taux avant et après pourront être comparés afin de déterminer si le vol d'identité est réellement diminué avec l'identité numérique.

Même s'il nous faut encore plusieurs années avant d'observer les résultats réels de l'identité numérique citoyenne, ce projet semble prometteur selon la recherche menée pour le présent rapport. En effet, l'initiative québécoise semble éviter les problèmes rapportés en Inde ou en Estonie puisque l'information ne sera pas centralisée et le programme sera basé sur une application mobile plutôt que des cartes physiques.

BIBLIOGRAPHIE

Access Now. (2018). *National digital identity programmes: What's next?* Accesnow.org. https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf

Ahmed, S. R. (2020). *Preventing Identity Crime: Identity Theft and Identity Fraud*. Brill Nijhoff. https://doi.org/10.1163/9789004395978_004

Anand, N. (2021). New principles for governing Aadhaar: Improving access and inclusion, privacy, security, and identity management. *Journal of Science Policy & Governance, 18*(1), 1-14. https://doi.org/10.38126/JSPG180101

Barbaschow, A. (2021, 15 février). Researchers want Australia's digital ID system thrown out and redesigned from scratch. *ZDNet*. https://www.zdnet.com/article/researchers-want-australias-digital-id-system-thrown-out-and-redesigned-from-scratch/

Bonyhady, N. (2022, 10 février). National digital ID plan sparks 'Australia Card' warnings. The Sydney Morning Herald. https://www.smh.com.au/technology/national-digital-id-plan-sparks-australia-card-warnings-20220209-p59v1t.html

Centre antifraude du Canada (2022). *Répercussions de la fraude depuis le début de l'année*. Centre antifraude du Canada. https://www.antifraudcentre-centreantifraude.ca/index-fra.htm

CNBC International (2019, 6 février). *How Estonia became one of the world's most advanced digital societies – CNBC Reports* [vidéo]. YouTube. https://www.youtube.com/watch?v=NAxOUBMMQd4

Digital Transformation Agency. (2022, mars). *Trusted Digital Identity Framework release* (4.2). Australian Government. https://www.digitalidentity.gov.au/sites/default/files/2022-

03/TDIF%2002%20Overview%20-%20Release%204.6%20%28Doc%20Version%201.3%29.pdf

Dupont, B., Amicelle, A., Boivin, R., Fortin, F. et Tanner, S. (2019, novembre). *Rapport de recherche sur l'avenir du travail policier*. Fraternité des policiers et policières de Montréal. https://www.fppm.qc.ca/medias/lettres/rapport-final-fppm.pdf

Frengley, B. (2020). *How trustworthy is the Trusted Digital Identity Framework? Evaluating security and privacy in Australian digital identity* [Thèse de maîtrise, University of Melbourne]. https://bfrengley.github.io/thesis.pdf

Frengley, B. et Teague, V. (2020). *Submission to the Consultation on Digital ID*. https://www.digitalidentity.gov.au/sites/default/files/2021-01/consultation01-vanessa-teague.pdf

Hanson, F., Ott, A. et Krenjova. J. (2018). *Introducing integrated e-government in Australia*. Australian Strategic Policy Institute. https://www.aspi.org.au/report/introducing-integrated-e-government-australia

Holt, T. J. (2018). Regulating cybercrime through law enforcement and industry mechanisms. *The ANNALS of the American Academy of Political and Social Science, 679*(1), 140-157. https://doi.org/10.1177/0002716218783679

Naudin, C. (2015). La criminalité identitaire. Dans *Identités criminelles : la vérité interdite*. Presses universitaires de France. https://doi.org/10.3917/puf.naudi.2015.03

Normandin, P. A. (2019, 23 juillet). Rapport sur la criminalité : hausse marquée des fraudes au Canada. *La Presse*. https://www.lapresse.ca/actualites/justice-et-faits-divers/2019-07-23/rapport-sur-la-criminalite-hausse-marquee-des-fraudes-au-canada

Parsovs, A. (2021). *Estonian electronic identity card and its security challenges* [Thèse de doctorat, University of Tartu]. DSpace. https://dspace.ut.ee/handle/10062/71481

Ronzaud, L. (2020). « E-Estonie » : le « nation-branding » numérique comme stratégie de rayonnement international. *Herodote*, *177178*(2), 267— 280. https://www.cairn.info/revue-herodote-2020-2-page-267.htm

Roy, G. (2022, 13 février). À quoi ressemblera l'identité numérique des Québécois ? *Le Quotidien*. https://www.lequotidien.com/2022/02/13/a-quoi-ressemblera-lidentite-numerique-des-quebecois-7aac7f3e6e8ccbaa7a778eaea513c006

Secrétariat du Conseil du trésor (2021, 2 décembre). Le ministère de la Cybersécurité et du Numérique verra le jour le 1er janvier 2022. Gouvernement du Québec, Secrétariat du Conseil du trésor. https://www.tresor.gouv.qc.ca/nouvelles/news/le-ministere-de-la-cybersecurite-et-du-numerique-verra-le-jour-le-1er-janvier-2022/?tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=43f8462fe2f8b243b07a1ea19b409d98

Song, H., Lynch, M. J. et Cochran, J. K. (2016). A macro-social exploratory analysis of the rate of interstate cyber-victimization. *American Journal of Criminal Justice*, *41*(3), 583-601. https://doi.org/10.1007/s12103-015-9308-4

Sullivan, C. (2018). Digital identity – From emergent legal concept to new reality. *Computer Law & Security Review*, *34*(4), 723-731. https://doi.org/10.1016/j.clsr.2018.05.015

Thales Group. (s.d.). *Identité numérique sécurisée — Les 5 forces qui façonnent notre présent.* https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/identite/identite-numerique

Toth, K. C. et Anderson-Priddy, A. (2019). Self-Sovereign digital identity: A paradigm shift for identity. *IEEE Security Privacy*, *17*(3), 17-27. https://doi.org/10.1109/MSEC.2018.2888782

Watts, J. M. (2019, 9 mai). One country's uber-convenient, incredibly invasive digital ID system. *Wall Street Journal*. https://www.wsj.com/articles/the-digitization-of-your-identity-11557403060

World Bank (2016, 13 janvier). *Transforming Government: Digital Identity in India* [video]. YouTube. https://www.youtube.com/watch?v=ty1Gpjho4dQ