



Enquête

sur la confiance et l'acceptabilité sociale dans l'usage de l'identité numérique au Québec

Daniel J. Caron
Pierre-Olivier Lamarche
Vincent Nicolini
Alexandre Prud'homme

obvia



Chaire de recherche en exploitation
des ressources informationnelles

Mai 2025

Auteurs

Daniel J. Caron

Professeur à l'ENAP, professeur associé à la SPPA de l'Université Carleton, titulaire de la Chaire de recherche en exploitation des ressources informationnelles (CRERI), chercheur et Fellow du CIRANO, 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.

Pierre-Olivier Lamarche

Professionnel de recherche à l'Obvia pour le Pôle d'expertise en cybersécurité et impacts sociétaux.

Vincent Nicolini

Chargé d'enseignement à l'ENAP et chercheur affilié à la Chaire de recherche en exploitation des ressources informationnelles (CRERI).

Alexandre Prud'homme

Professionnel de recherche au CIRANO.

Remerciements

Les auteurs tiennent à remercier Sébastien Brousseau et Isabelle Winter pour leur relecture ainsi que leurs commentaires qui ont contribué à améliorer la qualité de ce rapport.

Le projet de recherche ayant mené à la rédaction de ce rapport est issu d'une collaboration entre le Pôle d'expertise en cybersécurité et impacts sociétaux de l'Obvia (soutenu financièrement par le Fonds de recherche du Québec), et la Chaire de recherche en exploitation des ressources informationnelles – CRERI (financé, pour ce projet, par le MCN et le MSSS).

Produit avec le soutien financier du Fonds de recherche du Québec



Table des matières

Sommaire exécutif	4
Introduction	5
Contexte	6
Objectifs et Méthodologie	7
Outil de collecte de données	9
Collecte de données	10
Considérations éthiques	10
Résultats	11
Niveau de confiance générale selon différentes catégories d'individus	12
Confiance envers la capacité et la volonté du gouvernement du Québec	13
Degré d'ouverture face à l'identité numérique	14
Profils socio-démographiques en fonction du degré d'ouverture	17
Conclusion	19
Références	22
Annexe 1 : Questionnaire	23

Sommaire exécutif

Ce rapport présente les résultats d'une enquête portant sur la confiance et la disposition des citoyens envers l'adoption de l'identité numérique dans la province de Québec. L'enquête, fondée sur une méthodologie d'économie expérimentale, a exploré différentes dimensions de la confiance ainsi que les différents paramètres qui peuvent venir renforcer cette confiance. L'enquête a été réalisée auprès d'un échantillon représentatif de la population québécoise et le rapport qui suit présente les constatations qui peuvent être tirées des résultats obtenus.

Les résultats indiquent qu'une grande majorité des citoyens seraient ouverts à utiliser l'identité numérique, mais à certaines conditions. La mise en place de meilleurs systèmes de sécurité constitue, entre autres, un élément clé pour favoriser l'ouverture à l'utilisation de l'identité numérique. Les résultats permettent aussi de constater que les répondants avaient généralement confiance en la volonté du gouvernement de mener à bien le projet d'identité numérique. Cependant, sa capacité de le mener à bien était quant à elle plus généralement remise en question.

Cette enquête permet d'identifier des leviers pour accroître l'ouverture à l'utilisation d'une identité numérique au Québec et de faire un portrait de la confiance des citoyens québécois envers leur gouvernement, dans un contexte de transition vers le numérique. Il est important pour les citoyens que le gouvernement soit transparent lors de la mise en place de l'identité numérique. Par exemple, il faut que les différents systèmes de sécurité en place ainsi que les bénéfices et le fonctionnement général soient connus et clairement expliqués. De plus, les analyses différenciées présentées dans ce rapport montrent l'importance d'adapter les messages en fonction des différents profils sociodémographiques de la population.

Introduction

Le gouvernement du Québec progresse dans la mise en place d'une administration reposant toujours plus sur les technologies de l'information et de la communication. L'identité numérique fait partie d'une série de mesures législatives, réglementaires et organisationnelles ayant pour objectif de transformer le fonctionnement de l'État québécois¹. Le projet de loi 82 définit l'identité numérique comme: « l'ensemble des moyens dont dispose l'État pour garantir à toute personne un accès sécurisé aux prestations électroniques de services gouvernementales et lui permettre d'avoir un niveau de confiance élevé lors de ses interactions avec les organismes publics » (Projet de loi n° 82, Loi concernant l'identité numérique nationale et modifiant d'autres dispositions, 2025). Toutefois, pour devenir fonctionnel, ce passage vers une standardisation des rapports État-citoyen en utilisant un seul identifiant aura plusieurs ramifications sur les relations entre les ministères et organismes ainsi que sur le fonctionnement interne propre à chaque ministère et organisme. Le succès de ce chantier repose sur la simplification de la collecte, du partage, du traitement et de l'exploitation des informations personnelles à travers les institutions et organisations de l'État québécois. C'est un projet complexe qui aura des incidences sur la protection des renseignements personnels et sur le fonctionnement de l'appareil gouvernemental. Puisqu'il est annoncé que l'utilisation de l'identité numérique sera facultative dans sa phase initiale, le succès du chantier reposera également sur son acceptabilité sociale. Ainsi, il ne suffit pas de surmonter les obstacles techniques et organisationnels; pour garantir le succès de cette initiative, il sera essentiel qu'une partie de la population comprenne le concept, y adhère, et s'approprie la solution proposée. De ce fait, il faut que le gouvernement connaisse et comprenne les préoccupations citoyennes et les conditions nécessaires à cette appropriation. Le but du présent rapport est de présenter des résultats d'enquête contribuant à faire état du niveau de confiance des citoyens par rapport à l'identité numérique gouvernementale et d'établir quelles sont les principales conditions qui favorisent ou freinent l'ouverture à son utilisation.

¹ On peut ici penser au Plan stratégique 2023-2027 du ministère de la Cybersécurité et du Numérique (<https://www.quebec.ca/nouvelles/actualites/details/depot-du-plan-strategique-2023-2027-du-ministere-de-la-cybersecurite-et-du-numerique-48575>), la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (<https://www.legisquebec.gouv.qc.ca/fr/document/lc/G-1.03>), la loi 25 (<https://www.legisquebec.gouv.qc.ca/fr/document/lc/G-1.03>), etc.

Contexte

L'utilisation des technologies de l'information et de la communication prend différentes formes et crée une multitude d'attentes auprès des consommateurs et des citoyens. L'administration publique n'est pas en reste et est de plus en plus interpellée par ce potentiel, ce qui l'amène à devoir s'interroger sur ses modes de fonctionnement et sur la manière dont elle interagit avec les citoyens. Qu'il s'agisse de plateformes de collaboration pour élargir les modes de travail (Benedetto-Meyer & Boboc, 2021), de procédures cryptées garantissant la meilleure authenticité possible des données comme la chaîne de blocs (Institut de gouvernance numérique, 2019) ou encore de l'usage d'interfaces transactionnelles utilisant des assistants virtuels (Boudreau, 2023) la Ville de Laval a déployé divers projets numériques pour améliorer l'expérience des citoyens qui la contactent par divers moyens de communication et pour diverses raisons. Le projet de numérisation de la prestation le plus connu est certainement le projet « Requêtes citoyennes », entamé il y a environ 5 ans, qui a remporté différents prix¹. Ce projet a mené à la création d'un système de gestion de la relation client (CRM, ces outils demandent de repenser les systèmes bureaucratiques et leurs modes de fonctionnement.

Les conséquences de l'utilisation de ces technologies sont importantes sur le fonctionnement interne, l'interface de services avec les usagers ou encore la participation citoyenne aux délibérations sur les politiques publiques. Premièrement, les gouvernements sont appelés à se transformer pour intégrer ces nouveaux outils afin de maintenir leur pertinence, voire accroître leur efficacité et leur efficacie. Cette transformation est souvent rendue complexe du fait qu'elle touche à une multitude de sous-systèmes de l'organisation et que les organisations bureaucratiques ont des processus bien établis, voire rigides, avec des cadres opérationnels très normés. Deuxièmement, au-delà de ces enjeux organisationnels qui rendront possible ou non l'utilisation de ces technologies, il y a un prérequis obligatoire qui consiste à pouvoir utiliser l'information sous toutes ses formes, ce qui diffère des pratiques usuelles dans un univers dominé par la documentation papier. En fait, ces technologies fonctionnent grâce à une utilisation intensive de données de toute nature, ce qui engendre de nombreuses préoccupations concernant la protection et la sécurité des données, les usages qui pourraient en être faits ou encore les dérives potentielles en lien avec ces différents usages. Troisièmement, les citoyens s'attendent de plus en plus à participer aux décisions publiques en ce qui a trait au fonctionnement de l'administration tout comme à la définition et la conception des politiques publiques. C'est pourquoi il est crucial que les institutions publiques s'assurent du maintien d'un rapport de confiance entre elles et les citoyens en ce qui a trait à ses orientations et pratiques. La confiance est au cœur du fonctionnement de l'administration publique que celui-ci soit numérique ou non.

Le partage des données pour la conduite des affaires de l'État est donc un enjeu qui demande compréhension et balisage. Il en va de son effectivité. L'identité numérique est un projet qui touche à la fois la mise en place d'un système informatique et l'utilisation intensive de données personnelles. Elle nécessite la refonte de plusieurs mécanismes et fonctionnements à l'intérieur du système bureaucratique. Un tel projet doit en outre, pour cheminer, être appuyé par les citoyens qui auront à l'utiliser. Ce sont des changements notables dans les façons de faire de l'État qui soulèvent plusieurs questions qui nécessiteront des réponses. Par exemple, que pensent les citoyens de ces nouvelles manières de faire? L'utilisation de ces plateformes doit-elle répondre à des exigences particulières pour que les citoyens y adhèrent? C'est à ce genre de questions que la présente enquête, menée selon une approche d'économie expérimentale, a pour objectif de répondre.

1

Objectifs et méthodologie

Objectifs

La recherche s'est d'abord intéressée à la confiance des citoyens envers l'appareil étatique de manière générale. Ensuite, nous avons voulu savoir ce que les gens pensaient de la mise sur pied de l'identité numérique en évaluant s'ils étaient ouverts ou non à son utilisation. À partir de ce premier point de vue des participants, nous avons voulu savoir si ces derniers étaient prêts à changer d'idée dans la mesure où nous les informions de la nature et du fonctionnement de l'identité numérique. Ces informations touchaient les retombées positives de l'identité numérique telles que présentées par le MCN et les mesures de protection qui pourraient être mises en place pour garantir sécurité et confidentialité. De là, nous avons tenté de dégager les conditions nécessaires pour que les participants réticents au départ changent d'idée et s'ouvrent à utiliser cette solution.

Méthodologie

De façon à obtenir la couverture la plus large, l'enquête a été menée auprès de 2020 répondants suivant un mode de collecte bimodale, soit en ligne et par téléphone. La collecte de données a été effectuée par la firme de sondage SOM².

Population, échantillon et stratégie d'échantillonnage

La population ciblée était les adultes québécois de 18 ans ou plus, qui étaient en mesure de répondre à un sondage en français ou en anglais. L'échantillonnage a été stratifié proportionnellement selon trois grandes zones géographiques : la région métropolitaine de recensement (RMR) de Montréal (49 %), la RMR de Québec (10,5 %), et ailleurs au Québec (40,5 %).

Pour la partie téléphonique, l'échantillon initial a été généré aléatoirement à partir de tous les numéros de téléphone valides sur le territoire visé, à l'aide du progiciel « CONTACT » de SOM. L'échantillon contient des numéros de lignes fixes et cellulaires. Dans les RMR de Québec et Montréal, 75 % des répondants ont été rejoints via un numéro de cellulaire, et en région, 60 %. Pour les lignes fixes, un adulte a été sélectionné au sein du ménage via une procédure de sélection aléatoire basée sur l'âge. Pour les cellulaires, les répondants étaient sélectionnés s'ils avaient plus de 18 ans.

Pour la partie web, des répondants potentiels ont été d'abord sélectionnés via le panel « OR » de SOM, qui est un panel probabiliste constitué d'internautes recrutés de façon aléatoire par téléphone. Ensuite, l'échantillon a été constitué grâce à un algorithme visant la meilleure représentativité possible en fonction de la région, de l'âge, du genre, de la langue maternelle, de la scolarité et de la taille du ménage. Pour les groupes des 18 à 34 ans ainsi que des individus moins scolarisés, un panel externe a été utilisé pour compléter l'échantillon.

En raison d'une erreur technique lors de la collecte de données par téléphone³, des participants supplémentaires ont été ajoutés dans le volet web pour compenser. Aussi, 71 questionnaires n'ont pas été remplis correctement par les participants; ils ont donc été exclus des analyses. Au total, notre échantillon se constitue de 824 répondants par téléphone et 1196 répondants web.

2 SOM est une firme de recherche québécoise spécialisée dans la collecte, l'analyse et la visualisation des données (<https://www.som.ca/a-propos>).

3 Il y a eu une erreur de programmation dans la version initiale du questionnaire téléphonique : 175 répondants n'ont pas répondu à la question sur la confiance envers les élus provinciaux.

Outil de collecte de données

Le questionnaire⁴ a été conçu par l'équipe de recherche selon une approche d'économie expérimentale (Eber & Willinger, 2005), qui consiste à tester l'impact de l'introduction de différentes conditions sur les réponses des participants. Une première section du questionnaire visait à s'interroger sur le sentiment de confiance général envers les gouvernements dans le contexte de la protection des renseignements personnels et des services en ligne. Dans cette section, l'accent était également mis sur l'identification des risques perçus, ainsi que sur la capacité des gouvernements et du secteur privé de gérer ces risques. Pour compléter le portrait, nous avons pris le pouls de l'utilisation de différentes technologies numériques et services en ligne par les répondants.

Une seconde section du questionnaire visait à comprendre quels étaient les leviers et les freins à l'adoption d'un système d'identité numérique québécois. Cette section visait aussi à spécifier les causes de la confiance ou de l'absence de confiance des répondants à l'égard de l'implantation et la gestion de l'identité numérique par le gouvernement. À la suite d'une brève description de ce qu'est l'identité numérique, nous demandions aux répondants s'ils étaient ouverts à l'utiliser lors de la prestation de services gouvernementaux. Voici le détail des parcours des participants selon leurs réponses aux questions.

- 1 Pour ceux qui étaient totalement ouverts à l'utilisation de l'identité numérique, ils étaient redirigés vers une section qui approfondissait la confiance envers le gouvernement (voir point 4), à laquelle tous les participants répondaient.
- 2 Pour les participants qui n'étaient pas totalement ouverts à l'utilisation de l'identité numérique, on leur présentait des bénéfices associés à l'identité numérique. S'ils étaient ouverts à la suite de la présentation des bénéfices, ils étaient redirigés vers la section qui approfondissait la confiance envers le gouvernement (voir point 4).
- 3 Pour ceux qui étaient encore réticents, on leur présentait des mesures qui pourraient être mises en place pour atténuer les risques associés à l'identité numérique, pour voir si cela pouvait les rendre ouverts à son utilisation.
- 4 Tous les participants arrivaient à la section du questionnaire sur la confiance envers le gouvernement dans le contexte de la mise en place de l'identité numérique. On leur demandait s'ils étaient d'accord avec des affirmations concernant les moyens, la capacité et la volonté du gouvernement à bien gérer l'identité numérique⁵.
- 5 Pour tous les participants, on interrogeait leur ouverture à l'identité numérique si elle était mise en place par une institution financière ou un géant du web (Google, Amazon ou Apple) pour le compte du gouvernement québécois.
- 6 La dernière section du questionnaire visait à relever les caractéristiques sociodémographiques de tous les participants.

Un prétest a été fait le 12 avril 2024 auprès de 10 participants. Le questionnaire a par la suite été approuvé par l'équipe de recherche. Le questionnaire pour l'enquête en ligne a été adapté de la version téléphonique, en faisant le moins de changements possible pour diminuer les biais liés à l'instrument de mesure et au mode de collecte.

⁴ Le questionnaire complet peut être consulté à l'annexe 1.

⁵ Pour ceux qui étaient d'emblée totalement ouverts à l'utilisation de l'identité numérique, mais qui ne croyaient pas que le gouvernement avait les moyens ou la capacité de le faire, une question supplémentaire (ouverte) leur demandait ce qui pourrait augmenter leur perception de cette capacité du gouvernement. Ces données qualitatives seront analysées ultérieurement.

Collecte de données

La collecte de données s'est déroulée du 12 avril au 21 mai 2024 pour la partie par téléphone, du 25 avril au 9 mai 2024 pour la partie en ligne et du 17 au 22 mai 2024 pour les 175 répondants supplémentaires afin de compenser l'erreur de programmation. La durée moyenne des appels téléphoniques a été de 14,5 minutes et les répondants en ligne ont mis en moyenne 8,3 minutes pour remplir le questionnaire. Le taux de réponse pour les répondants au téléphone était de 9,7 %, et le taux de participation en ligne de 42,2 %. Les données recueillies par téléphone et par web ont été fusionnées en un tout et ont été pondérées pour chacune des trois zones géographiques en fonction d'une distribution conjointe âge/genre⁶, le fait ou non de vivre seul, le plus haut diplôme obtenu⁷ et une distribution de la langue maternelle⁸.

Considérations éthiques

Le projet a fait l'objet d'une demande éthique présentée au Comité d'éthique de l'École nationale d'administration publique. Cette étape a permis de vérifier que le projet de recherche était conforme aux normes en matière d'intégrité et d'éthique en recherche ainsi que sur les conflits d'intérêts. Le numéro de référence de la certification éthique est le CÉR-ÉNAP 2024 – 01.

6 Selon six catégories d'âge, soit 18-24 ans, 25-34 ans, 35-44 ans, 45-54 ans, 55-64 ans, 65 ans ou plus

7 Selon trois catégories, soit : 1) aucun diplôme/diplôme d'études secondaires/diplôme d'études professionnelles, 2) diplôme d'études collégiales, 3) diplôme d'études universitaires.

8 Selon deux catégories, soit ceux pour qui le français est la langue maternelle et ceux pour qui la langue maternelle en est une autre.

2

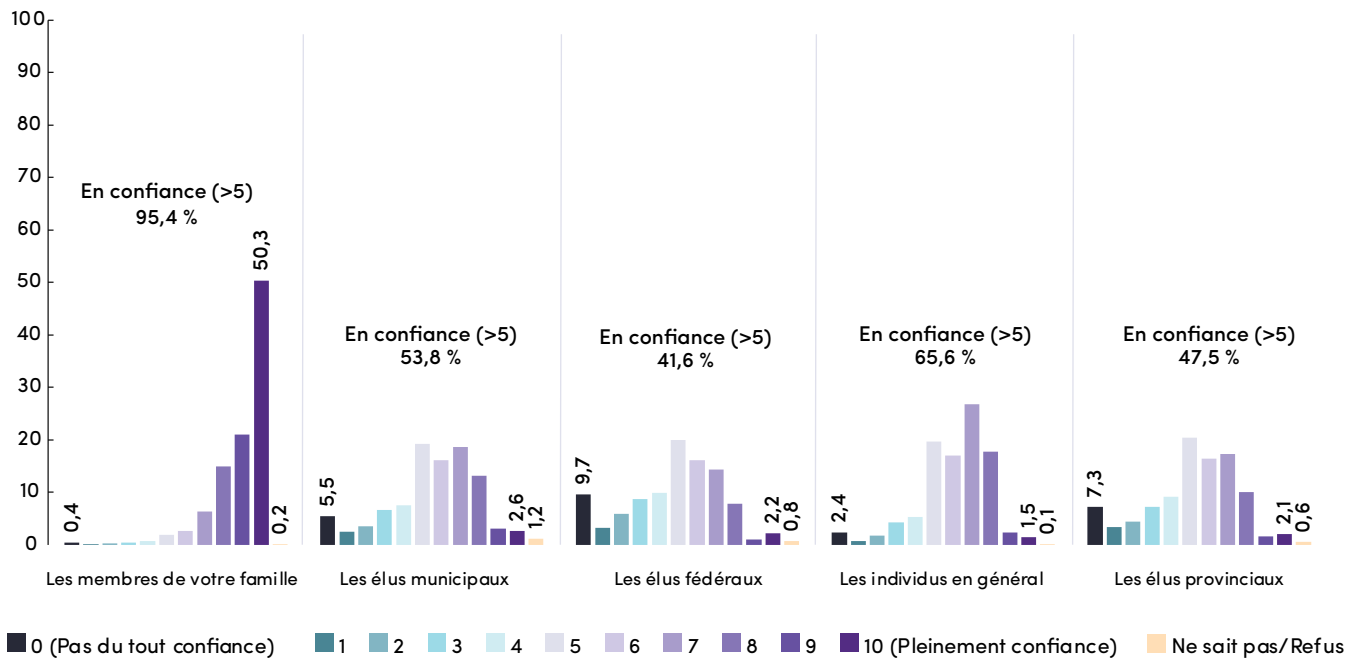
Résultats

Résultats

Niveau de confiance générale selon différentes catégories d'individus

Les répondants ont un niveau de confiance très élevé envers leurs proches et plus tempéré envers les élus à tous les niveaux de gouvernement.

Figure 1
Confiance générale (n=2020)



Les membres de leur famille sont les individus envers lesquels les répondants ont le plus confiance. Plus la proximité est grande, plus la confiance est élevée comme le montre la figure 1. En effet, 50,3 % des répondants ont une confiance totale envers leurs proches (10 sur 10) et plus de 85 % ont une confiance d'au moins 8 sur 10. Les répondants ont moins confiance envers les individus en général, mais un nombre important (65,6 %) affirme tout de même avoir un niveau de confiance de plus de 5. La confiance envers les élus municipaux, provinciaux et fédéraux est plus faible. 53,8 % des répondants ont une confiance de plus de 5 pour les élus municipaux, 41,6 % pour élus fédéraux et 47,5 % pour les élus provinciaux. Alors que le nombre de répondants n'ayant aucune confiance est assez faible lorsqu'il est question des membres de la famille et des individus en général (respectivement 0,4 % et 2,4 %), il atteint 9,7 % pour les élus fédéraux, 7,3 % pour les élus provinciaux et 5,5 % pour les élus municipaux.

Il est intéressant de noter que les niveaux de confiance varient aussi selon les profils sociodémographiques

En ce qui a trait plus précisément à la confiance envers les élus provinciaux, acteurs centraux dans la mise en place de l'identité numérique, il est possible d'identifier certaines variables sociodémographiques déterminantes, comme l'illustre la figure 2. Ainsi, les personnes âgées de 65 et plus, les personnes détenant un niveau de scolarité collégial ou universitaire et celles qui ont le français ou une autre langue comme langue maternelle sont associées à une plus grande probabilité d'être confiant envers les élus provinciaux.

Figure 2

Facteurs associés au fait d'être confiant envers les élus provinciaux

		Margins	p
Âge (réf.: Moins de 25 ans)	25-34 ans	-0,010	0,848
	35-44 ans	-0,022	0,674
	45-54 ans	0,034	0,519
	55-64 ans	0,090	0,087
	65 ans ou plus	0,183	0,001
Genre (réf.: Féminin)	Masculin	0,055	0,016
Niveau de scolarité (réf.: Primaire)	Secondaire ou DEP	0,105	0,076
	Collégiale	0,194	0,001
	Universitaire 1er cycle	0,272	< 0.001
	Universitaire 2e ou 3e cycle	0,302	< 0.001
Langue maternelle (réf.: Anglais)	Français	0,233	< 0.001
	Autres	0,160	0,015
Statut d'immigrant (réf.: Né au Canada)	Immigrant depuis moins de 10 ans	0,113	0,054
	Immigrant depuis 10 ans ou plus	-0,035	0,463
Taille du ménage (réf.: 1 personne)	2 personnes	0,032	0,300
	3 personnes	0,043	0,285
	4 personnes ou plus	0,095	0,010
Région de résidence (réf.: RMR de Québec)	RMR Montréal	0,101	0,007
	Ailleurs au Québec	0,113	0,003

Confiance envers la capacité et la volonté du gouvernement du Québec

On peut décomposer la confiance en deux éléments caractéristiques, soit la perception de la capacité et la perception de la volonté d'un acteur donné. Les résultats montrent un contraste important entre les niveaux de confiance face à ces deux éléments.

Trois affirmations étaient communiquées aux répondants : 1) Le gouvernement du Québec a **tous les outils nécessaires** pour bien gérer l'identité numérique; 2) Le gouvernement du Québec a **la volonté** d'assurer une gestion sécuritaire de l'identité numérique; 3) Le gouvernement du Québec a **la capacité** d'assurer une gestion sécuritaire de l'identité numérique.

Pour la première affirmation, 40,6 % sont soit totalement d'accord (5,7 %) ou plutôt d'accord (34,9 %) avec le fait que le gouvernement a tous les outils nécessaires pour bien gérer l'identité numérique. Ceci laisse une majorité de répondants (51,4 %) en désaccord avec cette affirmation. En ce qui a trait à la seconde affirmation, qui concernait la volonté, les deux tiers des répondants (67,1 %) sont d'accord pour dire que le gouvernement a la volonté d'assurer une gestion sécuritaire. Pour la troisième affirmation, 46,6 % des répondants sont soit totalement en désaccord (12,9 %) ou plutôt en désaccord (33,7 %) avec le fait que le gouvernement a la capacité d'assurer une gestion sécuritaire de l'identité numérique. Il y a 53,4 % des répondants qui croient que le gouvernement a la capacité nécessaire. Ceci montre un contraste significatif entre la perception qu'ont les répondants vis-à-vis de la volonté de bien faire par rapport à la capacité d'y parvenir.

Les réponses à ces trois affirmations peuvent être mises en parallèle avec une autre question qui portait sur le niveau de préparation du gouvernement du Québec par rapport à divers événements potentiels tels qu'une consultation non permise des données, une cyberattaque, l'inaccessibilité des données en raison d'une panne, l'utilisation des données à des fins de surveillance ou encore la fraude et l'hameçonnage. Dans les cinq cas, une proportion assez constante de répondants, soit autour de 60 %, estime que le gouvernement du Québec est peu ou pas du tout outillé pour faire face à ces événements. Très peu de répondants, soit autour de 5 %, considèrent que le gouvernement est très outillé alors qu'entre 28 et 33 % des répondants estiment qu'il était assez outillé. Finalement, les répondants ne semblent pas inquiets de voir le gouvernement utiliser les données à des fins de surveillance. Ceci concorde avec le fait que les répondants croient que le gouvernement a la volonté de bien faire⁹.

Les réponses appellent deux constats. Premièrement, une partie substantielle des répondants estiment que le gouvernement du Québec a la volonté d'assurer une gestion sécuritaire, c'est-à-dire qu'ils ne prêtent pas au gouvernement du Québec de mauvaises intentions ou un certain laxisme. Deuxièmement, une proportion importante des répondants, dépassant quelque peu ou s'approchant de la majorité, ne croit pas que le gouvernement du Québec a la capacité ou les outils nécessaires pour assurer une gestion sécuritaire. De ces deux constats se dégage un troisième : les répondants ne manifestent pas une méfiance intrinsèque envers le gouvernement du Québec en tant qu'institution. Leur scepticisme concerne plutôt l'expertise de celui-ci en matière de cybersécurité. La fiabilité technique du gouvernement du Québec semble ainsi être un déterminant majeur de la confiance que les citoyens accordent à celui-ci, dans le contexte du partage et de la protection de leurs renseignements personnels. Ceci fait écho à des résultats obtenus précédemment lors d'une recherche qui avait été menée auprès des Québécois, via des groupes de discussion, au sujet de la gestion de leurs renseignements personnels et de santé, recherche dans laquelle nous avons fait des constats similaires sur la perception de la capacité et de la volonté (Caron et al., 2025).

Degré d'ouverture face à l'identité numérique

Le degré d'ouverture quant à l'usage de l'identité numérique est assez faible au départ, mais évolue significativement suivant l'information fournie aux répondants sur les bénéfices potentiels et les conditions de mise en œuvre proposées.

Parmi les 2020 répondants, seuls 12,3 % se sont initialement montrés totalement ouverts à l'utilisation de l'identité numérique alors que près du double, soit 23,1 % ont signifié n'être pas du tout ouverts à l'utilisation de celle-ci. La plus grande proportion des répondants (64,7 %) se sont dits ouverts, mais à certaines conditions. La figure 3 résume les résultats des questions portant sur le degré d'ouverture des répondants à l'égard de l'identité numérique. Ces chiffres concordent en partie avec les résultats d'une enquête sur l'acceptabilité sociale du partage des renseignements de santé, dans laquelle le nombre des répondants qui avaient un accord total et sans condition avec le partage des renseignements de santé était lui aussi assez faible (7,1 %) (Caron et al., 2023).

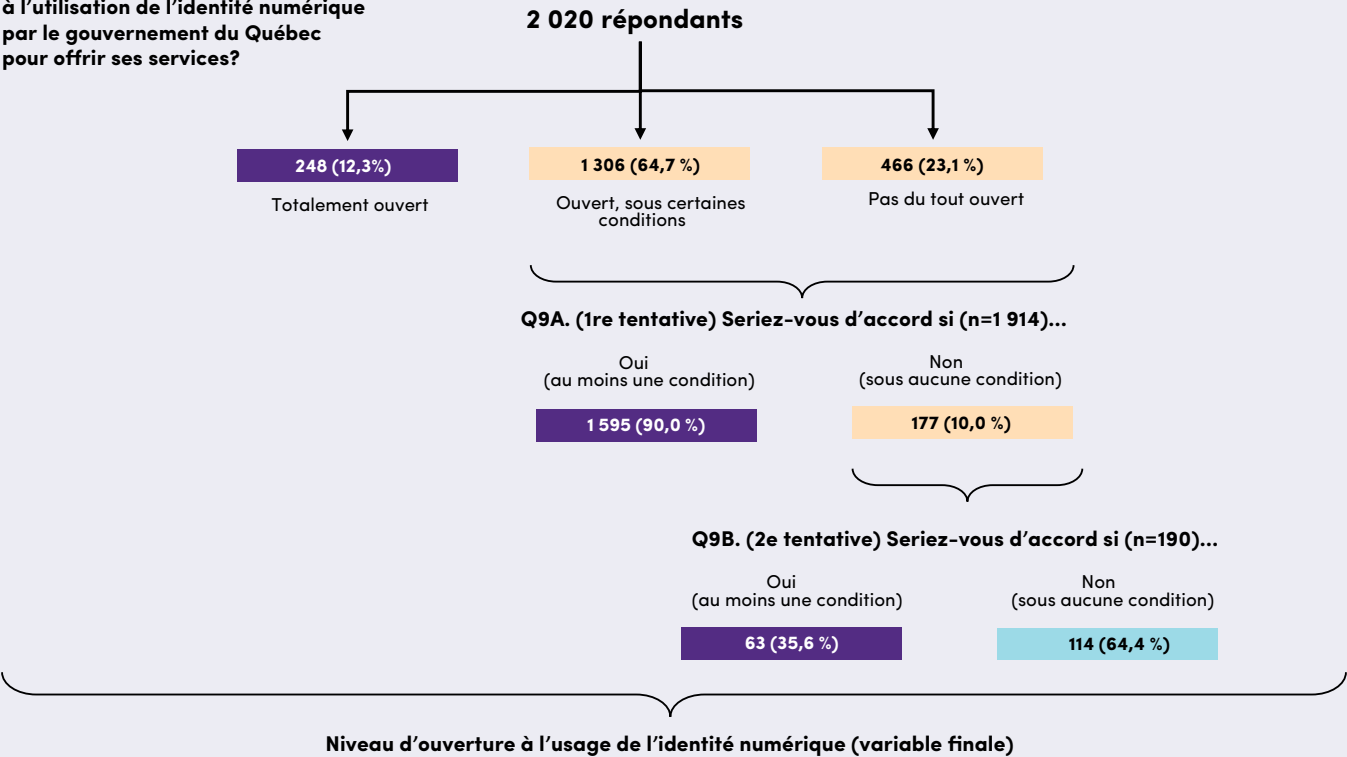
⁹ Il faut toutefois tenir compte de la formulation de la question. En demandant directement aux répondants si la surveillance par le gouvernement est une crainte qu'ils partagent, la réponse serait peut-être différente.

Figure 3

Niveau d'ouverture à l'utilisation de l'identité numérique par le gouvernement du Québec

Q9. (Opinion initiale)

Dans quelle mesure seriez-vous ouverts à l'utilisation de l'identité numérique par le gouvernement du Québec pour offrir ses services?

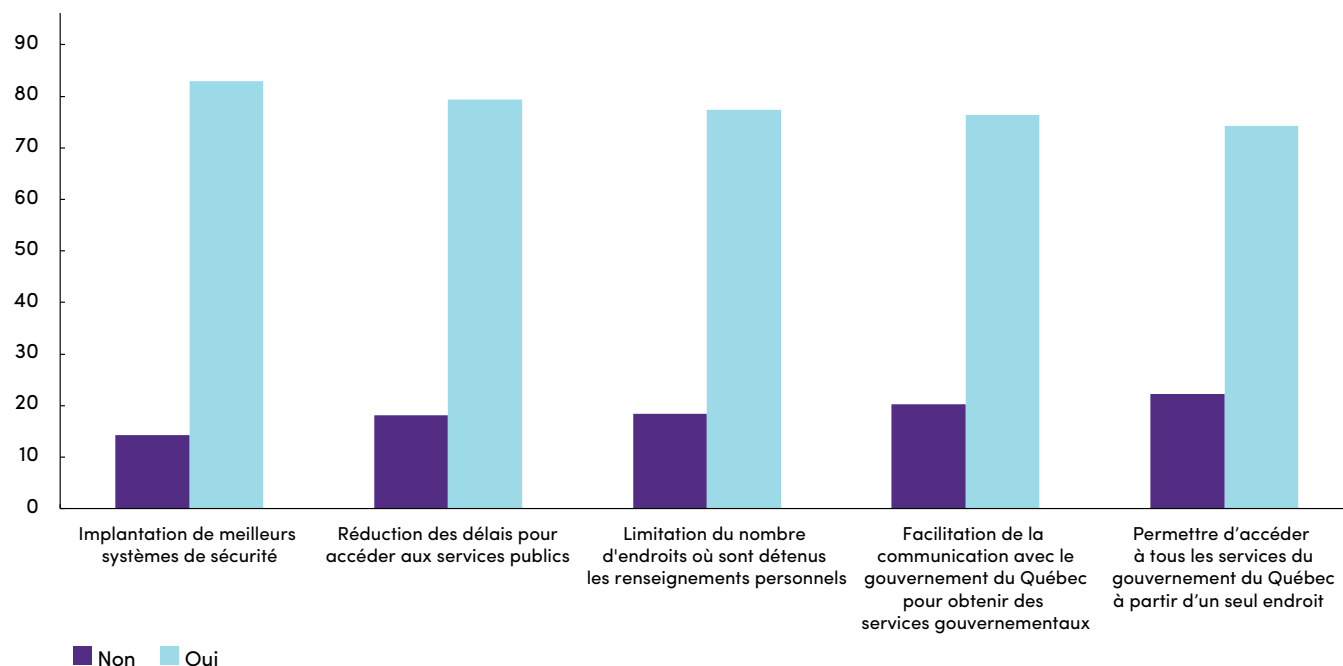


Tout comme pour le partage de leurs renseignements de santé, il est important de considérer que l'ouverture de la majorité des citoyens en matière d'identité numérique dépend du respect de certaines conditions.

Ainsi, après avoir présenté certaines modalités de fonctionnement aux répondants qui se disent « **ouverts sous certaines conditions** », « **pas du tout ouverts** » ou qui **ne savent pas** (1772 répondants sur 2020), 90 % de ces derniers (1595 sur 1772) deviennent favorables pourvu qu'au moins une des modalités suivantes soit respectée. La condition qui a le plus d'impact sur l'adhésion (83 %) est l'implantation de meilleurs systèmes de sécurité comme l'indique la figure 4. Il est intéressant de noter que pour les participants, l'amélioration de la sécurité est plus importante (9 points de pourcentage de plus) que la possibilité d'avoir accès à tous les services gouvernementaux à un seul endroit. D'ailleurs, pour adhérer à l'identité numérique, l'importance accordée par les participants aux facteurs de protection et de partage des renseignements personnels est sensiblement plus grande que celle accordée au facteur lié à l'amélioration de la qualité des services.

Figure 4

Conditions qui favorisent l'ouverture à l'utilisation de l'Identité numérique



Après cette première ronde de conditions, une deuxième série de modalités a été proposée aux 177 répondants qui ne se montraient toujours pas ouverts. Après la présentation de plusieurs nouvelles modalités mettant en avant une protection des renseignements personnels et une sécurité renforcée, une majorité d'entre eux (64,4 %) sont toujours réfractaires. En extrapolant à l'ensemble de la population, cela signifie qu'une partie de cette dernière, soit environ 5,4 %, pourrait demeurer complètement fermée même une fois informée de la présence de plusieurs mesures amenant à renforcer la sécurité et la protection des renseignements personnels ainsi qu'à garantir une meilleure qualité et efficacité des services.

Pour garantir son acceptabilité sociale, l'identité numérique devra idéalement être gérée par le gouvernement lui-même.

Très peu de répondants sont ouverts à utiliser l'identité numérique si elle est gérée par un géant du Web. 38,2 % sont totalement fermés à cette éventualité alors que 80 % ont une ouverture de 5 et moins sur 10. Ces réponses soulignent le peu de confiance que les répondants ont à l'égard des géants du Web. La gestion de l'identité numérique par les institutions financières génère toutefois davantage d'ouverture : 14,7 % des participants sont totalement fermés à une telle gestion et 48,8 % des participants sont ouverts à plus de 6 sur 10. Cette différence entre géants du Web et institutions financières peut s'expliquer de diverses manières, mais on peut faire l'hypothèse que le fait que les institutions financières soient déjà impliquées dans l'authentification pour certains services gouvernementaux, en particulier les services fiscaux, est un élément rassurant.

L'identité numérique devrait d'abord être utilisée pour les services gouvernementaux et avec prudence dans le cas de certains renseignements considérés sensibles.

Les répondants ont été questionnés sur la possibilité d'utiliser l'identité numérique développée par le gouvernement dans leurs transactions avec le secteur privé. Ici, les réponses sont partagées. 45,0 % sont en faveur d'une telle utilisation alors que 42,1 % sont contre.

Ensuite, 61,3 % des répondants ont dit avoir des craintes concernant une liaison de leur identifiant numérique avec leurs renseignements fiscaux, et 53,7 % ont manifesté une crainte quant à la liaison de leur identifiant numérique avec leurs renseignements de santé. Ces résultats mettent en lumière le fait que certains croisements ou échanges de données entre organisations gouvernementales semblent causer des préoccupations pour un nombre important de répondants.

Profils sociodémographiques en fonction du degré d'ouverture

Le profil démographique des individus a une incidence sur le niveau de confiance et l'appréhension quant à l'usage d'une identité numérique

On peut dégager certaines caractéristiques sociodémographiques pour les différents groupes de répondants aux questions sur le degré d'ouverture à l'utilisation de l'identité numérique. À partir de ces caractéristiques démographiques, nous pouvons constituer des profils types et associer ces profils à un niveau d'ouverture spécifique. Ces constatations pourraient informer les décideurs sur les besoins de communication et de sensibilisation avec les diverses parties de la population.

12,3 %

Chez les répondants qui ont dit être totalement ouverts (12,3 %), le profil type regroupe les caractéristiques sociodémographiques suivantes:



Les hommes



Les individus plus scolarisés



Les individus utilisant la technologie au quotidien¹⁰



Les individus faisant confiance aux élus provinciaux



Les individus étant moins inquiets/méfiant vis-à-vis de la technologie en général

¹⁰ Incluant des services en ligne en général, les réseaux sociaux, l'utilisation d'un ordinateur, d'une tablette ou d'un téléphone intelligent.

64,7 %

Chez les individus ouverts, mais sous certaines conditions (64,7 %), il est possible d'identifier une prédominance des caractéristiques sociodémographiques suivantes :



Les femmes



Les individus ayant un niveau de confiance « moyen » envers les élus provinciaux



Les individus qui sont généralement plus inquiets/méfiant vis-à-vis de la technologie en général

5,6 %

Enfin, les individus totalement fermés à l'identité numérique (5,6 %) partagent aussi certaines caractéristiques sociodémographiques :



Les hommes



Les individus ayant une utilisation moins fréquente d'outils technologiques



Les individus ayant un faible niveau de confiance envers les élus provinciaux



Les individus qui sont généralement plus inquiets/méfiant vis-à-vis de la technologie en général

Le profil sociodémographique des différents groupes de répondants selon leur degré d'ouverture à l'identité numérique permet de faire certains constats. Il convient de rappeler que près de 95 % des répondants seraient ouverts à l'utilisation de l'identité numérique si certaines conditions étaient remplies. Il semble que *le niveau d'inquiétude à l'égard de la technologie, le niveau de confiance envers les élus provinciaux et le niveau de scolarité* sont trois variables qui influencent de façon notable ce degré d'ouverture. Pour les trois groupes considérés ci-haut, l'effet de ces trois variables est clairement apparent. Nous devons toutefois souligner que le niveau de scolarité est lui-même déterminant par rapport au niveau d'inquiétude à l'égard de la technologie et par rapport au niveau de confiance envers les élus provinciaux. Ces variables ne sont donc pas totalement indépendantes. Conséquemment, l'efficacité potentielle des initiatives de communication ou des mesures visant à influencer le niveau de confiance sera tributaire de plusieurs facteurs comme les croyances, aprioris, etc., faisant partie du profil social des individus.

3

Conclusion

Conclusion

La présence grandissante des technologies de l'information et de la communication offrant un potentiel d'amélioration des services publics change la dynamique entre les gouvernements et les citoyens. Il ne s'agit plus simplement de faire reposer l'interaction sur la base d'un profil correspondant à certains critères donnant droit à des bénéfices, mais d'exploiter les données personnelles pour améliorer la prestation de services, le fonctionnement de l'appareil gouvernemental et la conception ainsi que l'évaluation des politiques publiques. Cette nouvelle dynamique présente de nombreux avantages potentiels en termes d'efficacité et d'efficacités des services publics, mais elle soulève du même coup de nombreuses questions quant aux besoins réels de partage de données, ainsi qu'au cadre entourant ce partage.

Un élément central de ce questionnement est l'appropriation par les citoyens de ces solutions et leur degré d'ouverture face à ces nouvelles manières de faire. Sans cette volonté d'appropriation des solutions proposées par les citoyens, de même que l'ouverture de ces derniers pour une exploitation accrue de leurs données personnelles, ces solutions pourraient mal fonctionner ou ne pas fonctionner du tout, et la confiance envers les gouvernements pourrait s'effriter. Il est donc important de connaître le degré d'acceptabilité sociale de ces solutions et aussi de comprendre les conditions pour maintenir cette acceptabilité sociale. Il est ici important de rappeler que nos travaux précédents ont démontré qu'il ne semble pas y avoir de compréhension commune autour du concept d'identité numérique (Caron et al., 2025) et cette compréhension jouera un rôle clé dans l'acceptation voire l'appropriation de la solution.

La présente enquête a permis de mettre de l'avant plusieurs éléments dont certains sont déterminants dans la recherche de l'acceptabilité sociale autour de la création et de l'usage de l'identité numérique des citoyens québécois par le gouvernement du Québec.

Premièrement, la confiance envers le gouvernement est essentielle et varie autour de deux principales composantes, soit la perception de la volonté et de la capacité gouvernementales. Si la première est perçue positivement, la seconde pose un problème. En effet, la capacité du gouvernement (au sens technique) est considérée comme déficiente par une majorité de répondants. Ces résultats rejoignent les propos récoltés lors de la conduite de groupes de discussion (Caron et al., 2025). Aussi, il est ressorti que le secteur privé est vu comme étant plus « compétent » techniquement que le secteur public lorsque vient le temps de construire et d'offrir des systèmes fiables et sécuritaires. En revanche, les répondants ont souligné qu'ils ne faisaient pas confiance au secteur privé dans ses motivations à promouvoir l'intérêt public. Cette donnée est très importante et requerra une attention particulière du législateur dans la conception de ses solutions.

Deuxièmement, si la population demeure ouverte face au concept d'identité numérique, elle est plutôt craintive face aux détails de son fonctionnement. De multiples raisons peuvent expliquer ces réserves, mais les conditions que nous avons mesurées, pour rendre plus acceptable l'identité numérique, donnent des indications sur les raisons derrière ces inquiétudes. Ces indications montrent que les citoyens souhaitent de la transparence quant aux mécanismes derrière le fonctionnement de l'identité numérique. De plus, ils souhaitent qu'il y ait des balises autour de sa gestion et ont une préférence pour un système d'identité géré par le public plutôt que par le privé. Parmi les différentes conditions mesurées, le fait d'assurer la sécurité des informations semble être la condition la plus efficace pour « convaincre » les participants. Cette condition surpasse même les bénéfices souhaités et attendus liés à des services plus efficaces.

Troisièmement, dans un but de sensibilisation pour une appropriation étendue à l'ensemble de la population, il est ressorti qu'une attention particulière devrait être portée aux divers profils sociodémographiques des individus. En effet, certaines caractéristiques semblent influencer l'attitude vis-à-vis l'acceptation de l'identité numérique.

De manière plus générale, on a pu constater que la confiance semble s'accroître en fonction de la proximité entre le citoyen et l'entité avec laquelle il est en relation. Ceci nous amène à poser l'hypothèse que dans l'éloignement, la relation de confiance basculerait d'une relation ancrée dans le jugement basé sur la connaissance vers une relation de confiance ancrée dans l'action et la fiabilité (« reliance »). En d'autres mots, si je ne peux m'assurer d'avoir une relation de confiance avec un individu en particulier, j'aimerais être certain que le « système » va fonctionner, qu'il est fiable. Par exemple, il est difficile d'avoir une pleine relation de confiance avec mon constructeur automobile avec lequel j'ai une relation de proximité très éloignée. Cependant, je « sais » que ma voiture est fiable. Sinon, je ne l'utiliserais pas. En corollaire, une telle relation construite autour de la fiabilité plutôt qu'autour de la confiance pourrait-elle avoir un impact négatif, à long terme, sur le fonctionnement démocratique (Hunyadi, 2023), sur sa dimension essentiellement humaine et adaptative aux besoins changeants des citoyens? Si oui, peut-on contrebalancer ce phénomène pour préserver le fonctionnement de nos institutions tout en utilisant des approches comme l'identité numérique?

En définitive, comme dans l'enquête sur le partage des renseignements de santé (Caron et al., 2023), les résultats offrent des pistes de réflexion pour le développement d'instruments de politiques publiques pertinents en appui à l'usage des données personnelles pour l'amélioration des services publics. Plus spécifiquement, les résultats montrent que l'identité numérique, pour être effective, devra être déployée en s'associant de près aux désirs des citoyens et cela, en continu.

Références

- Benedetto-Meyer, M., & Boboc, A. (2021). *Sociologie du numérique au travail*. <https://doi.org/10.3917/arco.bened.2021.01>
- Boudreau, C. (2023, mai). *Étude de cas sur le développement et l'utilisation d'un assistant virtuel au 311 de la Ville de Laval*. <https://espace.ensp.ca/id/eprint/430/>
- Caron, D. J., Lamarche, P.-O., & Nicolini, V. (2025). *La confiance comme levier pour le partage des renseignements personnels et de santé : Perspectives citoyennes*. Observatoire international sur les impacts sociétaux de l'IA et du numérique. <https://doi.org/10.61737/XOZU2116>
- Caron, D. J., Nicolini, V., & Prud'homme, A. (2023). Policy approaches for increasing participation with personal health information and data sharing (HIDS). *Canadian Health Policy*, 2023(3), 1-24.
- Eber, N., & Willinger, M. (2005). *L'économie expérimentale*. La Découverte. <https://doi.org/10.3917/dec.eber.2005.01>
- Hunyadi, M. (2023). *Faire confiance à la confiance*. Érès. <https://doi.org/10.3917/eres.hunya.2023.01>
- Institut de gouvernance numérique. (2019). *Registres distribués, évolution de la chaîne de bloc : Impacts, enjeux et potentiels pour le Québec [livre blanc]*.
- Projet de loi n° 82, Loi concernant l'identité numérique nationale et modifiant d'autres dispositions, 82, 41 1 (2025). <https://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-82-43-1.html>

Annexe 1 : Questionnaire

Étude sur l'implantation d'une identité numérique au Québec

SOM. Étude sur l'implantation d'une identité numérique au Québec

ENAP

*Si Toujours, Run Script:
DATEDEB.SetValue(DATE)*

CHOIXLAN. CHOIXLAN

LANG. (FR) Bienvenue

-- (EN) Welcome

- ☐ 1 Answer in English
- ☐ 2 Répondre en français

*Si ((LANG Au moins une 2)), continuer l'interview en Français (Canada)
Si ((LANG Au moins une 1)), continuer l'interview en Anglais (Canada)*

Questionnaire. Questionnaire

INTRO.

CLESOM : CLESOM

STRATE : STRATE

Bonjour, bonsoir, je m'appelle... de la firme de recherche SOM.

Au besoin : Nous réalisons actuellement une étude sur l'utilisation des données personnelles pour améliorer les services gouvernementaux avec des outils électroniques.

Au besoin : 'Cette étude est importante, car elle va nous permettre de comprendre ce que les Québécois considèrent comme essentiel quant à la sécurité de leurs données personnelles lorsqu'ils/elles accèdent à des sites web gouvernementaux. Les résultats de la recherche vont permettre de réfléchir aux meilleures manières d'offrir une prestation de services aux citoyens en toute sécurité.

NOTE_AV_QCELL. On pose CELL seulement dans les strates fixes, sinon on remplit CELL à 1 automatiquement pour aller à S22.

*Si Toujours, Run Script:
if STRATE.Answers.EntryCode has 136;166;196 Then
QCELL.SkipAndKeepData().SetValue(1)
EndIf*

QCELL. Est-ce que je vous parle sur un cellulaire présentement?

Valider si le répondant semble au volant ou pratique certaines activités : Est-ce sécuritaire de vous parler au téléphone?

Prendre rendez-vous au besoin.

- ☐ 1 *Oui
- ☐ 2 *Non/NSP/NRP

NOTE_AV_S22. On pose S22 seulement si CELL=1, sinon on va faire la sélection aléatoire pour les lignes fixe.

Si ((QCELL Au moins une 1)), Ne poser 'S22' que si

S22. Si évident, ne pas lire la question et inscrire 18 ans ou plus.

En cas de doute, demander : Est-ce que vous êtes âgé de...?

- ☐ 1 *18 ans ou plus
- ☐ 2 *16 ou 17 ans
- ☐ 3 *15 ans ou moins (Remercier et classer comme inéligible)
- ☐ 9 *NSP/NRP (Remercier et classer comme « Refus sur cellulaire »)

NOTE_AP_S22. Si S22=18 ans ou plus on va à DEBUT

Si S22=16 ou 17 ans / 15 ans ou moins on classe inéligible

Si S22=NSP/NRP (Remercier et classer comme « Refus sur cellulaire ») l'intervieweur classe l'appel en refus manuellement.

Si ((S22 Au moins une 1)), ne pas poser 'SELECTION_ALEATOIRE'

Si ((S22 Au moins une 2;3)), Aller à 'AVANTOUT' et marquer en tant qu'incomplet

Si ((S22 Au moins une 4)), lire le message suivant 'Classer en refus sur cellulaire.'

SELECTION_ALEATOIRE. On choisit le plus jeune ou le plus âgé au hasard.

CHOIXRD. CHOIXRD

Si ((QCELL Au moins une 2)), spécifier la valeur 'Dim Rand = Random(2)Return Rand' à la question 'AFFCHOIX'

AFFCHOIX. AFFCHOIX

- ☐ 1 J'aimerais parler à l'adulte le plus âgé chez vous qui est présentement à la maison.
- ☐ 2 J'aimerais parler à l'adulte le plus jeune chez vous qui est présentement à la maison.

Si ((AFFCHOIX Au moins une 1;2)), Ne poser 'CHOIX' que si

CHOIX. Au besoin, si changement d'interlocuteur : Bonjour, bonsoir, je suis... de la firme de recherche SOM.

AFFCHOIX

Au besoin, si la voix semble jeune : Êtes-vous bien âgé de 18 ans ou plus?

DEBUT. Au besoin, si changement d'interlocuteur : Bonjour, bonsoir, je suis... de la firme de recherche SOM.

Nous réalisons actuellement une étude pour le compte de l'École nationale d'administration publique (ÉNAP) sur l'utilisation des données personnelles pour améliorer les services gouvernementaux avec des outils électroniques. Le questionnaire dure environ 10 à 12 minutes et les données recueillies sont confidentielles.

À préciser au besoin : nous ne vous demanderons aucun renseignement personnel, nous voulons simplement connaître votre opinion.

Au besoin et pour tout le questionnaire : Lorsque le répondant hésite, vous pouvez lui mentionner « Il n'y a pas de bonne ou de mauvaise réponse ».

Au besoin : 'Cette étude est importante, car elle va nous permettre de comprendre ce que les Québécois considèrent comme essentiel quant à la sécurité de leurs données personnelles lorsqu'ils/elles accèdent à des sites web gouvernementaux. Les résultats de la recherche vont permettre de réfléchir aux meilleures manières d'offrir une prestation de services aux citoyens en toute sécurité.

NOTE_AV_LoopQ1. Rotation aléatoire des énoncés de la série Q1

Q1. Sur une échelle de 0 à 10, où 0 signifie « pas du tout confiance » et 10 « pleinement confiance », dans quelle mesure faites-vous confiance...

	*0	*1	*2	*3	*4	*5	*6	*7	*8	*9	*10	*Je
	(Pa										(Ple	ne
	s du										ine	sais
	tout										men	pas/
	conf										t	Je
	ianc										conf	préf
	e)										ianc	ère
											e)	ne
												pas
												rép
												ond
												re
aux membres de	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
votre famille												

aux élus municipaux	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
aux élus fédéraux	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
aux individus en général	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
aux élus provinciaux	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Randomiser les réponses

NOTE_AV_LoopQ2. Rotation aléatoire des énoncés de la série 2

Q2. Êtes-vous totalement en désaccord, plutôt en désaccord, plutôt d'accord ou totalement d'accord avec les énoncés suivants?

	*Totalment en désaccord	*Plutôt en désaccord	*Plutôt d'accord	*Totalment d'accord	*Je ne sais pas/Je préfère ne pas répondre
Vous faites confiance au fédéral pour administrer les services à la population	☐	☐	☐	☐	☐
Vous faites confiance au provincial pour administrer les services à la population	☐	☐	☐	☐	☐
Vous faites confiance au municipal pour administrer les services à la population	☐	☐	☐	☐	☐

Randomiser les réponses

NOTE_AV_LoopQ3. Rotation aléatoire des énoncés de la série 3

Q3. Au cours de la dernière année, à quelle fréquence avez-vous utilisé... Diriez-vous...

On peut se laisser interrompre.

Jamais	Quelques fois par mois	Quelques fois par semaine	Chaque jour	*Je ne sais pas/Je
--------	------------------------	---------------------------	-------------	--------------------

					préfère ne pas répondre
un téléphone intelligent	☐	☐	☐	☐	☐
un ordinateur	☐	☐	☐	☐	☐
une tablette électronique	☐	☐	☐	☐	☐
les réseaux sociaux	☐	☐	☐	☐	☐
des services en ligne (ex. : services bancaires, achats en ligne, etc.)	☐	☐	☐	☐	☐

Randomiser les réponses

Q4. De façon générale, avez-vous des craintes face à la sécurité de vos informations en ligne?

- ☐ 1 *Oui
- ☐ 2 *Non
- ☐ 9 *Je ne sais pas

NOTE_AV_LoopQ5. Rotation aléatoire des énoncés de la série 5

Q5. Êtes-vous... inquiet par rapport aux événements suivants?

	Pas du tout (inquiet)	Un peu (inquiet)	Assez (inquiet)	Très (inquiet)	*Je ne sais pas/Je préfère ne pas répondre
La fraude, le vol de données ou l'hameçonnage	☐	☐	☐	☐	☐
L'utilisation des données personnelles à des fins de surveillance par les gouvernements	☐	☐	☐	☐	☐
Que vos données soient rendues inaccessibles à cause de pannes internet	☐	☐	☐	☐	☐
Les cyberattaques	☐	☐	☐	☐	☐
La consultation non permise de vos données, par curiosité par exemple	☐	☐	☐	☐	☐

Randomiser les réponses

NOTE_AV_LoopQ6. Rotation aléatoire des énoncés de la série 6

Q6. Considérez-vous que le gouvernement du Québec est... outillé pour protéger vos données face à...

Pas du Peu Assez Très *Je ne

	tout (outillé)	(outillé)	(outillé)	(outillé)	sais pas/J e préfè re ne pas répondre
La fraude, le vol de données ou l'hameçonnage	☐	☐	☐	☐	☐
L'utilisation des données personnelles à des fins de surveillance par les gouvernements	☐	☐	☐	☐	☐
Que vos données soient rendues inaccessibles à cause de pannes internet	☐	☐	☐	☐	☐
Les cyberattaques	☐	☐	☐	☐	☐
La consultation non permise de vos données, par curiosité par exemple	☐	☐	☐	☐	☐

Randomiser les réponses

Q7. De façon générale, en qui avez-vous le plus confiance pour gérer les risques liés à la sécurité de vos informations en ligne et pour protéger vos données personnelles?

- ☐ 1 Le gouvernement du Québec
- ☐ 2 Le secteur privé comme Meta, Amazon, Google, etc.
- ☐ 9 *Je ne sais pas/J e préfère ne pas répondre

Q8. Voici maintenant une définition de l'identité numérique :

L'identité numérique consiste en une application mobile qui permet à la fois de prouver différents éléments de son identité comme l'âge ou l'adresse et de relier les informations personnelles nécessaires qui sont détenues par le gouvernement afin d'accéder de façon simple et sécuritaire aux services gouvernementaux.

Les technologies utilisées respectent les plus hauts standards de sécurité, lesquelles permettent de se connecter aux prestations électroniques de services gouvernementaux et d'effectuer des démarches en ligne ou en personne.

Q9. Seriez-vous... à l'utilisation de l'identité numérique par le gouvernement du Québec pour offrir ses services?

- ☐ 1 Totalement ouvert
- ☐ 2 Ouvert, mais sous certaines conditions
- ☐ 3 Pas du tout ouvert
- ☐ 9 *Je ne sais pas/J e préfère ne pas répondre

NOTE_AV_9ATXT. Les répondants qui ont des réserves ou qui ne sont pas ouverts (Q9=2, 3 ou 9) poursuivent à 9aTXT; les autres (totalement ouverts, Q9=1) vont à LoopQ9C

Si ((Q9 Au moins une 1)), Run Script:

Q9ATXT.Skip()

LoopQ9A.Skip()

Q9ATXT. À la question précédente, vous avez indiqué ne pas être ouvert ou avoir certaines réserves concernant l'utilisation d'une identité numérique.

Considérant que les recherches montrent que l'usage de l'identité numérique peut permettre d'obtenir plusieurs bénéfices dans vos interactions avec le gouvernement...

NOTE_AV_LoopQ9A. Rotation aléatoire des énoncés de la série 9aRotation aléatoire des énoncés de la série 9a

Q9A. Seriez-vous favorable à l'utilisation de l'identité numérique...

	*Oui	*Non	*Je ne sais pas/Je préfère ne pas répondre
Si elle permettait de réduire les délais pour accéder aux services publics?	☐	☐	☐
Si le nombre d'endroits où sont détenus vos renseignements d'identification était limité?	☐	☐	☐
Si de meilleurs systèmes de sécurité étaient implantés? (Services numériques gouvernementaux plus sécuritaires, ex. protection contre la fraude et le vol)	☐	☐	☐
Si cela facilitait la communication avec le gouvernement du Québec pour obtenir des services gouvernementaux?	☐	☐	☐
Si cela permettrait d'accéder à tous les services du gouvernement du Québec à partir d'un seul endroit?	☐	☐	☐
Randomiser les réponses			

NOTE_AV_9BTXT. Si le répondant a indiqué « non » (2) à tous les énoncés de la série 9a1 à 9a5, il continue à Q9bTXT; sinon, il va à Q9c

*Si (Q9A.Iteration(1).Answers.EntryCode Has 1;9 orQ9A.Iteration(2).Answers.EntryCode Has 1;9 orQ9A.Iteration(3).Answers.EntryCode Has 1;9 orQ9A.Iteration(4).Answers.EntryCode Has 1;9 orQ9A.Iteration(5).Answers.EntryCode Has 1;9 orQ9A.Iteration(6).Answers.EntryCode Has 1;9 orQ9A.Iteration(7).Answers.EntryCode Has 1;9) orQ9A.Answers.EntryCode Has 1, Run Script: Q9BTXT.Skip()
LoopQ9B.Skip()*

Q9BTXT. À la question précédente, vous avez indiqué être en désaccord avec l'utilisation de l'identité numérique malgré certaines conditions.

Considérant que les recherches montrent que les mesures suivantes peuvent diminuer les risques lors de l'usage de l'identité numérique...

NOTE_AV_LoopQ9B. Rotation aléatoire des énoncés de la série 9b

Q9B. Seriez-vous favorable à l'utilisation de l'identité numérique...

	*Oui	*Non	*Je ne sais pas/Je préfère ne pas répondre
Si seules les données essentielles étaient collectées?	☐	☐	☐
Si les données devenues inutiles étaient systématiquement détruites?	☐	☐	☐
Si des mesures efficaces connues de gestion de risques étaient mises en place?	☐	☐	☐
Si les systèmes sécuritaires les plus sophistiqués étaient toujours ceux utilisés?	☐	☐	☐
Si des peines sévères étaient mises en place pour les utilisateurs malveillants?	☐	☐	☐
S'il existait des assurances pour couvrir les dommages à la suite d'une perte ou d'un vol de données?	☐	☐	☐
Si les pratiques du gouvernement provincial en matière d'identité numérique étaient supervisées par un organisme indépendant?	☐	☐	☐
<i>Randomiser les réponses</i>			

NOTE_AV_LoopQ9C. Questions 9c1 à 9c3 posées à tous les répondants

Q9C. Êtes-vous totalement en désaccord, plutôt en désaccord, plutôt d'accord ou totalement d'accord avec les énoncés suivants?

	*Totalement en désaccord	*Plutôt en désaccord	*Plutôt d'accord	*Totalement d'accord	*Je ne sais pas/Je préfère ne pas répondre
Le gouvernement du Québec a tous les outils nécessaires pour bien gérer l'identité numérique	☐	☐	☐	☐	☐
Le gouvernement du Québec a la volonté	☐	☐	☐	☐	☐

d'assurer une gestion sécuritaire de
l'identité numérique
Le gouvernement du
Québec a la capacité
d'assurer une gestion sécuritaire de
l'identité numérique

☐☐☐☐☐

NOTE_AV_Q9D. La question 9d est posée aux répondants totalement ouverts (Q9=1) ET qui sont en désaccord avec les énoncés 9c1 OU 9c2 ou 9c3 (1,2); sinon 9e1

Si (Q9 Has 1) and (Q9C.iteration(1) has 1;2 or Q9C.iteration(2) has 1;2 or Q9C.iteration(3) has 1;2), Ne poser 'Q9D' que si

Q9D. Qu'est-ce qui pourrait améliorer votre perception de la capacité du gouvernement à gérer vos données?

Q9E1. Sur une échelle de 0 à 10, où 0 signifie « pas du tout ouvert » et 10 « totalement ouvert », dans quelle mesure seriez-vous ouvert à l'implantation de l'identité numérique si elle était gérée par une institution financière pour le compte du gouvernement provincial?

- ☐ 0 *0 (Pas du tout ouvert)
- ☐ 1 *1
- ☐ 2 *2
- ☐ 3 *3
- ☐ 4 *4
- ☐ 5 *5
- ☐ 6 *6
- ☐ 7 *7
- ☐ 8 *8
- ☐ 9 *9
- ☐ 10 *10 (Totalement ouvert)
- ☐ 99 *Je ne sais pas/Je préfère ne pas répondre

Q9E2. Sur une échelle de 0 à 10, où 0 signifie « pas du tout ouvert » et 10 « totalement ouvert », dans quelle mesure seriez-vous ouvert à l'implantation de l'identité numérique si elle était gérée par un géant du web comme Google, Amazon ou Apple pour le compte du gouvernement provincial?

- ☐ 0 *0 (Pas du tout ouvert)
- ☐ 1 *1
- ☐ 2 *2
- ☐ 3 *3
- ☐ 4 *4
- ☐ 5 *5
- ☐ 6 *6
- ☐ 7 *7

- ☐ 8 *8
- ☐ 9 *9
- ☐ 10 *10 (Totalement ouvert)
- ☐ 99 *Je ne sais pas/Je préfère ne pas répondre

Q9F. Seriez-vous prêt(e) à utiliser l'identité numérique développée par le gouvernement provincial pour vos transactions avec le secteur privé?

(Ex. : transactions bancaires, télécommunication, achats en ligne, santé au privé)

- ☐ 1 *Oui
- ☐ 2 *Non
- ☐ 9 *Je ne sais pas/Je préfère ne pas répondre

Q10. Avez-vous des craintes que votre identifiant numérique soit lié à...

	*Oui	*Non	* Je ne sais pas/Je préfère ne pas répondre
Vos renseignements fiscaux?	☐	☐	☐
Vos renseignements de santé?	☐	☐	☐

SD. SD

AGEGRP2. Nous terminons avec quelques questions pour classification, mais avant, je tiens à vous remercier du temps que vous m'avez consacré jusqu'à maintenant, votre collaboration est grandement appréciée.

À quel groupe d'âge appartenez-vous?

On peut accepter une réponse spontanée.

- ☐ 1 18-24 ans
- ☐ 2 25-34 ans
- ☐ 3 35-44 ans
- ☐ 4 45-54 ans
- ☐ 5 55-64 ans
- ☐ 6 65-74 ans
- ☐ 7 75-84 ans
- ☐ 8 85 ans ou plus
- ☐ 9 *Je ne sais pas/Je préfère ne pas répondre

GENRE. À quel genre vous identifiez-vous?

Par genre, on entend le genre actuel, qui peut différer du sexe assigné à la naissance ou de celui inscrit dans les documents légaux.

- ☐ 1 Masculin
- ☐ 2 Féminin
- ☐ 3 Autre

SE5. Quel est le plus haut diplôme, certificat ou grade que vous possédez ou avez terminé?

Lire au besoin

- ☐ 1 Aucun
- ☐ 2 Certificat d'études secondaires ou l'équivalent (D.E.S., diplôme d'études secondaires)
- ☐ 3 Certificat ou diplôme d'une école de métiers (D.E.P., diplôme d'études professionnelles)
- ☐ 4 Certificat ou diplôme collégial (autre certificat ou diplôme non universitaire obtenu d'un cégep, collège communautaire, institut technique, etc.)
- ☐ 5 Certificat ou diplôme universitaire inférieur au baccalauréat
- ☐ 6 Baccalauréat (ex. : B.A., B.Sc., LL.B.)
- ☐ 7 Certificat ou diplôme universitaire supérieur au baccalauréat
- ☐ 8 Maîtrise (ex. : M.A., M.Sc., M.Ed.)
- ☐ 9 Diplôme en médecine, en médecine dentaire, en médecine vétérinaire ou en optométrie (M.D., D.D.S., D.M.D., D.M.V., O.D.)
- ☐ 10 Doctorat acquis (ex. : Ph.D., D.Sc., D.Ed.)
- ☐ 90 Autre (Veuillez préciser dans l'espace ci-dessous)
- ☐ 99 Je préfère ne pas répondre

LANG1. Quelle est la langue que vous avez apprise en premier lieu à la maison dans votre enfance et que vous comprenez encore?

Plusieurs choix possibles

(3 réponses maximum)

- ☐ 1 *Anglais
- ☐ 2 *Français
- ☐ 3 *Autre

STATS. Quel est votre statut parmi les suivants? Êtes-vous...

- ☐ 1 Né(e) au Canada
- ☐ 2 Immigrant(e) récent(e) (moins de 10 ans)
- ☐ 3 Immigrant(e) de longue date (10 ans et plus)
- ☐ 90 Autre (veuillez préciser ci-dessous)
- ☐ 99 *Je préfère ne pas répondre

SE6. Au total, combien de personnes habitent chez vous en vous incluant et en incluant aussi les enfants qui habitent chez vous, que ce soit en permanence ou de temps en temps (ex. : en garde partagée).

- ☐ 1 *1
- ☐ 2 *2
- ☐ 3 *3
- ☐ 4 *4
- ☐ 5 *5 ou plus
- ☐ 9 *Je préfère ne pas répondre

EXTCP. Quels sont les 3 premiers caractères du code postal de votre résidence principale?

Si Dim reponseCp = EXTCP.Value.Trim() Dim re3 = "(?i)(^[ABCEGHJ-NPRSTVXY][ABCEGHJ-NPRSTV-Z])" Dim re6 = "(?i)(^[ABCEGHJ-NPRSTVXY][ABCEGHJ-NPRSTV-Z][-]?[ABCEGHJ-NPRSTV-Z])" Dim rta = reponseCp.Left(3) Dim final3 = reponseCp.Right(3) If (reponseCp.IsMatch(re6) Or (rta.IsMatch(re3)) Or (EXTCP.HasNoData)) Then Return False Else Return True EndIf, lire le message suivant 'Le code postal n'est pas dans un format valide / The postal code is not in a valid format.'

FINTEL. Merci de votre collaboration!

Note à l'intervieweur : La prochaine page permet de modifier les ouvertes, vous pouvez raccrocher.

Si mode=1, Ne poser 'FINTEL' que si

MODOUVTEL. MODIFICATION DES OUVERTES

```
!! Dim arrQuestions = Survey.Questions.FilterByTag("OpenSummary")
Dim str = ""
Dim i
For i = 1 To arrQuestions.Count
    If arrQuestions[i].HasNoData = False Then
        str = str + "" + arrQuestions[i].shortcut + " - " + arrQuestions[i].shortcaption + "" +
arrQuestions[i].InputValue() + ""
    EndIf
Next
return str !!
```

Si ((Q4 Au moins une 1;2;3)), ne pas poser 'AVANTOUT'

AVANTOUT. Merci de votre intérêt! Votre profil ne correspond pas à celui recherché pour l'étude.

The Obvia logo consists of the word "obvia" in a lowercase, sans-serif font. The letter "o" is stylized with a small white dot above it. The logo is positioned in the bottom left corner of the page, which has a solid purple background. A large, light purple circular shape is partially visible on the left side of the page, overlapping the logo.

obvia

obvia.ca