CFP-005M
C.P. PL 82
Loi concernant
identité numérique nationale

Pour une identité numérique québécoise au service des citoyens : enjeux et recommandations

Hugo Loiseau
Daniel J. Caron
Sébastien Gambs
Sébastien Brousseau

Mémoire présenté à la Commission des finances publiques lors des consultations particulières et auditions publiques sur le projet de loi 82, Loi concernant l'identité numérique nationale et modifiant d'autres dispositions.

obvia

Janvier 2025

Présentation des auteurs du mémoire

Hugo Loiseau

Professeur titulaire à l'École de politique appliquée de l'Université de Sherbrooke. Il est membre chercheur associé à l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (Obvia) et membre du Pôle d'expertise en cybersécurité et impacts sociétaux de l'Obvia. Il se spécialise dans les enjeux politiques du cyberespace, notamment l'identité numérique.

Daniel J. Caron

Professeur à l'ÉNAP, où il est titulaire de la Chaire de recherche en exploitation des ressources informationnelles. Il est chercheur et Fellow du CIRANO et membre chercheur associé à l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (Obvia). Il est aussi professeur associé à la SPPA à l'Université Carleton.

Sébastien Gambs

Professeur au département d'informatique de l'Université du Québec à Montréal et titulaire de la Chaire de recherche du Canada en analyse respectueuse de la vie privée et éthique des données massives. Sa thématique de recherche principale porte sur la protection de la vie privée dans le monde numérique ainsi que les problématiques éthiques telles que l'équité et la transparence des systèmes algorithmiques. Il est membre chercheur associé à l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (Obvia) et membre du Pôle d'expertise en cybersécurité et impacts sociétaux de l'Obvia.

Sébastien Brousseau

Professionnel de recherche à l'Université Laval et coordonnateur du Pôle d'expertise en cybersécurité et impacts sociétaux de l'Obvia. Il mène des recherches interdisciplinaires sur les interactions entre l'humain et la technologie. Il se spécialise en matière d'intelligence artificielle et de technologies émergentes, en explorant leur dimension sociotechnique.

Remerciements

Les auteurs tiennent à remercier Pierre-Martin Tardif, Steve Jacob et Esther Poisson pour leur relecture attentive et leurs précieux commentaires qui ont permis d'améliorer la qualité de ce mémoire. Leurs suggestions pertinentes ont grandement contribué à la version finale de ce travail.

Résumé

Ce mémoire analyse le projet de loi 82 sur l'identité numérique nationale dans le contexte de la transformation numérique de l'État québécois. S'appuyant sur des recherches approfondies sur les enjeux techniques et éthiques, ainsi que sur une enquête récente auprès de 2 000 citoyens québécois, il examine les conditions nécessaires à la réussite de ce projet structurant.

L'analyse révèle que l'acceptabilité sociale constitue un enjeu fondamental, avec 86,9 % des citoyens favorables à l'identité numérique sous certaines conditions, particulièrement en matière de sécurité et de protection des renseignements personnels. Le mémoire souligne l'importance d'une gouvernance centralisée, incarnée par le ministère de la Cybersécurité et du Numérique, tout en relevant certaines zones d'ombre concernant l'hébergement des données, les enjeux de vie privée et le rôle du secteur privé.

Six recommandations principales sont formulées, portant sur l'acceptabilité sociale, la cybersécurité, la protection de la vie privée, l'implication des parties prenantes, la présence d'une autorité centrale et l'utilité du système pour les citoyens. Ces recommandations s'appuient sur une analyse des expériences internationales et visent à assurer le succès durable de l'identité numérique nationale québécoise.

Le mémoire conclut que le projet de loi 82 constitue une avancée significative, mais nécessite des précisions et des garanties supplémentaires pour répondre pleinement aux attentes et aux préoccupations des citoyens en matière de sécurité, de protection des données et d'accessibilité des services.

Recommandations

Recommandation 1 : Miser sur le dialogue et la transparence pour construire l'acceptabilité sociale de l'identité numérique nationale

Recommandation 2 : Renforcer les capacités de cybersécurité pour protéger l'intégrité de l'identité numérique nationale

Recommandation 3 : Assurer une protection robuste des renseignements personnels par une architecture décentralisée et des mécanismes de contrôle citoyens

Recommandation 4 : Adopter une approche inclusive et collaborative impliquant l'ensemble des parties prenantes dans le développement et le déploiement de l'identité numérique nationale

Recommandation 5 : Confirmer le rôle central du ministère de la Cybersécurité et du Numérique dans la gouvernance de l'identité numérique nationale

Recommandation 6 : Maximiser la valeur et l'utilité quotidienne de l'identité numérique nationale pour les citoyens

Présentation de l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (Obvia)

Fondé en 2019, l'Obvia est un réseau de recherche qui fédère les expertises interdisciplinaires de plus de 240 chercheuses et chercheurs en sciences humaines et sociales, en sciences et génie, et en santé. Il soutient les acteurs de la recherche québécoise sur les impacts sociétaux de l'IA et du numérique, pour favoriser l'émergence d'un encadrement et d'une gouvernance responsable de l'IA. L'Obvia est un point de rencontre, un lieu d'échange et de collaboration, pour celles et ceux qui souhaitent maximiser les promesses de l'IA tout en étant mieux sensibilisé à ses impacts sociétaux.

Pôle d'expertise en cybersécurité et impacts sociétaux

Présentation du Pôle d'expertise en cybersécurité et impacts sociétaux de l'Obvia

À travers ses activités et projets de recherche, le Pôle d'expertise en cybersécurité et impacts sociétaux de l'Obvia vise l'émergence d'une réflexion transdisciplinaire sur les cyberrisques et la cybersécurité, ainsi que le développement de nouvelles connaissances empiriques, théoriques et normatives sur la cybersécurité et la gouvernance des risques numériques. Les résultats de ces activités et projets de recherches ont pour objectif de contribuer au renforcement et à la stabilité de l'écosystème numérique public du Québec et à l'optimisation de la résilience des ministères et organismes. Le Pôle bénéficie du soutien financier des Fonds de recherche du Québec (FRQ).

Les chercheures et chercheurs membres du Pôle sont :

Lyse Langlois, Professeure titulaire, Directrice générale de l'Obvia, Université Laval

Steve Jacob, Professeur titulaire, Université Laval

Benoît Dupont, Professeur titulaire, Université de Montréal

Céline Castets-Renard, Professeure titulaire, Université d'Ottawa

Nadia Tawbi, Professeure titulaire, Université Laval

Daniel J. Caron, Professeur, École nationale d'administration publique (ENAP)

Hugo Loiseau, Professeur titulaire, Université de Sherbrooke

Sébastien Gambs, Professeur, Université du Québec à Montréal

Pierre-Martin Tardif, Professeur agrégé**,** Université de Sherbrooke

Table des matières

Introduction

Les consultations particulières et auditions publiques sur le projet de loi 82, Loi concernant l'identité numérique nationale, offrent l'occasion de réfléchir aux enjeux fondamentaux entourant la transformation numérique de l'État québécois. Cette initiative législative s'inscrit dans un contexte où la numérisation des services publics et la sécurité des données citoyennes sont devenues des impératifs incontournables pour les administrations publiques contemporaines.

Le présent mémoire s'intéresse aux multiples dimensions de l'identité numérique nationale, un projet structurant qui vise à simplifier l'accès aux services gouvernementaux tout en assurant la protection des renseignements personnels des citoyens. Cette démarche témoigne d'une évolution significative de la relation entre l'État et les citoyens à l'ère numérique, où la confiance, l'acceptabilité sociale, la sécurité, la convivialité et l'accessibilité doivent coexister.

Les réflexions et recommandations contenues dans ce mémoire s'appuient sur une analyse approfondie des expériences internationales en matière d'identité numérique, des enjeux de gouvernance et de cybersécurité, ainsi que des considérations sociales et éthiques qui en découlent. Cette analyse permet notamment d'examiner comment le projet de loi 82 positionne le Québec dans ce domaine, en confiant au ministère de la Cybersécurité et du Numérique un rôle central dans la gestion et la protection des identités numériques.

Les transformations proposées soulèvent des questions importantes sur l'équilibre entre l'efficience administrative, la protection des renseignements personnels et l'inclusion numérique. Ces enjeux seront abordés à la lumière des meilleures pratiques observées tant au Québec qu'à l'international, en gardant à l'esprit l'objectif ultime : offrir aux citoyens des services numériques accessibles, sécuritaires et adaptés à leurs besoins.

1. Contexte et opportunité de la démarche

Évolution du contexte technologique et social

Le projet gouvernemental québécois de la transformation numérique vise à permettre aux citoyens de s'authentifier en ligne pour accéder aux services gouvernementaux de manière sécuritaire. L'identité numérique fonctionne comme un substitut pour les documents d'identité physiques tels que le passeport ou le permis de conduire. Les systèmes de gestion de l'identité numérique gouvernementale (SGING) sont complexes en raison des défis sociaux, sécuritaires, de respect de la vie privée et d'interopérabilité. Pour qu'un SGING soit un succès auprès de la population, il est important de reconnaître son utilité et sa nécessité. En 2019, au Québec, le gouvernement s'est engagé à créer le Service québécois d'identité numérique (SQIN) pour doter chaque membre de la population d'une identité numérique. Le déploiement complet du service sera plus long que prévu et est finalement attendu pour 2028. Ainsi, le projet de loi 82 est une étape importante dans cette direction.[1]

État de la situation au Québec

La quatrième révolution industrielle, basée sur le numérique et les données, mène vers une cinquième révolution où l'IA, l'automatisation et la robotisation agissent comme principales locomotives. Les changements entraînés dépassent toutefois le cadre technologique : ils bouleversent profondément notre société, redéfinissent les modèles économiques et soulèvent d'importantes questions éthiques. Ils requièrent des modifications importantes au niveau du fonctionnement de l'administration publique, particulièrement en ce qui a trait à son cadre normatif.[2] Ces modifications ont pour but de favoriser l'implantation de nouveaux outils à l'intérieur des organisations publiques tout en préservant la confiance citoyenne envers l'administration publique. Tous ces développements représentent une occasion d'accélérer la transformation des services publics du Québec au bénéfice des citoyennes et des citoyens.

En 2019, le gouvernement du Québec a adopté sa *Stratégie de transformation numérique gouvernementale 2019-2023*[3] dans le but de fournir une vision commune et cohérente à l'administration publique en vue de réaliser la transformation de l'État par le numérique. La *Stratégie gouvernementale de cybersécurité et du numérique 2024-2028*[4] s'inscrit dans les progrès réalisés par les organismes publics, en mettant l'accent sur un usage responsable, transparent et éthique des données. L'usage des appareils technologiques ou numériques est par ailleurs de plus en plus présent chez les Québécoises et Québécois, avec 95 % d'adultes possédant au moins un tel appareil.[5] Les citoyennes et citoyens du Québec s'attendent désormais aux meilleurs services numériques de la part de l'administration publique grâce à la multiplication des plateformes technologiques offertes par le secteur privé.

---

1 Observatoire international sur les impacts sociétaux de l'intelligence artificielle et du numérique, (2024). *Dans l'œil de l'Obvia - Vers une identité numérique au Québec : Enjeux et défis.* Obvia. https://doi.org/10.61737/DNFC4193

2 Caron, D. J., Bernardi, S. (2021), *Écosystème de la transformation de l'administration publique vers le numérique.* Presses de l'Université du Québec.

3 Gouvernement du Québec, *Stratégie de transformation numérique gouvernementale 2019-2023* (2019). En ligne : https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/Strategie_TNG.pdf

4 Gouvernement du Québec, *Stratégie gouvernementale de cybersécurité et du numérique 2024-2028* (2024). En ligne : https://www.quebec.ca/nouvelles/actualites/details/depot-de-la-nouvelle-strategie-gouvernementale-de-cybersecurite-et-du-numerique-2024-2028-57107

5 Académie de la transformation numérique (2022), *Portrait numérique des foyers québécois.* En ligne : https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/portrait-numerique-des-foyers-quebecois-2022/

Expériences internationales pertinentes

Les expériences internationales en matière d'identité numérique sont nombreuses et ont connu autant de succès que d'échecs. Ce mémoire se base, entre autres, sur les cas de l'Estonie, de l'Australie, de Singapour et de la Suède pour les bonnes pratiques et sur le Royaume-Uni et la Finlande à propos des leçons apprises. Ces études de cas démontrent que l'utilité perçue d'une identité numérique nationale est essentielle à son adoption, voire à son succès. Pour assurer cette utilité, il faut impliquer différents acteurs gouvernementaux et privés dans le processus, ainsi qu'inclure la population utilisatrice pour développer un système répondant à ses besoins. L'adoption ou la modification de normes et de lois, ainsi que la mise en place d'une entité de supervision sont importantes pour la réussite de la gouvernance et de la gestion centralisée de l'identité numérique nationale du Québec. La présence d'une autorité centrale facilite la coordination entre les acteurs impliqués. Les ressources techniques, humaines et financières doivent être mises à disposition des différents acteurs du projet pour assurer le développement, la sécurité et le maintien du système de gestion de l'identité numérique gouvernementale.[6]

6 Gariépy, F., Dupont, B., Castets-Renard, C., Loiseau, H., Langlois, L., Tawbi, N., Tardif, P.-M., Gambs, S., & Jacob, S. (2024), *Guide sur les conditions et bonnes pratiques pour la mise en place d'une identité numérique nationale.* Observatoire international sur les impacts sociétaux de l'intelligence artificielle et du numérique (Obvia). En ligne : https://doi.org/10.61737/AFQC2028

2. Analyse des principales dispositions du projet de loi

Les principes guidant la création d'une identité numérique nationale

Le projet de loi 82, notamment dans ses articles 3 à 6, propose en filigrane des principes guidant la création d'une identité numérique nationale. Ceux-ci sont à souligner et à faire ressortir. Par exemple, dans l'article 6, la sécurité et la confiance se retrouvent dans la définition même de l'identité numérique. Les fins non commerciales, le contrôle des utilisateurs et des utilisatrices sur leurs attestations numériques gouvernementales, l'interopérabilité avec l'environnement numérique existant et la non-imposition de l'identité numérique à une personne sont autant de principes qui sont à mettre en évidence dans la promotion de ce projet de loi. De plus, le registre d'identité numérique nationale, prévu par le projet de loi, prétend répondre aux normes habituelles de cybersécurité que sont la disponibilité, la confidentialité, la non-répudiation et l'intégrité. Seules les modalités d'authentification semblent être passées sous silence dans l'article 6. Autrement dit, qui aura accès au registre, comment la vérification de l'identité sera-t-elle effectuée et comment ces accès seront-ils attribués? Sera-t-il possible pour les citoyens, les personnes morales ou les sociétés de corriger les erreurs concernant leurs données directement dans ce registre? Qu'entend donc le gouvernement par la mention « 3° tout autre renseignement que détermine le gouvernement » et comment cet alinéa sera-t-il balisé? Il serait opportun de clarifier les liens entre l'identité numérique nationale, le registre d'identité numérique nationale, les données numériques gouvernementales et les attestations numériques gouvernementales. Par exemple, est-ce que les attestations numériques gouvernementales seront déposées dans le registre d'identité numérique nationale? Des réponses claires à ces questions favoriseront la transparence nécessaire à une plus grande acceptabilité sociale.

La gouvernance de l'identité numérique nationale

L'identité numérique s'appuie à la fois sur la technologie et les données. Il est donc essentiel qu'elle s'inscrive dans le cadre plus large de la gouvernance informationnelle de l'administration publique[7] pour éviter la création de fonctions trop spécialisées et en silos, contraire à l'esprit de ce qu'est une identité numérique nationale. En effet, l'identité numérique demande une conception différente de l'administration publique qui doit être beaucoup plus fluide dans son fonctionnement interorganisationnel. À cet égard, le projet de loi 82, dans son article 3, n'aborde que les questions de la gouvernance des infrastructures et des services de télécommunications, sans traiter clairement de la gouvernance des ressources informationnelles, financières ou humaines. Certes, la gouvernance des infrastructures est essentielle pour le développement d'une identité numérique nationale, mais il serait réducteur de se limiter à ce seul aspect. Le projet de loi devrait baliser les initiatives de transformations numériques de l'administration publique et des organismes publics en fonction des besoins de l'identité numérique nationale qu'il entend mettre en œuvre.

Par ailleurs, dans ce projet de loi, l'État s'attribue le rôle d'autorité centrale en matière d'identité numérique. Ce second aspect de la gouvernance doit aussi être mis en relief. En effet, dans le projet de loi 82, le gouvernement prévoit que le ministère de la Cybersécurité et du Numérique agisse à titre d'institution centralisatrice pour la mise en œuvre de l'identité numérique nationale en son article 6. Le ministère « développe et soumet au gouvernement une vision globale des infrastructures et des services de télécommunications jugés utiles ou essentiels pour la conduite des affaires de l'État » et agit ainsi comme « source officielle de données numériques gouvernementales ».

7 Caron, D. J., Bhérer, H. et Bernardi, S. (2020), *La gouvernance informationnelle au sein de l'administration publique.* Rapport de recherche. Chaire de recherche en exploitation des ressources informationnelles. École nationale d'administration publique (ÉNAP). En ligne : https://www.creri.org/_files/ugd/8c3d8e_5fb68c99709e4af4bfc93986176eeeec.pdf

De plus, « [l]e ministre assume la responsabilité de la gouvernance et de la gestion centralisée de l'identité numérique nationale ». La verticalité ainsi imposée aux organismes publics du gouvernement du Québec facilite la coordination et la coopération entre les différents acteurs dans le but de déployer un système d'identité numérique uniforme et donc plus intelligible pour l'ensemble du gouvernement et de la population visée. Enfin, cette position centrale que prend le MCN favorise la confiance du public envers ce projet, car elle assure un contrôle démocratique sur la portée de l'identité numérique et une meilleure protection des renseignements personnels.[8]

Les infrastructures technologiques et le rôle du privé

Les articles 7 à 12 du projet de loi sont à souligner puisqu'ils rehaussent, de différentes façons, les mesures pour assurer la cybersécurité et la cyberrésilience des systèmes et des infrastructures essentielles du Québec ainsi que des actifs informationnels du gouvernement du Québec. Ce rehaussement rassurera les autres acteurs présents dans l'environnement de l'identité numérique (citoyens, tiers de confiance, entreprises privées, autres ordres de gouvernements, etc.). Pour des questions d'interopérabilité et de déploiement du projet, notamment sur le plan des infrastructures technologiques et numériques, le secteur privé sera vraisemblablement présent. À l'heure actuelle, il y a un enjeu de manque de transparence important dans la mesure où le projet de loi aborde très peu les choix technologiques à la base de l'identité numérique, laissant une grande marge de manœuvre au MCN. Par exemple, le rôle du secteur privé et son ampleur dans la constitution des infrastructures à la base de l'identité numérique nationale ne sont pas abordés dans le projet de loi. Pour une question de ressources humaines ou technologiques, il est parfois nécessaire d'avoir recours au secteur privé pour réaliser un système d'identité numérique à grande échelle.[9] Deux questions demeurent néanmoins centrales dans ce débat : y aura-t-il un dispositif infonuagique souverain au Québec pour héberger les données gouvernementales? Qui sera propriétaire des données inférées et des données d'usage?

Pour des raisons de transparence et d'acceptabilité sociale, il serait donc judicieux de clairement baliser et justifier le recours éventuel à la sous-traitance et aux partenariats publics-privés dans le projet de loi et de clarifier où seront hébergées les données gouvernementales et les attestations numériques gouvernementales. Pour des raisons d'analyse des enjeux de sécurité et de vie privée, il est important que l'architecture envisagée, ainsi que les protocoles d'authentification et d'échanges de données qui seront mis en place, soient détaillés afin de pouvoir être audités par des experts en sécurité et protection des données. La transparence sur ces aspects est un ingrédient nécessaire pour réaliser une étude des facteurs relatifs à la vie privée (EFVP) qui analyserait en amont les risques de vie privée liés au projet d'identité numérique, permettant d'intégrer adéquatement cette analyse dès la conception du système.

La numérisation des pièces d'identité, qui remplace progressivement les documents papier traditionnels, soulève des préoccupations en matière de confidentialité. En effet, chaque fois qu'un citoyen utilise son identité numérique, cette action peut créer des empreintes électroniques qui sont susceptibles d'être collectées et stockées de manière automatique. En fonction du choix d'architecture effectué pour implémenter l'identité numérique, en particulier si les données collectées sont centralisées, il devient possible de les croiser facilement et de générer de nouvelles données qui peuvent mener à un profilage précis et à des risques de surveillance. Cela ouvre ainsi la possibilité pour le gouvernement d'utiliser ces données pour catégoriser les citoyens par rapport à leurs comportements en termes de santé, de mobilité ou de gestion financière. Ces questions se posent d'autant plus dans un contexte d'exception juridique justifié par un état d'urgence ou par un changement de gouvernement, où il pourrait être décidé d'utiliser ces données à des fins différentes de celles initialement prévues, possiblement en contournant les garde-fous qui avaient été mis en place.

8 Gariépy, F. *et al.*, (2024), *Guide sur les conditions et bonnes pratiques pour la mise en place d'une identité numérique nationale*, p.9-10, Observatoire international sur les impacts sociétaux de l'intelligence artificielle et du numérique (Obvia). En ligne : https://doi.org/10.61737/AFQC2028

9 *Ibid*, p.11

3. Recommandations

1 Miser sur le dialogue et la transparence pour construire l'acceptabilité sociale de l'identité numérique nationale

Un des grands enjeux pour nos gouvernements est d'assurer l'acceptabilité sociale de ses projets. Que ce soit en matière d'environnement, de transport ou de l'usage de technologies permettant l'utilisation et le partage de renseignements personnels, l'acceptabilité sociale est aujourd'hui un levier pour favoriser le succès de ce type d'initiatives. Le concept d'acceptabilité sociale a plusieurs connotations, mais sa signification et sa manifestation sont profondément ancrées dans le dialogue et le fruit de ce dialogue entre les décideurs publics et la population. L'acceptabilité sociale se construit inévitablement par la confiance. Comme nous l'avons constaté dans nos travaux, l'identité numérique n'y échappe pas et la manière d'aborder ce projet de création d'une identité numérique nationale aura donc une incidence sur son taux d'acceptation et d'utilisation.

Une enquête auprès de 2 000 citoyens québécois, menée à la fin du printemps 2024[10], portant sur la confiance, le partage de données et l'identité numérique a montré que 25 % des personnes interrogées ne sont pas du tout ouvertes à l'identité numérique. Plus spécifiquement, une grande majorité de répondants [86,9 % (n=1724/1985)] s'est déclarée favorable à l'utilisation de l'identité numérique si certaines conditions étaient respectées. Par exemple, sur le plan de la sécurité, les citoyens seraient plus ouverts à l'identité numérique si le gouvernement implantait de meilleurs systèmes de sécurité ou s'il s'assurait de limiter le nombre d'endroits où les renseignements d'identification sont détenus. Sur le plan du service, une meilleure communication avec le gouvernement et une réduction du délai des prestations seraient des éléments qui favoriseraient l'adhésion citoyenne à l'identité numérique.

Enfin, l'enquête a fait ressortir que les craintes sont plus élevées lorsque l'identité numérique touche au partage de données fiscales ou de données de santé. Toutes les initiatives de partage de données qui satisfont les attentes citoyennes en matière de partage de renseignements de santé devraient être mieux acceptées.[11]

10 Caron, D. J., Lamarche, P-O et Nicolini, V. (2025, à paraître), *Étude sur le partage de renseignements personnels et l'utilisation d'outils numériques dans les services publics*, dans : Confiance, administration publique et numérique. Rapport de recherche. CRERI et Obvia.

11 *Ibid.*

2 Renforcer les capacités de cybersécurité pour protéger l'intégrité de l'identité numérique nationale

Il est essentiel de prendre en compte les risques et le niveau d'assurance nécessaire pour développer un système d'identité numérique nationale, cherchant l'équilibre entre simplicité et sécurité. Dès la conception, des mécanismes doivent être adoptés pour assurer la pérennité et la résilience du système ainsi que pour le protéger contre les intrusions, les usages malveillants et les fuites de données personnelles. C'est pourquoi il est nécessaire d'investir et de réglementer pour assurer la cybersécurité des infrastructures numériques et technologiques sous-jacentes à la réalisation d'une identité numérique nationale. Il ressort de l'enquête citée ci-dessus que pour adhérer à l'idée d'utiliser l'identité numérique, la sécurité apparaît globalement comme plus importante que des facteurs comme l'efficacité des services.[12]

Dans un même ordre d'idée, une majorité de Québécois est d'accord pour dire que le gouvernement du Québec a la volonté d'assurer une gestion sécuritaire des données. Toutefois, seulement 40 % croient que ce dernier possède les outils nécessaires pour le faire. Plus précisément, près de 60 % des répondants pensent que le gouvernement est peu outillé ou pas du tout outillé pour répondre à certains enjeux comme les cyberattaques, la consultation non permise de données ou la fraude. D'ailleurs, l'enquête a montré que les citoyens craignent davantage les cyberattaques et l'hameçonnage que la surveillance par le gouvernement.[13]

3 Assurer une protection robuste des renseignements personnels par une architecture décentralisée et des mécanismes de contrôle citoyens

La protection des renseignements personnels devrait être un aspect essentiel de la conception du système d'identité numérique. En particulier, cela requiert que l'architecture mise en place pour l'identité numérique évite une centralisation excessive des données des citoyens, ce qui causerait aussi des enjeux de cybersécurité importants puisque cette base centralisée deviendrait une cible de choix pour les attaquants, comme cela a été le cas dans plusieurs pays. Pour éviter des enjeux de surveillance généralisée, il est également important de s'assurer que l'identité numérique mise en place limite les renseignements personnels échangés (incluant les données d'usage et inférées), en cherchant à minimiser les données révélées lors d'un accès à un service par son identité numérique. Ainsi, il serait possible, en utilisant des approches cryptographiques de type « accréditation anonyme », de fournir une preuve liée à son identité (comme son âge ou le droit d'accès à une ressource) sans révéler toutes les informations de son identité.[14]

La transparence est aussi un enjeu clé de la protection des renseignements personnels. En particulier, les standards techniques utilisés pour implémenter l'identité numérique devraient être rendus publics en amont afin de permettre à des chercheurs en sécurité informatique et cryptographie de contribuer à analyser et à corriger les failles de sécurité potentielles. La publication de l'évaluation des facteurs relatifs à la vie privée (EFVP) permettrait aussi de comprendre toute la réflexion qui a été suivie pour s'assurer que les enjeux de protection de la vie privée ont été adéquatement pris en considération, en plus de renforcer la confiance du public. Il est aussi important de mettre en place des mécanismes permettant à un citoyen de mieux contrôler les données de son identité numérique, en particulier en lui donnant un accès facile à son profil, lui permettant de corriger des informations erronées, voire d'exercer un droit à l'effacement sur certains renseignements personnels non critiques.

---

12 Caron, D. J., Lamarche, P-O et Nicolini, V. (2025, à paraître), *Étude sur le partage de renseignements personnels et l'utilisation d'outils numériques dans les services publics*, dans : Confiance, administration publique et numérique. Rapport de recherche. CRERI et Obvia.

13 *Ibid.*

14 Deswarte, Y., Gambs, S. (2010), *A Proposal for a Privacy-preserving National Identity Card.* Dans, Transaction on Data Privacy 3(3): 253-276 (2010). En ligne : http://www.tdp.cat/issues/abs.a060a10.php

4 Adopter une approche inclusive et collaborative impliquant l'ensemble des parties prenantes dans le développement et le déploiement de l'identité numérique nationale

Grâce à des processus de consultation, l'implication des acteurs concernés (comme des organisations gouvernementales et des entreprises privées dans certains cas) permet de concilier les attentes et objectifs de tous pour que le projet de création d'une identité numérique nationale réponde aux préoccupations de toutes les parties prenantes. Pour contrer les effets de la fracture numérique et augmenter l'accessibilité au système d'identité numérique, une approche centrée sur l'utilisateur, de type « identité autosouveraine », est donc nécessaire. Cette dernière souligne les avantages de l'usage de l'identité numérique, tels que la simplification des démarches administratives, l'amélioration de l'accès aux services publics, la simplicité d'utilisation et la compatibilité entre diverses plateformes technologiques (ordinateur, tablette et téléphone cellulaire) ou systèmes d'exploitation.[15]

5 Confirmer le rôle central du ministère de la Cybersécurité et du Numérique dans la gouvernance de l'identité numérique nationale

La présence d'une autorité publique centrale telle que le MCN permet la coordination et la coopération entre les organisations publiques, facilitant la communication entre celles-ci tout en guidant une transformation numérique de l'administration publique pour développer des compétences et des expertises pertinentes. Cette centralisation contribue aussi à uniformiser l'identité numérique en évitant le dédoublement des systèmes et clarifie les rôles et responsabilités des organismes publics impliqués dans la démarche, établissant ainsi une gouvernance saine. De plus, il est fortement recommandé que le gouvernement du Québec pérennise sa souveraineté numérique en demeurant pleinement propriétaire des données des citoyens du Québec et en s'assurant que ces données soient entreposées dans une infrastructure infonuagique souveraine. L'ensemble de ces éléments favorise la cybersécurité du système d'identité numérique nationale et la confiance du public.[16]

6 Maximiser la valeur et l'utilité quotidienne de l'identité numérique nationale pour les citoyens

Les expériences internationales sur la création et l'implantation de système d'identité numérique démontrent que l'utilisation croissante de l'identité numérique augmente sa valeur aux yeux des citoyens. Par exemple, une utilisation quotidienne de ce système accroît son taux d'adoption parce qu'il est perçu comme étant utile et sécuritaire.[17] Si nécessaire, la collaboration avec le secteur privé, par exemple pour élargir les possibilités d'utilisation, peut renforcer cette perception d'utilité auprès de la population visée. Pour ce faire, il est crucial de protéger les données personnelles et de respecter la vie privée des utilisateurs en renforçant les processus et mécanismes d'authentification, en limitant le partage des informations personnelles, en permettant aux utilisateurs de garder le contrôle sur leurs données personnelles et en assurant une interaction sécuritaire avec les organismes publics et les entreprises privées prestataires de services.

---

15 Observatoire international sur les impacts sociétaux de l'intelligence artificielle et du numérique, (2024). *Dans l'œil de l'Obvia - Vers une identité numérique au Québec : Enjeux et défis.* Obvia. https://doi.org/10.61737/DNFC4193

16 Melin, U., Karin, A., et Fredrik, S. (2016), *Managing the Development of E-ID in a Public e-Service Context.* Dans, Transforming Government: People, Process and Policy, 2016, 10 (1): 72-98. En ligne : https://doi.org/10.1108/TG-11-2013-0046

17 OCDE (2011), *National Strategies and Policies for Digital Identity Management in OECD Countries.* OECD Publishing. En ligne : https://doi.org/10.1787/5kgdzvn5rfs2-en

Conclusion

Le projet de loi 82 marque une étape importante dans la transformation numérique de l'État québécois. L'analyse présentée dans ce mémoire démontre que la création d'une identité numérique nationale représente bien plus qu'un simple changement technologique – elle incarne une redéfinition substantielle de la relation entre les citoyens et leur gouvernement à l'ère numérique.

Les résultats de nos travaux révèlent que les Québécois sont majoritairement favorables à cette évolution, tout en exprimant des attentes légitimes en matière de sécurité et de protection de leurs renseignements personnels. La confiance des citoyens, essentielle au succès de ce projet, repose sur la capacité de l'État à démontrer non seulement sa volonté, mais aussi ses moyens de protéger adéquatement les données personnelles des Québécois et des Québécoises contre les cybermenaces.

La décision de confier la gouvernance de l'identité numérique nationale au ministère de la Cybersécurité et du Numérique constitue un pas dans la bonne direction. Toutefois, certains aspects cruciaux du projet de loi mériteraient d'être précisés, notamment concernant l'hébergement souverain des données, l'encadrement des partenariats avec le secteur privé ainsi que la prise en compte des enjeux de vie privée dès la conception. Aussi, comme l'ont démontré les expériences d'autres juridictions, le succès d'un tel projet dépend de sa capacité à susciter et maintenir la confiance des citoyens, notamment à travers des garanties claires concernant la protection des renseignements personnels et la cybersécurité.

En nous basant sur la littérature scientifique et des enquêtes récentes[18], nous avons proposé plusieurs leviers et facteurs pouvant influencer l'acceptabilité sociale de projets comme celui de l'identité numérique : la confiance, la sécurité et la protection de la vie privée, la littératie citoyenne à l'égard de ces questions, les modalités de partage et la transparence quant à ces modalités, les connaissances des bénéfices potentiels et les caractéristiques sociodémographiques des individus. Il est recommandé de travailler ces aspects dès maintenant et de les inscrire dans les outils normatifs appropriés – lois, politiques publiques, politiques administratives, règlements, etc.

En définitive, le succès de ce projet structurant pour le Québec reposera sur notre capacité collective à maintenir un équilibre entre innovation technologique, protection des droits individuels et accessibilité des services. Les recommandations formulées dans ce mémoire visent précisément à contribuer à l'atteinte de cet équilibre. L'identité numérique nationale représente un projet d'envergure qui, bien encadré et déployé avec les garanties appropriées, peut contribuer significativement à la modernisation de l'État québécois tout en renforçant la confiance des citoyens dans leurs institutions.

18 Voir, entre autres :

Caron, D. J., Bernardi, S. et Nicolini, V. (2020), *L'acceptabilité sociale du partage des données de santé : revue de la littérature.* Rapport de recherche. Chaire de recherche en exploitation des ressources informationnelles. École nationale d'administration publique (ÉNAP). En ligne : https://www.creri.org/_files/ugd/8c3d8e_30a35caa9d374e3884c5680258e7ae9f.pdf

Caron, D. J., Montmarquette, C., Prud'homme, A., Bernardi, S. et Nicolini, V. (2020), *Projet sur l'acceptabilité sociale du partage des renseignements de santé - Enquête sur l'acceptabilité sociale du partage des renseignements de santé : constatations, résultats et variations.* Rapport final. Chaire de recherche en exploitation des ressources informationnelles. École nationale d'administration publique (ÉNAP). En ligne : https://www.creri.org/_files/ugd/8c3d8e_d54364e9bab546c48166c7f553fe4c95.pdf

Bibliographie

Académie de la transformation numérique (2022), *Portrait numérique des foyers québécois*. En ligne : https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/portrait-numerique-des-foyers-quebecois-2022/

Assemblée nationale du Québec (2024), *Projet de loi 82 Loi concernant l'identité numérique nationale et modifiant d'autres dispositions*. En ligne : https://www.assnat.qc.ca/fr/travaux-parlementaires/%20projets-loi/projet-loi-82-43-1.html

Caron, D. J., Bernardi, S. (2021), *Écosystème de la transformation de l'administration publique vers le numérique*. Presses de l'Université du Québec.

Caron, D. J., Bernardi, S. et Nicolini, V. (2020), *L'acceptabilité sociale du partage des données de santé : revue de la littérature*. Rapport de recherche. Chaire de recherche en exploitation des ressources informationnelles. École nationale d'administration publique (ÉNAP). En ligne : https://www.creri.org/_files/ugd/8c3d8e_30a35caa9d374e3884c5680258e7ae9f.pdf

Caron, D. J., Bhérer, H. et Bernardi, S. (2020), *La gouvernance informationnelle au sein de l'administration publique*. Rapport de recherche. Chaire de recherche en exploitation des ressources informationnelles. École nationale d'administration publique (ÉNAP). En ligne : https://www.creri.org/_files/ugd/8c3d8e_5fb68c99709e4af4bfc93986176eeeec.pdf

Caron, D. J., Lamarche, P-O et Nicolini, V. (2025, à paraître), *Étude sur le partage de renseignements personnels et l'utilisation d'outils numériques dans les services publics*, dans : Confiance, administration publique et numérique. Rapport de recherche. CRERI et Obvia.

Caron, D. J., Montmarquette, C., Prud'homme, A., Bernardi, S. et Nicolini, V. (2020), *Projet sur l'acceptabilité sociale du partage des renseignements de santé - Enquête sur l'acceptabilité sociale du partage des renseignements de santé : constatations, résultats et variations*. Rapport final. Chaire de recherche en exploitation des ressources informationnelles. École nationale d'administration publique (ÉNAP). En ligne : https://www.creri.org/_files/ugd/8c3d8e_d54364e9bab546c48166c7f553fe4c95.pdf

Deswarte, Y., Gambs, S. (2010), *A Proposal for a Privacy-preserving National Identity Card*. Dans, Transaction on Data Privacy 3(3): 253-276 (2010). En ligne : http://www.tdp.cat/issues/abs.a060a10.php

Gariépy, F., Dupont, B., Castets-Renard, C., Loiseau, H., Langlois, L., Tawbi, N., Tardif, P.-M., Gambs, S., & Jacob, S. (2024), *Guide sur les conditions et bonnes pratiques pour la mise en place d'une identité numérique nationale*. Observatoire international sur les impacts sociétaux de l'intelligence artificielle et du numérique (Obvia). En ligne : https://doi.org/10.61737/AFQC2028

Gouvernement du Québec, *Stratégie de transformation numérique gouvernementale 2019-2023* (2019). En ligne : https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/Strategie_TNG.pdf

Gouvernement du Québec, *Stratégie gouvernementale de cybersécurité et du numérique 2024-2028* (2024). En ligne : https://www.quebec.ca/nouvelles/actualites/details/depot-de-la-nouvelle-strategie-gouvernementale-de-cybersecurite-et-du-numerique-2024-2028-57107

Groupe de recherche interdisciplinaire en cybersécurité (GRIC) (2021), *Guide d'encadrement sécuritaire de l'identité numérique dans un contexte de transformation organisationnelle numérique infonuagique*. Université de Sherbrooke.

Melin, U., Karin, A., et Fredrik, S. (2016), *Managing the Development of E-ID in a Public e-Service Context*. Dans, Transforming Government: People, Process and Policy, 2016, 10 (1): 72-98. En ligne : https://doi.org/10.1108/TG-11-2013-0046

Ministère de la Cybersécurité et du Numérique (2024), *Mémoire au conseil des ministres — Projet de loi concernant l'identité numérique nationale et modifiant d'autres dispositions*, gouvernement du Québec. En ligne : https://cdn-contenu.quebec.ca/cdn-contenu/gouvernement/MCE/dossiers-soumis-conseil-ministres/24-25/2024-0179_memoire.pdf

Observatoire international sur les impacts sociétaux de l'intelligence artificielle et du numérique, (2024). *Dans l'œil de l'Obvia - Vers une identité numérique au Québec : Enjeux et défis*. Obvia. https://doi.org/10.61737/DNFC4193

OCDE (2011), *National Strategies and Policies for Digital Identity Management in OECD Countries*. OECD Publishing. En ligne : https://doi.org/10.1787/5kgdzvn5rfs2-en

obvia

obvia.ca