La confiance comme levier pour le partage des renseignements personnels et de santé : perspectives citoyennes

Daniel J. Caron
Pierre-Olivier Lamarche
Vincent Nicolini

obvia

Chaire de recherche en exploitation des ressources informationnelles

Mars 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 de 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).

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

Fonds de recherche Québec

ISBN: 978-2-925138-77-8

Pour citer ce document : Caron, D.J., Lamarche, P.-O. et Nicolini, V. (2025). *La confiance comme levier pour le partage des renseignements personnels et de santé : perspectives citoyennes.* Obvia. https://doi.org/10.61737/XOZU2116

Table des matières

Sommaire exécutif

Ce rapport expose les conclusions issues de groupes de discussion portant sur la notion de confiance liée au partage d'informations personnelles et médicales avec les organismes publics. L'étude a exploré cette confiance sous un angle général, mais également de façon plus précise, en examinant deux projets de transformation numérique gouvernementale : le Dossier de santé numérique (DSN) et le Service québécois d'identité numérique (SQIN). Les groupes de discussion ont été réalisés auprès de citoyens québécois et le rapport qui suit présente les différentes constatations qui peuvent être tirées des propos récoltés.

Les résultats indiquent d'abord que les initiatives de transitions numériques gouvernementales interrogées (DSN et SQIN) sont assez peu connues des participants. Nous avons pu constater aussi que les participants étaient confiants quant à la volonté du gouvernement de bien gérer les données des citoyens. Cependant, ils étaient moins ou peu confiants quant à la capacité du gouvernement à bien gérer ces données.

Ces groupes de discussion nous ont permis de dégager certains leviers qui pourraient renforcer la confiance dans le contexte de projets gouvernementaux de transition numérique. D'abord, il est clair que les citoyens demandent davantage de transparence autour de ces projets. Il est aussi primordial que le gouvernement se donne la capacité de mener à bien ces projets en faisant les investissements nécessaires. De plus, il faut convaincre et rassurer les citoyens que les moyens et l'expertise nécessaire sont mis en œuvre pour garantir non seulement que ces projets soient menés à bien, mais aussi plus généralement, que leurs renseignements soient bien gérés et protégés.

Introduction

Les gouvernements sont de plus en plus appelés à considérer le point de vue des citoyens lors du déploiement de projets qui touchent divers secteurs de la société comme l'environnement (ministère de l'Environnement, de la Lutte contre les changements climatiques, de la Faune et des Parcs, 2025), le développement économique (gouvernement du Québec, 2020) ou encore les questions liées aux usages de technologies comme l'intelligence artificielle (Conseil de l'innovation du Québec, 2023). Un des éléments clés qui permet de rendre possibles ces projets est le partage d'informations et de données. Dans l'univers numérique, cet usage élargi d'informations et de données personnelles soulève plusieurs questions quant aux pratiques qui entourent l'utilisation et la protection de ces informations. Les défis relevant de la cybersécurité, de la protection des données, ainsi que du consentement des citoyens quant à ces usages peuvent ralentir, voire entraver l'acceptabilité sociale de ces projets et possiblement priver le gouvernement et les citoyens des bénéfices potentiels liés à de telles initiatives (Ghafur et al., 2020). Entre autres, les études montrent que l'acceptabilité sociale est importante pour obtenir l'aval des populations lors du partage de leurs renseignements de santé (Caron, Bernardi, et al., 2020). De plus, les recherches montrent que l'acceptabilité sociale, au-delà de l'instrumentation traditionnelle comme le consentement ou la réglementation, est facilitée par l'existence d'une relation de confiance entre l'État et les citoyens (Maiorana et al., 2012; Platt et al., 2018). Cette confiance n'est pas donnée et est le résultat d'un apprentissage; la générer requiert des efforts et du temps (Luhmann, 2017).

L'intérêt pour la notion de confiance abordée sous l'angle du partage de l'information, et plus spécifiquement du partage de données sensibles liées à la santé, est assez récent. Historiquement, la confiance était davantage liée et mesurée, en rapport aux institutions et à l'appareil politique en général. Les nouvelles responsabilités que crée la manipulation croissante de données personnelles dans un univers fluide et immatériel soulèvent de nouveaux enjeux. Plus précisément, la loi 5 ou *Loi sur les renseignements de santé et de services sociaux* instaure un nouveau cadre juridique pour la gestion des renseignements de santé et des services sociaux, en permettant d'ouvrir encore plus largement le partage des renseignements de santé à plusieurs fins, dont celles de la performance du système de santé, de la qualité de l'expérience usager et de la recherche.

Pour que la loi soit effective et donne les résultats attendus, il est donc important que les citoyens se sentent en confiance quant au partage de leurs renseignements personnels et de santé. La présente recherche a pour but d'enrichir une réflexion déjà amorcée lors d'une étude en économie expérimentale menée en 2020-2021. Le but de la présente recherche est d'approfondir certains aspects liés à l'acceptabilité sociale du partage des renseignements personnels et de santé ainsi que les principaux leviers pour améliorer la confiance des citoyens dans le contexte du partage de leurs renseignements.

Contexte

Le partage des renseignements personnels se trouve à la base de nombreuses initiatives de transformation numérique comme le Dossier de santé numérique (DSN) ou le Service québécois d'identité numérique (SQIN). La Chaire de recherche en exploitation des ressources informationnelles (CRERI) avait mené en 2020-2021 une étude portant sur l'acceptabilité sociale du partage des renseignements de santé (Caron et al., 2023; Caron, Montmarquette, et al., 2020). Fondée sur une approche d'économie expérimentale à travers un sondage auprès de 2016 Québécois, l'étude avait identifié plusieurs facteurs influençant l'acceptabilité sociale du partage des renseignements de santé. Surtout, l'étude avait montré que les citoyens étaient prêts à changer d'avis et à s'ouvrir davantage au partage de leurs renseignements de santé si certaines conditions étaient remplies. L'enquête avait aussi permis de révéler des conditions qui étaient susceptibles de favoriser cette acceptabilité.

Plus précisément, les résultats de l'étude montraient qu'une très grande majorité des sondés (97,8 %) qui avaient au départ des réserves sur le partage de leurs renseignements de santé étaient prêts à changer de position lorsqu'on leur mentionnait les bénéfices associés au partage des renseignements de santé, ainsi que les conditions qui devaient être respectées dans le contexte de ce partage (ex. : amélioration de la sécurité des données). La principale conclusion tirée de ces résultats est qu'une meilleure communication des bénéfices liés au partage des renseignements de santé, couplée à une plus grande transparence liée aux pratiques informationnelles dans les organisations publiques, aurait un effet positif sur l'acceptabilité sociale du partage des renseignements de santé.

Les résultats de l'étude ont aussi mis en exergue l'importance de la confiance des citoyens envers l'État et l'administration publique comme déterminant de l'acceptabilité sociale. De plus, elle a permis de constater que la confiance envers le ministère de la Santé et des Services sociaux (MSSS) était faible ou moyenne pour trois quarts des répondants[1].

La confiance, les bénéfices potentiels liés au partage et les conditions qui encadrent le partage constituent des enjeux pour l'acceptabilité sociale. Ils ont un impact sur l'engagement des citoyens à s'ouvrir au partage de leurs renseignements de santé.

Pour aller plus loin, la présente recherche vise à obtenir davantage de précisions quant à la signification de ces enjeux en examinant plus à fond les déterminants de la confiance envers le gouvernement et les organisations publiques dans le cadre du partage des renseignements de santé. Ces résultats pourraient permettre de mieux informer et outiller les décideurs quant aux pratiques à explorer et à mettre en œuvre pour favoriser le partage d'informations personnelles et son acceptabilité sociale, et ainsi pouvoir bénéficier des retombées administratives et cliniques de ce partage.

Pour ce faire, des groupes de discussion ont été menés auprès d'un échantillon de la population québécoise avec pour principal objectif d'approfondir certaines dimensions de la confiance envers le gouvernement. Ensuite, à partir d'exemples concrets comme le DSN ou le SQIN, les groupes de discussion visaient à jauger le niveau de connaissance de la population ainsi que sa compréhension des enjeux et des retombées potentielles associés à la mise en place de telles initiatives. Enfin, l'exercice visait également à préciser comment les citoyens perçoivent ou conçoivent l'idée de « confiance ».

Cette recherche s'inscrit dans une volonté de prolonger dans un ancrage empirique des notions habituellement discutées à un niveau plus philosophique. La confiance est trop souvent peu définie et mal opérationnalisée. Cette recherche souhaite contribuer à rendre la notion de confiance plus agissante afin d'appuyer les initiatives qui en dépendent.

1 Selon un indice composite portant sur trois questions : 1) les renseignements de santé des Québécois sont bien protégés contre le vol des données; 2) le ministère de la Santé et des Services sociaux gère bien vos renseignements de santé et 3) le ministère de la Santé et des Services sociaux vous dit la vérité quant au partage des renseignements de santé.

1
Approche et méthodologie

Approche et méthodologie

L'animation des groupes était basée sur un guide de discussion semi-dirigé[2], rédigé par l'équipe de recherche en collaboration avec la firme SOM[3]. La première partie du guide concernait la notion de confiance en général ainsi que la confiance spécifiquement liée à la gestion des renseignements personnels par le gouvernement. Une activité brise-glace invitait les participants à définir la confiance, dans leurs propres mots. Ceux-ci étaient aussi invités à donner une note de 1 à 10 pour illustrer leur niveau de confiance envers le gouvernement du Québec au sujet de 1) la gestion de leurs données personnelles en général, et de 2) la gestion de leurs renseignements de santé. Par la suite, les participants ont discuté de leur sentiment par rapport à la protection de leurs données personnelles et de leurs renseignements de santé, dans le contexte des services gouvernementaux en ligne. Finalement, les participants ont été amenés à identifier les principaux risques qu'ils percevaient en lien avec le partage de leurs données personnelles et de leurs renseignements de santé.

La seconde partie de la discussion visait à interroger les participants par rapport à l'instauration du DSN. À main levée, les participants devaient d'abord indiquer s'ils avaient déjà entendu parler du DSN. Ensuite, un bref énoncé explicatif présentant le fonctionnement et les bénéfices attendus du DSN était lu par l'animatrice. On demandait ensuite aux participants s'ils croyaient que le gouvernement était fiable (capable et motivé) pour assurer la gestion des risques associés au partage des renseignements de santé, dans le contexte du DSN. Enfin, les participants devaient énoncer des mesures qui pourraient être mises en place pour améliorer ou maintenir leur sentiment de confiance lors de la mise en place du DSN.

La troisième partie de la discussion portait sur l'identité numérique. D'abord, toujours à main levée, les participants devaient indiquer s'ils avaient déjà entendu parler de l'identité numérique et étaient invités à dire comment ils se sentaient par rapport à ce concept (positifs, négatifs, neutres). Par la suite, l'animatrice a lu un énoncé expliquant l'identité numérique telle qu'elle serait éventuellement utilisée par le Gouvernement du Québec, en présentant son fonctionnement et les avantages qui lui sont habituellement associés. Les participants étant mieux informés sur le sujet devaient maintenant, encore à main levée, signaler leur ouverture à utiliser cette identité numérique pour interagir avec le gouvernement, et discuter des appréhensions qu'ils pouvaient avoir à ce sujet. Par la suite, on demandait aux participants s'ils croyaient que le gouvernement serait fiable (capable et motivé) pour assurer la gestion des risques associés à l'identité numérique. Finalement, l'animatrice leur demandait s'ils seraient également ouverts à utiliser un système d'identification numérique pour partager leurs renseignements personnels avec le gouvernement fédéral.

Recrutement et caractéristiques des participants

Les participants ont été recrutés à partir du panel Or de SOM. Les participants potentiels ont reçu par courriel une brève explication du projet ainsi qu'une invitation à remplir en ligne le questionnaire de recrutement. La population visée était des adultes de 18 ans et plus en mesure de se présenter physiquement aux bureaux de SOM ou de participer en ligne aux groupes de discussion.

La sélection des participants visait à rassembler des personnes avec des profils divers en termes d'âge, de genre et de niveau de scolarité. En effet, le niveau d'éducation, l'âge, ainsi que le genre ont été identifiés comme pouvant influencer la confiance envers le gouvernement et l'administration publique, dans une variété de contextes (Camoes & Mendes, 2019; Falcone et al., 2020; Foster & Frieden, 2017; Mesa, 2023). Voulant nous assurer de récolter les points de vue de participants qui peuvent ne pas avoir les mêmes expériences et conceptions des enjeux étudiés en raison de leur réalité géographique, nous avons constitué des groupes de discussion avec des représentants des régions suivantes : deux groupes pour la région de Québec, deux groupes pour la région de Montréal, deux groupes pour l'est du Québec[4], et deux groupes pour l'ouest du Québec[5]. Le tableau 1 présente les caractéristiques des groupes et permet de faire le portrait démographique des participants. Dans certains cas, des participants n'étaient pas en mesure de se connecter, ou se sont désistés à la dernière minute. Cela dit, le minimum visé de 6 participants a été atteint pour chacun des 8 groupes et au total, 58 personnes ont participé.

2 Le guide complet est disponible en annexe.
3 SOM est une firme de recherche québécoise spécialisée dans la collecte, l'analyse et la visualisation des données (https://www.som.ca/a-propos).
4 Incluant les régions suivantes : Bas-St-Laurent, Saguenay–Lac-Saint-Jean, Estrie, Côte-Nord, Gaspésie-Îles-de-la-Madeleine, Centre-du-Québec et Chaudière-Appalaches (ceux qui ne sont pas dans la RMR de Québec).
5 Incluant les régions suivantes : Mauricie, Outaouais, Abitibi-Témiscamingue, Nord-du-Québec, Lanaudière, Laurentides et Montérégie (pour ces trois dernières régions, nous avons inclus seulement ceux qui ne sont pas dans la RMR de Montréal).

Les participants retenus ont, par la suite, été contactés par téléphone pour confirmer leur participation et planifier la tenue des groupes de discussion. Un nombre de 6 à 8 participants était visé pour chaque groupe, afin de pouvoir recueillir des points de vue variés, sans pour autant avoir trop de participants. Le but était de garantir que chacun ait le temps de s'exprimer correctement.

Compensation et considérations éthiques

Un montant de compensation de 100 $ a été remis à chacun des participants. 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 2023 – 27.

Collecte des données

La moitié des groupes de discussion a été rencontrée en présentiel, dans les bureaux de SOM, et l'autre moitié via la plateforme ZOOM. Dans chacun des cas, deux groupes étaient consultés l'un à la suite de l'autre à 17h30 et à 19h30, pour la région concernée. Les groupes pour l'ouest du Québec (ZOOM) l'ont été le 7 février 2024; le 8 février pour Québec (bureaux de SOM à Québec); le 15 février pour l'est du Québec (ZOOM); le 19 février pour Montréal (bureaux de SOM à Montréal). Les groupes étaient dirigés par une animatrice de SOM, et un observateur du groupe de recherche était présent pour observer, soit en ligne pour les groupes sur ZOOM ou derrière un miroir double pour les groupes en présentiel. Chacune des séances a été enregistrée (audio et vidéo) pour pouvoir être analysée par la suite. En moyenne, les rencontres des groupes de discussion ont duré 1 heure et 45 minutes.

Analyse des données

L'analyse des données s'est effectuée de manière collaborative entre les analystes de SOM et l'équipe de recherche. Du côté de SOM, un rapport a été produit lorsque toutes les rencontres des groupes avaient été conduites. Ce rapport a pu être réalisé grâce à une prise de notes détaillées ainsi que la production d'un verbatim effectuée par un employé de SOM lors du visionnement de tous les groupes. Une analyse par thème a été effectuée à partir de ces notes, appuyant les constatations par des citations provenant des verbatims lorsque c'était pertinent. Finalement, une experte en méthodologie de SOM a lu et validé le rapport. Les statistiques descriptives concernant les caractéristiques démographiques des participants étaient aussi incluses dans ce rapport fourni par SOM.

Pour faciliter les analyses propres à l'équipe de recherche (ENAP), lors de la réécoute des enregistrements, une grille d'analyse a été construite pour aider à collecter les propos des participants. Cette grille avait pour but d'identifier les faits saillants et les éléments qui revenaient le plus dans les groupes en fonction des différentes parties du guide d'entretien. Il faut noter ici que la démarche ne s'inscrivait pas dans un désir de faire une analyse qualitative « systématique », mais de dégager les grandes lignes des propos des participants et d'orienter les recherches futures sur le sujet. C'est pour cette raison qu'une méthode exploratoire à l'aide de ces grilles d'analyse a été préférée à une analyse par codage systématique à partir d'un logiciel d'analyse qualitative.

Par la suite, les éléments pertinents ont été dégagés à partir du rapport de SOM et des grilles d'analyses. Ces éléments sont présentés dans la section des résultats qui suit.

Tableau 1

Profil des participants

	Groupe 1	Groupe 2	Groupe 3	Groupe 4	Groupe 5	Groupe 6	Groupe 7	Groupe 8	Total
	ZOOM (n=7)	ZOOM (n=7)	SOM Québec (n=8)	SOM Québec (n=8)	ZOOM (n=6)	ZOOM (n=6)	SOM Montréal (n=8)	SOM Montréal (n=8)	(n=58)
Région									
Abitibi-Témiscamingue	1	1	–	–	–	–	–	–	2
Bas-Saint-Laurent	–	–	–	–	–	1	–	–	1
Capitale-Nationale	–	–	8	5	–	–	–	–	13
Centre-du-Québec	–	–	–	–	2	1	–	–	3
Chaudière-Appalaches	–	–	–	3	–	2	–	–	5
Côte-Nord	–	–	–	–	–	1	–	–	1
Estrie	–	–	–	–	–	1	–	–	1
Gaspésie-Iles-de-la Madeleine	–	–	–	–	2	–	–	–	2
Lanaudière	2	1	–	–	–	–	1	1	4
Laurentides	–	1	–	–	–	–			1
Laval	–	–	–	–	–	–	2	1	3
Mauricie	2	2	–	–	–	–			4
Montérégie	–	1	–	–	–	–	3	1	5
Montréal	–	–	–	–	–	–	3	5	8
Outaouais	2	1	–	–	–	–	–	–	3
Saguenay-Lac-Saint-Jean	–	–	–	–	2	–	–	–	2
Sexe									
Homme	4	4	4	4	3	3	4	4	29
Femme	3	3	4	4	3	3	4	4	29
Âge									
18 à 24 ans	1	–	1	1	1	2	1	1	8
25 à 34 ans	1	–	2	1	1	1	2	–	8
35 à 44 ans	2	2	2	2	2	1	1	2	14
45 à 54 ans	–	1	1	–	–	1	1	2	6
55 à 64 ans	2	2	1	2	1	–	2	1	11
65 à 74 ans	1	2	1	2	1	1	1	2	11
Scolarité									
Secondaire ou moins	2	–	2	3	1	1	2	1	12
Collégial	1	2	3	2	3	4	1	3	19
Université	4	5	3	3	2	1	5	4	27

2 Observations et constatations

Observations et constatations

La recherche a d'abord permis de faire un certain nombre d'observations concernant la confiance des citoyens envers le gouvernement, et leur niveau de connaissance du Dossier de santé numérique (DSN) et du Service québécois d'identité numérique (SQIN). Aussi, elle a permis de faire plusieurs constatations au sujet des leviers et des freins liés à l'acceptabilité sociale de ces initiatives. Ces constatations concernent les facteurs qui rendent les citoyens réticents à l'idée de partager leurs informations si celles-ci doivent être exploitées par ces nouvelles solutions technologiques, ainsi qu'aux mécanismes et leviers qui rendraient plus acceptable le partage de leurs renseignements et favoriseraient l'usage de ces solutions.

Observations sur la confiance et la connaissance préalable des initiatives numériques gouvernementales

La confiance envers le gouvernement quant à la gestion des renseignements personnels est assez élevée

De manière générale, on constate que les participants sont assez confiants vis-à-vis du gouvernement en ce qui concerne la gestion de leurs données personnelles ainsi que de leurs renseignements de santé. Nous avons demandé aux participants d'indiquer sur une échelle de 1 à 10 ce niveau de confiance (1 = aucune confiance et 10 = pleine confiance) et la moyenne se situait autour de 7 pour les données personnelles et autour de 8 pour les renseignements de santé[6].

Les citoyens connaissent peu ou pas le DSN

Lorsqu'on a demandé aux participants s'ils avaient déjà entendu parler du DSN, 20 ont répondu oui, 7 ont répondu vaguement et 31 ont répondu non (n = 58). Ceci indique un certain niveau d'ignorance au sujet de ces projets chez les participants interrogés. Après leur avoir soumis un texte explicatif décrivant le DSN [7], plusieurs participants reconnaissaient désormais que des avantages pouvaient lui être associés. Une autre interrogation qui est revenue à quelques reprises concernait la différence entre le Dossier de santé Québec (DSQ) et le DSN, qui pouvait créer un peu de confusion chez des participants déjà familiers avec le DSQ. À cela, on peut ajouter qu'il y avait un sentiment généralisé de ne pas avoir suffisamment d'informations pour porter un jugement éclairé sur la mise en place du DSN. Ceci nous rappelle que les opinions que nous avons récoltées doivent être considérées avec une certaine réserve.

Le Système québécois d'identité numérique (SQIN) est généralement peu compris même si la plupart des participants avaient déjà entendu parler du concept d'identité numérique.

La plupart des participants avaient déjà entendu parler d'identité numérique, mais très peu d'entre eux se sentaient assez sûrs d'eux-mêmes pour pouvoir en fournir une définition. Après la lecture d'un texte explicatif sur l'identité numérique par l'animatrice, seule une minorité de participants indiquaient être enclins à utiliser l'identité numérique pour interagir avec le gouvernement. En revanche, un plus grand nombre de participants se sentaient prêts à partager leurs renseignements de santé, comparativement aux autres renseignements personnels. Pour certains, les bénéfices potentiels pourraient compenser les risques (notamment, la simplicité pour se connecter aux services en ligne). Une connaissance plus approfondie, engendrée par une plus grande transparence de la part du gouvernement, pourrait possiblement changer les perceptions. Aussi, la conception qu'avaient les participants de ce qu'est un portefeuille numérique s'est avérée être un élément intéressant. En effet, certains participants croyaient que le portefeuille numérique allait seulement exister de manière locale, sur leur téléphone, ce qui augmentait le risque perçu si celui-ci était perdu ou volé.

6 Étant donné la nature qualitative de l'étude, on ne peut en tirer des conclusions statistiquement significatives pour l'ensemble de la population. Ces valeurs ne représentent que les connaissances des participants aux groupes de discussion.

7 Voir le guide d'entretien en annexe.

Constatations sur les freins et les leviers pour la confiance envers le gouvernement

À partir de l'analyse des réponses des participants, certaines tendances émergent qui nous permettent d'identifier des facteurs qui influencent positivement ou négativement le sentiment de confiance quant au partage de renseignements personnels. La section qui suit présente une synthèse de ces facteurs. Les contextes de partage sont spécifiés lorsque pertinents.

Freins

Les participants ont indiqué avoir des réticences quant au partage de leurs renseignements sur la base des risques qu'ils perçoivent

Un premier frein important à la confiance envers le gouvernement dans le contexte du partage de renseignements personnels est lié aux risques inhérents à ce partage. Il est important de souligner que ces risques sont des risques perçus et non nécessairement des risques nommés sur la base de faits réels. Pour la plupart des participants, les risques étaient différents selon le type de renseignement partagé. Par exemple, nous avons pu noter une différence de perception du risque entre la fraude d'identité en lien avec les renseignements d'identification personnels et la discrimination en lien avec les données de santé. Pour la majorité des participants, les risques étaient aussi reliés à la « valeur » des renseignements pour des individus potentiellement mal intentionnés. En effet, les renseignements qui pourraient permettre d'obtenir un gain financier étaient perçus comme plus à risque. Les propos d'un participant résument bien cette observation :

> *Le risque est plus élevé dans les autres sphères que la santé. On parle d'argent, des gens malveillants qui veulent frauder. C'est plus facile d'obtenir des renseignements personnels comme le NAS pour usurper l'identité d'une personne.*

Le tableau 2 résume les risques les plus importants qui ont été relevés par les participants, en faisant la distinction entre les renseignements personnels en général et les renseignements de santé plus spécifiquement.

Les participants se méfient d'un manque éventuel d'éthique et de professionnalisme.

En ce qui concerne spécifiquement le DSN et les renseignements de santé, les participants sont davantage méfiants quant à la possibilité d'un manque d'éthique et de professionnalisme chez ceux qui utilisent les renseignements de santé (employés du secteur public, médecins, etc.) qu'envers le « gouvernement » de manière générale. À cet effet, les propos d'un participant sont révélateurs :

> *Le gouvernement a ma confiance. Ma réserve est plus envers l'humain qui va traiter les données. Les informations seront-elles accessibles seulement aux docteurs, ou aussi à toutes les infirmières, aux préposés aux bénéficiaires, etc.? J'ignore si tous les intervenants de la santé font partie d'un ordre professionnel, et donc si quiconque commet une faute peut se faire taper les doigts. Un accès étendu à trop de monde ouvre la porte à certains qui ne devraient pas y avoir accès.*

La manière dont les données sont organisées et gérées soulève des craintes chez les participants.

Pour les participants, dans le contexte de l'identité numérique, le fait de retrouver toutes les informations d'identification au sein d'un seul point d'accès revenait à « mettre tous ses œufs dans le même panier » et engendrait des risques considérables. Pour cette raison, on peut dire que la centralisation apparaissait comme un frein considérable au sentiment de confiance. Les participants étaient aussi d'avis que la centralisation pourrait introduire un autre risque important, soit celui de dérive du gouvernement pouvant éventuellement porter atteinte aux libertés individuelles. À cet effet, certains participants ont fait référence au gouvernement chinois comme exemple de dérive :

> *Je trouve un peu dangereux que le gouvernement ait toutes nos informations en même temps (ex. : la reconnaissance faciale qui empiète sur les droits des citoyens chinois). On l'a vu pendant la pandémie, le gouvernement s'octroie des droits supplémentaires en état d'urgence, il fait des choses qu'il ne ferait pas habituellement. Toutes nos données seraient à sa portée.*

Tableau 2

Types de risques (source : rapport SOM)

Renseignements personnels		Renseignements de santé	
Vol d'identité	Risques accrus pour l'identité, l'adresse, le compte bancaire, le NAS, et tout ce qui est lié au nom de la personne.	**Intégrité des renseignements**	Perte, vol ou partage non autorisé (ex. : vente de données à des compagnies pharmaceutiques)
Fraude et manipulation avec l'IA	Risque de fraude avec l'utilisation de l'IA (ex. : imitation de la voix pour obtenir des renseignements personnels).	**Discrimination**	Discrimination potentielle envers une personne sur la base de ses informations de santé par un employeur, un assureur ou un individu malveillant; un gestionnaire pourrait avoir accès à des informations sensibles lors d'une demande d'emploi.
Sécurité financière	Risque de « vidage » des comptes bancaires (avec des difficultés, pour les compagnies concernées, de rembourser); difficultés à rétablir un dossier financier après une tentative de fraude.	**Impact financier**	Primes plus élevées pour une assurance vie en cas de fuite de renseignements de santé non déclarés ou refus d'assurance; association erronée de problèmes médicaux non liés pouvant nuire à une demande d'indemnisation (ex. : CNESST).
Fuite et usage non autorisé	Utilisation non autorisée des données personnelles à des fins non consenties.	**Fraude**	Un individu malveillant pourrait utiliser les données d'une personne vulnérable pour l'extorquer ou pour lui vendre un produit.
Erreurs et risques liés à l'humain	Des erreurs d'authentification et des risques d'erreurs humaines accrus lorsqu'un grand nombre de personnes manipulent les données.	**Diagnostic médical biaisé**	Un médecin pourrait être influencé par les avis de ses confrères dans son diagnostic plutôt que se fier à ses propres observations.
Publicité et sollicitation	Profilage pour la publicité (ex. : sur les réseaux sociaux); sollicitation téléphonique et par courriel (ex. : pourriel)	**Gestion des dossiers**	Préoccupation liée au facteur humain, incluant la destination des dossiers, les personnes qui les consultent (ex. : par curiosité), et leur destruction inappropriée.

Il existe une perception négative quant à la capacité du gouvernement de bien gérer les données personnelles.

Un second frein important qui affecte le sentiment de confiance quant à l'ouverture à partager ses données personnelles réside dans la perception de la capacité du gouvernement à les gérer. Il est important de souligner qu'il ne s'agit pas, chez nos participants, d'une crainte de potentielles malversations, mais de doute sur une capacité que nous pourrions qualifier de « technique ». En effet, pour beaucoup de participants, le gouvernement n'a pas nécessairement la capacité de bien gérer les renseignements personnels ni de mener à bien ses grands chantiers de transition numérique tels que le DSN ou la mise en place de l'identité numérique. Cette perception négative de la capacité du gouvernement provient surtout de l'échec de projets gouvernementaux antérieurs, l'exemple de SAAQclic ayant été nommé à maintes reprises. Dans cette lignée, des participants ont exprimé des doutes quant à l'investissement du gouvernement dans le développement d'une expertise adéquate. Certains ont mentionné l'importance de débloquer des fonds nécessaires pour faire affaire avec des entreprises compétentes, mais également l'amélioration des conditions de travail, en faisant notamment mention des salaires peu compétitifs, au sein du gouvernement, ce qui n'attirait peut-être pas les experts les plus compétents. Les mots d'un participant à propos de la mise en place du DSN reflètent bien ce sentiment :

> *Je pense que le gouvernement a la volonté de bien le faire, c'est assez unanime. C'est la capacité qui est questionnée.*

De manière générale, il y a une impression partagée que le gouvernement doit faire ses preuves avant qu'on lui attribue la capacité de mener à bien de tels projets.

Leviers

Les freins mentionnés par les participants sont parfois fondés sur des expériences vécues, des expériences relatées dans les médias ou encore des craintes face à de potentiels problèmes. Les participants ont toutefois de nombreuses suggestions pour atténuer ces craintes et plusieurs éléments peuvent être mis à contribution pour venir renforcer le sentiment de confiance et favoriser une plus grande ouverture quant au partage des renseignements personnels et de santé, dans les divers contextes visés.

Les points suivants font état des principaux leviers suggérés par les participants. Nous pouvons les classer en deux catégories : les mesures ou pratiques existantes et celles qui pourraient être mises de l'avant. Ces pratiques peuvent certainement être améliorées, mais les participants sont d'avis qu'elles soutiennent l'adhésion au partage des renseignements.

Éléments déjà existants qui favorisent la confiance

Un certain nombre de pratiques existantes contribuent à maintenir le niveau de confiance des citoyens envers le gouvernement dans le cadre de ce type de projets.

Compréhension des bénéfices associés au partage des renseignements

Les bénéfices qui pouvaient être associés au fait de partager des renseignements personnels et de santé étaient souvent associés à une plus grande ouverture au partage. Il n'est toutefois pas évident de déterminer si les bénéfices ont comme fonction d'augmenter le sentiment de confiance ou plutôt de venir compenser les risques perçus. Quoi qu'il en soit, connaître les bénéfices semble jouer un rôle positif dans la volonté des participants de partager leurs renseignements. Le bénéfice principal qui était relevé concernait l'amélioration de la qualité des services. Que ce soit pour rendre l'accès aux services gouvernementaux plus « pratique » ou pour améliorer la qualité des soins, dans le contexte du DSN, pour plusieurs participants, les bénéfices sont un levier considérable pour favoriser l'ouverture au partage des renseignements avec le gouvernement.

Perception positive de la volonté gouvernementale de bien faire

Un autre élément qui semblait mettre en confiance les participants, lorsqu'il était question de la gestion de renseignements personnels dans le contexte numérique, était la volonté du gouvernement, qui était généralement perçue positivement. En somme, on considère que le gouvernement est bien intentionné lorsqu'il gère les renseignements personnels et qu'il met en place ses chantiers de transitions numériques. Il s'agit d'un élément clé dont les autorités peuvent tirer profit pour accroître l'adhésion aux projets.

Mesures existantes satisfaisantes et rassurantes

Dans la même veine, certaines mesures de sécurité et encadrements venaient aussi renforcer le sentiment de confiance ainsi que l'ouverture au partage des renseignements personnels avec le gouvernement. Plusieurs se disaient rassurés par les mesures existantes telles que les questions de sécurité et l'authentification à deux facteurs. Un participant faisait à cet effet la remarque suivante :

> *La connexion aux services en ligne est très sécurisée (plusieurs questions sont posées et, après trois réponses incorrectes, l'accès est bloqué; la double vérification avec envoi d'un code sur le téléphone pour accéder au compte) c'est rassurant.*

Aussi, spécifiquement en lien avec les renseignements de santé, ceux-ci bénéficient d'un niveau d'encadrement plus strict, via des codes de déontologie, les ordres professionnels, les règles éthiques, etc., ce qui rassure et favorise le sentiment de confiance.

Nouvelles mesures qui pourraient favoriser la confiance

Nous avons aussi pu explorer plus à fond les différentes mesures qui pourraient être mises en place pour augmenter le sentiment de confiance, dans les différents contextes de partage des renseignements personnels. Voici les principales :

Faire preuve de transparence

Comme nous l'avons souligné, il y a beaucoup d'inconnu pour les participants en ce qui concerne des projets comme le DSN et le Système québécois d'identité numérique. Ceci influence négativement le sentiment de confiance. De manière générale, les participants ont souligné qu'il était important d'informer et de rassurer la population au sujet du fonctionnement de ces infrastructures numériques, des mécanismes de protection qui seront utilisés, des avantages, des risques, etc. Il a aussi été mentionné qu'il serait pertinent d'identifier les données qui seront utilisées et conservées et de s'assurer que seules les données nécessaires soient conservées. Aussi, certains ont mentionné qu'il serait approprié de faire un suivi des projets auprès de la population; identifier les étapes prévues, les résultats attendus pour chaque étape, les problèmes, les budgets, l'échéancier, les noms des entreprises impliquées, etc. En bref, les participants demandent plus de communication dans un langage compréhensible.

Se donner la capacité

Une autre mesure cruciale concerne le fait de faire les investissements nécessaires afin d'utiliser l'expertise adéquate pour mener à bien les projets de transition numérique gouvernementaux. En effet, comme nous l'avons maintenant vu à quelques reprises, la perception négative de la capacité du gouvernement contribuait à diminuer le sentiment de confiance; il est donc assez logique que plusieurs participants indiquent qu'il est crucial que le gouvernement fasse tous les efforts nécessaires afin de mobiliser les meilleurs experts et d'utiliser des technologies de pointe.

Plusieurs participants ont d'ailleurs indiqué qu'il était important de s'assurer d'avoir les experts les plus qualifiés plutôt que de se contenter de choisir le soumissionnaire le moins cher.

S'inspirer d'ailleurs

Une autre mesure qui pourrait venir rassurer la population, si l'on en croit les propos des participants, rejoint certains des éléments mentionnés en lien avec la transparence. Il s'agit, plus spécifiquement, de s'inspirer des réussites de projets d'identité numérique réalisés ailleurs dans le monde. En plus de s'en inspirer, le gouvernement pourrait aussi démontrer que la direction qu'il choisira en matière d'identité numérique a déjà fait ses preuves. Autrement dit, il pourra montrer qu'ailleurs ça « fonctionne ». Pour plusieurs, le fait de pouvoir se référer à d'autres projets qui ont été un succès les rassurerait.

Bien baliser les accès et compartimenter les données

Que ce soit pour le DSN ou l'identité numérique, il a été souligné qu'il était crucial de bien gérer les accès aux données. Par exemple, dans le cadre du DSN, les accès au dossier de santé pourraient être autorisés par le médecin de famille et il pourrait y avoir une « empreinte numérique » pour retracer les accès ainsi que les modifications au dossier. Il est important que l'on utilise seulement les données nécessaires et que les accès soient contrôlés en fonction des différents services gouvernementaux. À cet effet, un des participants donnait l'exemple suivant lorsqu'il était question d'identité numérique :

> *Je ne veux pas que tout le monde ait accès à tout. La SAQ n'a pas besoin d'avoir accès à mon dossier de santé, même chose pour le médecin et mon retour d'impôt.*

À cet effet, des participants ont mentionné que les dispositifs qui permettent de punir un employé contrevenant, qui accéderait sans autorisation aux données, pourraient potentiellement à être mis à jour. En d'autres termes, le cadre normatif et éthique doit être mis à niveau au fur et à mesure que le partage des données s'accroîtra.

Prendre le temps

Concernant spécifiquement l'identité numérique, plusieurs participants ont suggéré que le gouvernement n'avance pas trop rapidement afin d'éviter des problèmes. Le fait d'y aller progressivement, par secteur, augmenterait le sentiment de confiance des participants. Dans le même ordre d'idée, il est suggéré de procéder à des projets pilotes de façon à démontrer la capacité du gouvernement à gérer ce type de données. Aussi, ces projets pilotes pourraient prouver que les projets comme l'identité numérique ou le DSN peuvent être à la hauteur de leurs promesses en ce qui concerne les bénéfices attendus et leur degré de sécurité. À cela, on peut ajouter que, pour la majorité des participants, il est important que l'adhésion à l'identité numérique demeure facultative, pour laisser un temps de transition adéquat. Cela dit, sur le long terme, des participants concédaient que de maintenir deux systèmes parallèles serait inefficace.

Autres constatations

Deux autres dimensions du partage de données personnelles ont été explorées lors des groupes de discussion, soit la différence perçue entre les pratiques du secteur privé et celles du secteur public, ainsi que la pertinence d'étendre ce partage au gouvernement fédéral.

Différence entre le secteur public et le secteur privé

Les participants se sont prononcés sur les différences perçues entre le secteur public (gouvernement) et le secteur privé (entreprises) en ce qui a trait à la confiance dans le cadre de la gestion de renseignements personnels et de santé. Ces différences peuvent être groupées autour de la volonté et de la capacité d'agir ainsi que de l'enjeu des potentiels abus de confiance.

Volonté et capacité : une relation inverse entre le privé et le public

Premièrement, il existe une différence notable sur le plan de la perception de la capacité et de la volonté, entre les deux secteurs. Comme nous l'avons déjà dit, du côté du gouvernement, les participants identifiaient que la volonté n'était pas remise en cause, autrement dit, que le gouvernement était bien intentionné et qu'il voulait bien faire les choses. Cependant, la capacité était perçue plus négativement, c'est-à-dire que malgré cette bonne volonté, plusieurs participants ne croyaient pas que le gouvernement ait la capacité de bien protéger leurs renseignements et de mener à bien ses grands projets de transition numérique (DSN et identité numérique). Pour ce qui est du secteur privé, nous observons le phénomène inverse, c'est-à-dire que la capacité est perçue plus positivement, alors que la volonté est souvent remise en question. La plupart des participants associaient davantage les technologies et les systèmes de pointe aux compagnies privées, alors que, pour le gouvernement, on référait souvent à des technologies et des systèmes plus archaïques et moins performants.

> *Les entreprises privées, étant imputables de leurs fautes, auront tendance à être plus à jour, à faire plus attention, à disposer d'experts en sécurité un peu plus calés qu'au gouvernement.*

Contrairement au gouvernement, le privé est associé à la volonté de faire un profit. Ceci est vrai pour tous types de renseignements, mais dans le secteur de la santé, les participants ont soulevé des craintes supplémentaires. En effet, dans leur recherche de profit, les acteurs privés pourraient vendre des données à des compagnies pharmaceutiques. Pour plusieurs participants, cette possibilité diminuait le sentiment de confiance. Aussi, cette observation valait encore plus pour les « GAFAM »[8], qui étaient généralement perçus comme encore moins dignes de confiance.

> *Les réseaux sociaux, Visa et d'autres entreprises privées vendent nos données à des annonceurs, entre autres. Je leur fais moins confiance. Elles ont un intérêt pécuniaire, alors que l'intérêt du gouvernement est de préserver notre sécurité. Quant aux services médicaux privés, je crois que c'est moins pire que les GAFAM*. Ça demeure des données de santé, donc il y a un code d'éthique à respecter, plus grand que chez Facebook, par exemple.*

Abus de confiance

Pour certains participants, un sentiment de confiance généralisé envers le gouvernement contribuait à une confiance plus spécifique lorsqu'il s'agissait du contexte de la gestion et la protection des données personnelles. Il a été mentionné que pour le gouvernement, il n'y avait pas encore eu d'« abus de confiance majeur », contrairement à des entreprises telles que Desjardins. Autrement dit, le fait qu'il n'y ait pas eu d'abus de confiance majeur de la part du gouvernement mène certains à avoir plus confiance envers celui-ci qu'envers des entreprises privées.

Partage provincial-fédéral des renseignements de santé

Le dernier élément concernait l'ouverture des participants à utiliser le système d'identité numérique pour partager des renseignements de santé avec le gouvernement fédéral. Cette dernière question était plus spéculative, mais nous constatons que pour la majorité des participants, on ne voit pas nécessairement l'utilité d'un tel partage, la santé relevant pour l'essentiel d'une juridiction provinciale.

> *Revenu Québec et l'ARC partagent déjà des informations. Je ne vois pas ce que le fédéral aurait à faire dans le système québécois de santé. C'est de compétence provinciale et non fédérale.*

L'exception qui semble être acceptée par la plupart des personnes rencontrées est le partage de renseignements de santé de façon anonyme pour des **finalités de recherche** (ex. statistiques). Dans ce contexte, elles aimeraient que leur consentement soit demandé pour chaque utilisation.

> *Si l'on donne notre consentement une fois, le gouvernement fédéral ne doit pas garder notre dossier par la suite, mais redemander notre consentement chaque fois qu'il a des besoins.*
>
> *Pour ce qui est d'un projet de recherche, c'est du cas par cas et ça prendrait une autorisation plus spécifique de ma part, si je suis intéressée. Mais j'aurais une réserve si c'était ouvert at large à n'importe qui au gouvernement pour faire des recherches sur je ne sais quoi.*

D'autres exceptions mentionnées par quelques participants : en cas de voyage dans d'autres provinces du Canada ou à l'étranger; dans des contextes graves (une pandémie, par exemple, ou pour demander l'avis d'un médecin de l'extérieur du Québec doté d'une expertise sur un problème de santé très spécifique). On retrouve ici encore l'idée, précédemment énoncée dans le cadre des projets provinciaux, que des bénéfices tangibles sont nécessaires pour justifier le partage des renseignements de santé avec le gouvernement fédéral.

8 Les participants se référaient ici, par cette expression assez connue, aux géants du numérique : Google, Amazon, Facebook, Apple, Microsoft.

3 Discussion

Discussion

Les résultats des groupes de discussion permettent à la fois de renforcer et de préciser les constatations faites lors de l'enquête de 2020-2021 sur le partage des renseignements de santé (Caron, Bernardi, et al., 2020). Entre autres, mais essentiellement, ils mettent en évidence l'importance pour le gouvernement et l'administration publique de construire un modèle d'affaires transparent et robuste. Dans cette veine, il importe de souligner certains éléments spécifiquement liés à la question de la confiance. En effet, ces éléments nouveaux ont été discutés lors des groupes de discussion et ont mis en lumière l'existence d'un lien étroit entre les attentes citoyennes et la perception de la volonté, la motivation et la capacité du gouvernement et de l'administration publique.

Nous avons pu constater que lorsqu'il est question de la protection des renseignements personnels et de santé, et de la mise en place de nouvelles plateformes et outils numériques par le gouvernement, la volonté et la motivation de ce dernier sont rarement remises en question. Les participants croient que le gouvernement veut généralement bien faire. Le gouvernement veut réussir ce qu'il entreprend et il est motivé à atteindre ses objectifs du mieux qu'il peut. Les participants ne doutent généralement pas de la bonne foi du gouvernement sur ces dimensions. Ils accordent donc, dans une certaine mesure, leur confiance au gouvernement. En revanche, la troisième composante de la confiance, soit la capacité, est souvent identifiée comme un point faible. Ceci est central pour que l'acceptabilité sociale puisse cheminer, mais surtout, c'est un enjeu qui n'est pas insoluble. Par exemple, les raisons évoquées pour cette remise en question de la capacité concernent les investissements qui ne sont pas jugés suffisants, ainsi que les « échecs » de projets gouvernementaux antérieurs. Il s'agit d'abord et avant tout de perceptions. En ce sens, les répondants justifiaient cette attitude en reflétant ce qu'ils savaient de ces projets à partir de ce qu'ils avaient pu entendre dans les médias ou ailleurs.

Les communications gouvernementales autour de ces projets jouent un rôle fondamental dans la construction de la confiance citoyenne autour de la perception de la *capacité*. Si la motivation et la volonté ne sont pas des enjeux, ou sont moins significatives, la perception de la capacité est une chose fragile. Le gouvernement doit avoir des messages simples, exhaustifs et empreints de neutralité politique. C'est-à-dire qu'ils doivent montrer, dans un langage accessible, la complexité des transformations projetées, faire valoir et appuyer les innovations et la prise de risques, et montrer les embûches, les difficultés et les gains liés aux projets. Ce qui ressort de notre étude, c'est que les gouvernements ne semblent pas assez présents sur la place publique pour soutenir l'administration et défendre les difficultés liées à ce type de projets. Il faut arriver à montrer que le gouvernement, à travers ses bons coups et ses opérations, a la capacité de mener à bien ces projets. Il ne faudrait pas laisser aux seuls critiques la possibilité de commenter les ratés et difficultés et ainsi influencer l'opinion publique; ceci ne rend pas nécessairement justice à la réalité ni à l'envergure des transformations, des efforts et des progrès réalisés. Bien entendu, lorsque les projets ont des ratés majeurs, il faut aussi les expliquer publiquement et en tirer les leçons appropriées. Évidemment, au-delà de la transparence, la capacité technique doit aussi être au rendez-vous. C'est-à-dire qu'il faut que les gouvernements aient les moyens de leurs ambitions et que ces moyens soient mis en évidence dans les communications à la population.

La différence entre le sentiment de confiance envers le secteur privé et le secteur public est un autre élément qui est ressorti des discussions. Il est intéressant de noter que lorsqu'on demandait aux répondants quel était leur sentiment de confiance envers le secteur privé, toujours dans le contexte de la protection des renseignements personnels et de santé, le phénomène était inversé. C'est-à-dire que la capacité était généralement perçue positivement dans le cas du privé, alors que le manque de confiance provenait plutôt de la volonté ou de la motivation, qui étaient associées à une volonté de faire un profit et non de défendre le bien public.

Ceci nous amène à un autre point qui concerne les risques associés au partage et à la gestion des renseignements personnels et des renseignements de santé. Nous avons constaté que bien que ces risques soient assez variés, il demeure que les risques qui pouvaient avoir un impact financier étaient identifiés comme plus importants par la plupart des participants. On peut ici penser à la fraude financière ou au vol d'identité. Ceci s'explique sans doute par le fait que ce type de risque est celui qui aurait le plus d'impact sur la vie des participants. Aussi, on peut penser que l'occurrence de ce type de risque est plus élevée parce que dans la majorité des cas, les acteurs malveillants sont motivés par les gains financiers immédiats. Cependant, il est aussi important de soulever que les bénéfices, associés au partage des renseignements et à l'utilisation des plateformes telles que le DSN ou de l'identité numérique, pouvaient venir compenser ces risques. Ce sentiment n'était pas partagé de manière unanime, mais mettre l'accent sur les avantages associés au partage des renseignements pourrait augmenter le sentiment de confiance. La connaissance des bénéfices était clairement ressortie lors de l'enquête de 2020-2021 (Caron, Bernardi, et al., 2020) comme un élément qui faisait évoluer l'opinion des répondants vers une plus grande ouverture quant au partage de leurs renseignements de santé. La communication des bénéfices associés aux différents projets est donc une approche prometteuse pour favoriser la confiance de la population.

Pour ce qui est d'autres mesures qui pourraient être mises en place afin de renforcer la confiance et, éventuellement, mener à une plus grande ouverture au partage des renseignements et à l'utilisation des plateformes numériques gouvernementales, nous pouvons réitérer les deux orientations globales déjà mentionnées à plusieurs reprises.

Premièrement, nous avons vu que, pour plusieurs, le manque de connaissance influençait négativement le sentiment de confiance; lorsqu'ils étaient mieux informés, tant sur le fonctionnement qu'au sujet des avantages associés aux plateformes telles que le DSN ou l'identité numérique, ils se sentaient plus en confiance. Deuxièmement, il est important de s'attaquer aux doutes quant à la capacité du gouvernement de mener à bien ces projets de transitions numériques tout en protégeant les renseignements personnels. Il faut non seulement que le gouvernement se donne cette capacité, via les investissements et le temps nécessaires, le recrutement des meilleurs experts, etc., mais il doit aussi prouver à la population qu'il a cette capacité. À cet effet, des projets pilotes, des projets de transitions numériques menés avec succès, et une plus grande transparence quant à ces initiatives, pourraient influencer positivement la perception de la capacité à réussir la transition numérique.

Conclusion

En conclusion, il faut souligner qu'il y a convergence entre les constatations découlant des analyses quantitatives issues de l'enquête de 2020-2021 (Caron, Bernardi, et al., 2020) et celles des groupes de discussion de la présente enquête. Il y a maintenant plus de précisions sur les leviers à actionner pour accroître l'acceptabilité sociale, l'engagement citoyen et la confiance autour de ces projets. Entre autres, la capacité des gouvernements doit se matérialiser, être davantage mise en lumière en mettant l'accent sur les acquis et en manifestant, par exemple, un appui aux efforts de transformation, même si le succès n'est pas toujours immédiat. De ce fait, l'autre élément central est que les gouvernements doivent communiquer et informer davantage les citoyens. Ces derniers fondent en partie leur confiance sur leurs interactions avec l'administration, sur ce qu'ils entendent au sujet des différents projets et sur la compréhension qu'ils ont du fonctionnement de l'État. Il y a définitivement un enjeu de littératie et plus d'informations, ciblées selon différents groupes de la population, devraient favoriser une plus grande confiance.

Références

Camoes, P., & Mendes, S. (2019). Do Citizens Trust the Civil Service Differently ? Comparing the Determinants of Confidence in Political-Administrative Institutions. *INTERNATIONAL JOURNAL OF PUBLIC ADMINISTRATION*, *42*(14), 1234-1244. https://doi.org/10.1080/01900692.2019.1592187

Caron, D. J., Bernardi, S., & Nicolini, V. (2020). *L'acceptabilité sociale du partage des données de santé : Revue de la littérature*. Chaire de recherche en exploitation des ressources informationnelles.

Caron, D. J., Montmarquette, C., Prud'homme, A., Bernardi, S., & 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, ENAP. https://espace.enap.ca/id/eprint/323/1/Rapport_accept.sociale_caron_20220114.pdf

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.

Conseil de l'innovation du Québec. (2023). *Analyse des contributions publiques : Dans le cadre de l'appel à contributions lancé par le Conseil de l'innovation du Québec* (réflexions collectives sur l'encadrement de l'IA). https://conseilinnovation.quebec/wp-content/uploads/2023/10/CIQ_Contributions_publiques-2.pdf

Falcone, R., Coli, E., Felletti, S., Sapienza, A., Castelfranchi, C., & Paglieri, F. (2020). All We Need Is Trust : How the COVID-19 Outbreak Reconfigured Trust in Italian Public Institutions. *FRONTIERS IN PSYCHOLOGY*, *11*. https://doi.org/10.3389/fpsyg.2020.561747

Foster, C., & Frieden, J. (2017). Crisis of trust : Socio-economic determinants of Europeans' confidence in government. *EUROPEAN UNION POLITICS*, *18*(4), 511-535. https://doi.org/10.1177/1465116517723499

Ghafur, S., Van Dael, J., Leis, M., Darzi, A., & Sheikh, A. (2020). Public perceptions on data sharing : Key insights from the UK and the USA. *The Lancet. Digital Health*, *2*(9), e444-e446. https://doi.org/10.1016/S2589-7500(20)30161-8

Gouvernement du Québec. (2020). *Penser le Québec de demain durablement—Consultation Québec*. https://consultation.quebec.ca/processes/developpementdurable?locale=en

Luhmann, N. (2017). *Trust and power* (English edition). Polity.

Maiorana, A., Steward, W. T., Koester, K. A., Pearson, C., Shade, S. B., Chakravarty, D., & Myers, J. J. (2012). Trust, confidentiality, and the acceptability of sharing HIV-related patient data : Lessons learned from a mixed methods study about Health Information Exchanges. *Implementation Science: IS*, *7*, 34. https://doi.org/10.1186/1748-5908-7-34

Mesa, D. (2023). Digital divide, e-government and trust in public service : The key role of education. *FRONTIERS IN SOCIOLOGY*, *8*. https://doi.org/10.3389/fsoc.2023.1140416

Ministère de l'Environnement, de la Lutte contre les changements climatiques, de la Faune et des Parcs. (2025). *Participation du public dans le cadre des procédures d'évaluation environnementale*. https://www.environnement.gouv.qc.ca/evaluations/participation-public/index.htm#consultation-enjeux

Platt, J. E., Jacobson, P. D., & Kardia, S. L. R. (2018). Public Trust in Health Information Sharing : A Measure of System Trust. *Health Services Research*, *53*(2), 824-845. https://doi.org/10.1111/1475-6773.12654

Annexe 1 : Guide de discussion

GROUPES DE DISCUSSION

Ouest du Québec, ZOOM - Mercredi 7 février 17 h 30 et 19 h 30

RMR Québec, SOM Québec - Jeudi 8 février 17 h 30 et 19 h 30

Est du Québec, ZOOM - Jeudi 15 février 17 h 30 et 19 h 30

RMR Montréal, SOM Montréal - Lundi 19 février 17 h 30 et 19 h 30

Introduction 10 min.

- Mot de bienvenue, remerciement et présentation de l'animatrice et de l'assistante technique.
- Objectif de la rencontre : L'ÉNAP (École nationale d'administration publique) souhaite explorer la confiance des Québécois à l'égard du partage de leurs renseignements de santé dans le cadre technologique actuel et avec l'utilisation d'un identifiant numérique pour savoir de quelle manière encadrer le tout. Nous allons aussi aborder la question de l'identité numérique.
- Rôle de l'animatrice et des participants.
- Déroulement de la rencontre : durée, règles, enregistrement, confidentialité, observatrices.
- Questions des participants, s'il y a lieu.

Le type de données 60 min.

- **(Activité brise-glace)** : En quelques mots ou une courte phrase, j'aimerais que vous me disiez c'est quoi pour vous la confiance? (Tour de table)
- J'aimerais que vous me donniez une note de 1 à 10 pour illustrer votre niveau de confiance envers le gouvernement pour la gestion :
  - De vos données personnelles de manière générale?
  - De vos renseignements de santé?
  - *(Tour de table pour obtenir les deux notes, sans demander d'explications)*
- Si vous pensez aux services gouvernementaux en ligne (Santé, revenu, travail, obtention de permis, etc.) comment vous sentez-vous par rapport à la protection de vos renseignements personnels en ce qui concerne :
  - Vos données personnelles de manière générale? (Creuser les appréhensions, le cas échéant)
  - Vos renseignements de santé? (Creuser les appréhensions, le cas échéant)
- Si vous pensez à la protection de vos renseignements personnels dans le secteur privé, par exemple, les services médicaux privés (ex : Dynacare, Telus santé), sur les réseaux sociaux, pour des achats en ligne, est-ce que c'est différent? (Plus, autant, moins à l'aise qu'avec le gouvernement?)
- (*Si aucune appréhension nommée précédemment* : D'après-vous est-ce qu'il existe des risques quand on pense à la gestion des renseignements de santé?) Ce serait quoi selon vous les deux principaux risques?
  - Est-ce que c'est différent si vous pensez à vos autres renseignements personnels (revenus, diverses bases de données etc.)?

(Énoncé à lire) : V*ous avez peut-être entendu parler du Dossier de santé numérique communément appelé le DSN? (Main levée) La mise en œuvre du DSN signifie qu' « (…) ultimement, (…) autant pour les professionnels de la santé que pour le patient, cette transformation fera gagner un temps précieux, en limitant la paperasse. Avec le dossier de santé numérique, les données suivront le patient. Il n'aura donc plus à raconter son histoire plusieurs fois en changeant d'établissement (…) »*

Ceci veut dire que vos données de santé seront liables selon les besoins et consultables par les professionnels qui en ont besoin. Il s'agit donc d'un système qui permet la mise en commun des renseignements de santé qui vous concernent principalement par l'interopérabilité des différents systèmes utilisés et non par une immense base de données où serait regroupé tous vos renseignements. (Au besoin : interopérabilité = des systèmes différents qui sont capables de fonctionner conjointement).

- Dans ce contexte, croyez-vous que le gouvernement soit fiable (capable/motivé) pour assurer la gestion des risques lorsqu'il s'agit de vos renseignements de santé (*rappeler les principaux risques mentionnés précédemment*)? (Note de 1 à 10 – main levée)

- Qu'est-ce qui pourrait être fait (mesures législatives, administratives, autres) pour augmenter/maintenir votre confiance que le gouvernement va bien gérer les risques?

Les solutions de liage et de partage (l'identité numérique) 30 min.

- Qui a déjà entendu parler d'identité numérique? (Main levée) Qui se sentirait assez sûr de lui/elle pour expliquer ce que c'est? (Main levée) Comment vous sentez-vous par rapport au concept d'identité numérique (Plutôt positifs, négatifs)?

(Énoncé à lire) : *L'identité numérique c'est « (..) la représentation numérique d'une personne qui lui permet de prouver son identité (…) » et de s'authentifier au moyen de données d'identification personnelle (ex. : identifiant, mot de passe). Par exemple pour les applications sur un téléphone intelligent, la carte à puce ou un compte en ligne.*

Le gouvernement est en train de déployer une nouvelle solution d'authentification pour accéder à certains de ses services et à vos dossiers en ligne. Elle permettra de répondre aux exigences de sécurité qui ont été rehaussées pour protéger votre identité numérique. En gros, il s'agit d'une application pour téléphone intelligent (portefeuille numérique) qui permettra de prouver son identité, mais aussi de démontrer une compétence (ex. : diplôme) ou une autorisation (ex. : permis de conduire). Le clic SÉQUR qu'on connaît sera graduellement remplacé par cette nouvelle solution.

(Au besoin seulement : Pour le citoyen, il n'y aura plus de mots de passe différents à retenir et de validation via des numéros sur relevé d'impôt, par exemple. À partir d'un seul endroit (portefeuille numérique), le citoyen pourra prouver son identité et stocker des éléments d'identification sous format numérique (ex. : permis de conduire). Aussi, bien que l'identité numérique soit distribuée par le gouvernement, elle pourra aussi être utilisée dans le contexte de services non gouvernementaux, exemple prouver son âge en achetant de l'alcool au dépanneur.)

(Au besoin seulement : La différence avec clicSÉQUR : clicSÉQUR ne permettait pas le liage des informations, il s'agissait seulement d'une manière de valider son identité via l'utilisation d'un utilisateur/mot de passe.)

Voici quelques-uns des bénéfices attendus (lire les trois premiers et les autres au besoin)

- *Démarches administratives simplifiées par la réduction des formalités et des délais d'accès aux services publics;*
- *Baisse du risque de fraude lié à l'identité en augmentant la robustesse des processus et des justificatifs;*
- *Limitation du nombre de renseignements personnels partagés;*
- *Interaction plus sécuritaire avec les organismes publics prestataires de services;*
- *Cadre structurant pour bâtir des services numériques sécuritaires;*
- *Gestion des données personnelles des citoyens plus efficiente;*
- *Meilleure accessibilité aux prestations électroniques de services du gouvernement du Québec;*
- *Meilleure compatibilité des diverses plateformes technologiques (ordinateur, tablette et téléphone cellulaire).*

- Avec cette description en tête, qui serait ouvert à utiliser un système d'identification numérique pour interagir avec le gouvernement si cela inclut :
  - Des renseignements de santé? (Main levée – valider réserves)
  - Les autres renseignements personnels? (Main levée – valider réserves)
- Croyez-vous que le gouvernement soit fiable (capable/motivé) pour assurer la gestion des risques lorsqu'il s'agit de l'utilisation de l'identité numérique? (Note de 1 à 10 – main levée)
- Seriez-vous ouverts à utiliser un système d'identification numérique pour partager vos renseignements de santé avec les deux paliers de gouvernement (les deux paliers se partageraient les renseignements)? (Main levée – valider réserves)

Retour aux observateurs et mot de la fin **5 min.**

Conclusion et remerciements.

Total : 1 h 45

obvia

obvia.ca