Citizen FIRST

POWERED BY Institute for Citizen-Centred Service

CITOYENS en tête

OPTIMISÉ PAR L'Institut des services axés sur les citoyens

RAPPORT FINAL

PERSPECTIVES SUR L'ACCEPTATION PAR LE PUBLIC DE L'UTILISATION DES DONNÉES PAR LE GOUVERNEMENT

17 NOVEMBRE, 2021

Numéro de la version	Date de publication	Auteur	Brève description
1.0	31 août 2021	Davis Pier Consulting	Première ébauche
1.1	2 septembre 2021	Davis Pier Consulting	• Ajout du résumé et des recommandations • Ajout d'infographies pour remplacer certains espaces réservés au texte • Mise à jour de la mise en page et de la mise en forme du document
1.2	23 septembre 2021	Davis Pier Consulting	• Mise à jour de la mise en page et de la mise en forme du document • Autres perfectionnements au contenu • Insertion des commentaires des membres du Groupe de travail sur les renseignements axés sur les données (GT RAD)
1.3	21 octobre 2021	Davis Pier Consulting	• Rétroaction incorporée de l'ISDE et des coprésidents du GT RAD
1.4	17 novembre 2021	Davis Pier Consulting	• Insertion de la rétroaction du SCT, du président du Sous-comité sur la protection de la vie privée des Conseils mixtes, de l'ARC et des MSDO.

Table des matières

01.
Résumé

Résumé

À mesure que les gouvernements cherchent à améliorer la prestation des services, un accent accru est mis sur l'adoption des principes de la conception axée sur la personne. Pour appuyer cette approche de conception centrée sur l'utilisateur, il est nécessaire de recueillir et de conserver des renseignements (dans de nombreux cas, des renseignements personnels) des citoyens desservis. En adoptant des initiatives comme « Une fois suffit », les renseignements peuvent être recueillis auprès d'un citoyen et ensuite communiqués à d'autres secteurs ou ministères qui lui fournissent des services. Ces renseignements peuvent également jouer un rôle essentiel dans la planification et la prestation des services, informant ainsi les gouvernements de ce que les citoyens veulent (et ne veulent pas) d'une expérience de prestation de services.

L'utilisation de données visant à améliorer la prestation de service dans tous les ordres du gouvernement du Canada soulève des questions comme l'utilisation responsable des données et des analyses, et la protection des renseignements personnels des citoyens. Les mesures législatives sur la protection des renseignements personnels exigent la notification de l'autorisation d'une partie de recueillir des renseignements personnels et de l'objet de la collecte. Si ces renseignements personnels sont ensuite utilisés, communiqués et/ou conservés pour des raisons qui ne sont pas compatibles avec cette fin, le consentement doit être obtenu. Toutefois, des concepts tels que le consentement implicite et l'« usage compatible » peuvent créer des situations dans lesquelles les renseignements sont légalement recueillis, utilisés et partagés à l'insu d'un citoyen.

Un autre aspect à prendre en considération n'est pas tant de savoir si les renseignements personnels des citoyens **peuvent** être utilisés et partagés légalement par le gouvernement, mais plutôt si les citoyens pensent que le gouvernement **devrait** utiliser et échanger leurs renseignements.

Le Groupe de travail sur les renseignements axés sur les données (GT RAD) de l'Institut des services axés sur les citoyens (ISAC) a entrepris une initiative visant à développer une compréhension globale de l'acceptation par le public de l'utilisation et de l'échange de données pour l'amélioration des services publics à l'intérieur et dans l'ensemble des ordres de gouvernements. Dans le cadre de cette initiative, Davis Pier a été chargé d'entreprendre des recherches sur le niveau d'acceptation par le public de l'utilisation et de l'échange des données gouvernementales, en mettant l'accent sur l'utilisation des données afin d'améliorer les services. Ce projet vise à éclairer l'orientation future de l'utilisation intergouvernementale des données au Canada, ainsi qu'à orienter les recherches futures sur les obstacles l'échange de données pour les services publics dans l'ensemble du gouvernement.

Il conviendrait de prendre note que, même si le présent rapport peut porter sur l'utilisation des données pour les canaux numériques, il est essentiel que les services soient toujours conçus pour être mis à la disposition de ceux qui n'ont pas d'accès en ligne ou au numérique, tels que les populations vulnérables ou marginalisées.

Approche

Afin de fournir un aperçu complet des niveaux publics d'acceptation de l'échange de données à partir de diverses sources et perspectives, l'équipe de projet a effectué des recherches en trois parties :

- **Analyse des perspectives géographiques :** Recherche documentaire et consultation auprès des intervenants au Canada et à l'étranger afin de déterminer les approches permettant de répondre à l'acceptation par le public de l'échange et de l'utilisation des données et des renseignements personnels afin d'améliorer la prestation des services gouvernementaux.

- **Revue de la littérature :** Résumé et analyse de sources de la documentation parallèle de qualité et examinées par les pairs, mettant l'accent sur les niveaux comparatifs d'acceptation de l'échange de données entre les régions géographiques et les groupes démographiques.
- **Analyse législative :** Analyse de la législation régissant la collecte, l'utilisation et la communication de renseignements personnels dans les provinces, territoires et municipalités du Canada et le gouvernement du Canada, notant les principales similitudes et les différences notables.

Ces approches distinctes ont permis de recueillir une gamme variée de points de vue qui permettent de mieux comprendre l'acceptation par le public de l'échange de données pour l'amélioration des services publics au Canada.

Principales perspectives

Les trois méthodes d'enquête utilisées fournissent une gamme variée de points de vue sur les niveaux d'acceptation par le public de l'utilisation des données par le gouvernement, tant dans un contexte canadien qu'international. Voici les principales constatations de chaque section :

Analyse des perspectives géographiques

- La majorité des administrations consultées dans le cadre de ce projet ne surveillent pas officiellement la perception du public quant à l'utilisation des données par le gouvernement. Malgré cela, la plupart des administrations recueillent encore ponctuellement des renseignements sur les perceptions du public provenant de diverses sources – par exemple, dans le cadre de consultations liées à une initiative stratégique ou à une modification législative.
- Les intervenants ont indiqué deux enjeux qui préoccupent le plus le public : une perception selon laquelle le gouvernement utilise les renseignements publics à des fins secondaires non communiqués et une frustration quant à l'obligation de fournir les mêmes renseignements à plusieurs reprises au gouvernement. Ces préoccupations du public représentent deux groupes de population de plus en plus divergents : l'un qui fait davantage confiance au gouvernement, et l'autre qui fait de moins en moins confiance au gouvernement.
- Conformément aux constatations ci-dessus, les effets de la pandémie de la COVID-19 variaient considérablement, allant de l'acceptation accrue de l'utilisation des renseignements par le gouvernement à une perte de confiance envers le gouvernement.

Revue de la littérature

- Revue de la littérature Les niveaux d'acceptation par le public de l'utilisation et de l'échange des données peuvent différer considérablement d'une région géographique à l'autre. On constate que les Canadiens ont généralement des niveaux de confiance plus élevés dans l'échange des données sur la santé par le gouvernement que les citoyens du Royaume-Uni, quoique moins élevés que ceux de l'Australie et des États-Unis.
- Les niveaux d'acceptation dans la collecte, l'utilisation et l'échange des données différaient sensiblement en fonction de l'utilisation prévue et du destinataire des données. Par exemple, l'utilisation de données dans le but d'améliorer la sécurité publique ou la santé publique est plus acceptable que pour les services généraux et l'administration. De même, on fait en général davantage

confiance aux médecins et aux chercheurs en santé pour la collecte et l'échange de données que d'autres parties, notamment les gouvernements et les entreprises privées.

- Bien que les données disponibles soient limitées dans un contexte canadien, les recherches suggèrent que la confiance envers l'utilisation et l'échange des données est généralement plus faible parmi les populations vulnérables, y compris les membres des collectivités LGBTQ et des collectivités de personnes autochtones, noires et de couleur.

Analyse législative

- Il existe 41 lois distinctes, chacune ayant son propre règlement, qui traitent de la protection de la vie privée aux niveaux fédéral, provincial et territorial (FPT). Seules trois administrations ont une législation distincte pour les municipalités : Ontario, Saskatchewan et Nouvelle-Écosse. Toutes les autres municipalités relèvent de leur législation provinciale respective sur *l'accès à l'information et la protection des renseignements personnels.*
- Un examen approfondi de la législation relative aux secteurs public et privé au Canada a indiqué que pour tirer pleinement parti de l'économie numérique et échanger des données à des fins administratives et non administratives, une réforme législative est nécessaire. La volonté politique, un examen obligatoire intégré de la législation et un commissariat à l'information et à la protection de la vie privée actif ont aidé certaines administrations à apporter des changements substantiels à leur législation liée au secteur public.

Recommandations

S'appuyant sur ces perspectives clés, les recommandations suivantes ont été proposées pour l'examen par l'ISAC et sont classées dans trois thèmes généraux :

Thème 1 : Comprendre les niveaux de confiance du public

A Communiquer directement avec le public de partout au Canada afin de mieux comprendre les niveaux d'acceptation de l'utilisation des données par le gouvernement.

B Encourager les administrations provinciales, territoriales ou municipales (PTM) à établir une surveillance officielle des niveaux d'acceptation par le public de l'utilisation et de l'échange des données par les Canadiens (en mettant l'accent sur la détermination des différences dans les niveaux d'acceptation entre les différentes régions géographiques, les centres urbains, ruraux, les petits centres et les groupes démographiques).

Thème 2 : Renforcement des relations entre le gouvernement et le public

C Appuyer le gouvernement à prendre des mesures précises pour promouvoir la transparence en vue de gagner ou de regagner la confiance.

D Encourager les gouvernements à permettre aux citoyens d'adopter l'approche « Une fois suffit », où les données peuvent être partagées avec d'autres ministères pour un ensemble d'utilisations convenues, conformément aux contextes législatifs du secteur public au Canada.

E Plaider pour que les organisations gouvernementales donnent la priorité à la souveraineté des données autochtones.

Thème 3 : Amélioration des opérations internes du gouvernement

F Encourager les gouvernements à établir des autorités centralisées responsables des données, en conformité avec les contextes législatifs du secteur public au Canada.

G Éduquer les fonctionnaires sur les renseignements qu'ils peuvent et ne peuvent pas échanger (utilisation secondaire) et les exigences en matière de consentement, conformément à la loi sur la protection des renseignements personnels de leur administration.

H Encourager et appuyer la réforme législative FPTM afin de permettre l'utilisation secondaire des données qui ne sont pas actuellement autorisées.

Toutes les recommandations sont décrites en détail à la section 6 du présent rapport.

02.

Contexte et aperçu du projet

Contexte et aperçu du projet_____

Le Groupe de travail sur les renseignements axés sur les données (GT RAD) travaille sous la direction des Conseils mixtes (le Conseil de prestation des services du secteur public [CPSSP] et le Conseil des dirigeants principaux de l'information du secteur public [CDPISP]) afin d'explorer le cadre des enjeux qui influent sur la capacité des gouvernements à améliorer l'expérience des clients, en s'appuyant sur les données ouvertes et l'analyse avancée des données pour améliorer la prestation des services.

Bien que les citoyens puissent être utilisés pour fournir des renseignements aux entités publiques afin de recevoir des biens et des services, ils ne sont pas nécessairement à l'aise de **ne pas** savoir où sont stockés leurs renseignements, avec qui elles sont partagées et comment elles sont [ou seront] utilisées. Nombre d'entre eux fournissent des renseignements sans même connaître l'étendue de l'utilisation de leurs renseignements sous les auspices d'une utilisation uniforme. Cette situation est particulièrement vraie pour les populations marginalisées et vulnérables, qui peuvent peut-être se concentrer sur leur propre soutien et celui de leur famille et moins sur la compréhension de leurs droits en vertu de la législation sur la protection de la vie privée.

Le sujet du consentement est complexe et compliqué davantage par la couverture et l'utilisation de concepts tels que le consentement *explicite* et *implicite* qui diffèrent dans leur application aux niveaux fédéral, provincial, territorial et municipal. Par exemple, les concepts de prestation de services tels qu'« Une fois suffit » dépendent du consentement éclairé et devraient être fournis pour être conformes aux lois applicables locales et nationales. Une analyse plus approfondie du consentement, quoique justifiée, ne relève pas de la portée du présent rapport. Toutefois, il serait instructif d'approfondir cette question lors d'une phase ultérieure de ce travail.

Il est essentiel de connaître le niveau d'acceptation par un citoyen de la portée de l'utilisation des renseignements par un organisme public pour concevoir un service efficace centré sur l'utilisateur. Cela crée un besoin pour les gouvernements auquel l'ISAC répond dans le cadre de ce projet, afin de mieux comprendre ce que le public pense des organisations du secteur public qui utilisent ses données.

En réponse à une demande des Conseils mixtes, le GT RAD a commandé l'élaboration de cette recherche afin d'examiner le contexte actuel de l'acceptation par le public de l'utilisation des données pour améliorer les services au sein et dans l'ensemble des ordres de gouvernements. Les connaissances acquises dans le cadre de cette recherche devraient contribuer à éclairer l'utilisation par les gouvernements canadiens des données sur les citoyens dans les programmes et services futurs. Elles serviront également de fondement à de futurs projets qui permettront de déterminer et de fournir des options pour surmonter les obstacles législatifs, stratégiques et ceux qui échangent des données pour concevoir, mettre en œuvre et offrir des services à l'échelle des gouvernements du Canada.

Une grande partie du contenu du rapport porte sur les attitudes, les innovations nécessaires et les tendances importantes relatives à l'échange des données. Il est important de prendre note que la portée de cette recherche se limite spécifiquement aux niveaux d'acceptation par les **citoyens** de l'échange des données du gouvernement. Les phases ultérieures de ce travail devraient consister à examiner l'utilisation des données sur les citoyens (et leur degré d'acceptation) par l'industrie, ainsi que les contraintes et les mesures de contrôle législatives existantes, pour assurer le contrôle et la transparence.

L'équipe de projet a abordé la réalisation de ce projet de recherche au cours de trois phases distinctes :

1. **Analyse des perspectives géographiques** à l'égard des approches visant à répondre à l'acceptation par le public de l'échange et de l'utilisation des données et des renseignements personnels afin d'améliorer la prestation des services gouvernementaux. Il s'agit notamment de consulter les comités fédéraux-provinciaux-territoriaux-municipaux canadiens qui peuvent s'occuper de questions semblables, et les administrations internationales susceptibles de faire face à ces enjeux ou d'aussi composer avec eux.
2. **Revue de la littérature** des recherches universitaires et d'opinion publique en cours sur l'acceptation par le public et la confiance du public en ce qui concerne l'utilisation de données et des renseignements personnels pour la prestation de services gouvernementaux. Cela comprend l'identification d'écarts importants entre les lieux géographiques ou les groupes démographiques, et porte également sur l'examen des attitudes au sein des populations vulnérables et minoritaires.
3. **Aperçu des principales lois** régissant la collecte, l'utilisation et la communication de renseignements personnels dans les provinces, territoires et municipalités et le gouvernement du Canada. Des similitudes clés et des différences notables dans la collecte, l'utilisation et la communication au sein des administrations et à d'autres administrations sont relevées, ainsi que des modifications apportées à la législation pour faciliter l'échange de données. Un examen des pratiques exemplaires dans certaines administrations internationales est également inclus.

Les renseignements recueillis dans le cadre de ce projet sont nécessaires pour éclairer l'orientation future entourant l'utilisation de données intergouvernementales au Canada. Il fournira également du matériel de base pour un projet ultérieur qui permettra d'étudier et de définir les options permettant de surmonter des obstacles législatifs, stratégiques et relatifs aux données à l'égard de la prestation de services intégrés et harmonieux dans l'ensemble des ordres du gouvernement.

Par conception, ce projet est motivé par le besoin d'une meilleure intégration et d'un meilleur échange des renseignements au sein des administrations et entre elles, tout en tenant compte des attitudes des citoyens à l'égard de cet échange de renseignements personnels et de l'acceptation de ceux-ci. **Même si le présent rapport peut porter sur l'utilisation des données pour les canaux numériques, il est essentiel que les services soient toujours conçus pour être mis à la disposition de ceux qui n'ont pas d'accès en ligne ou au numérique, tels que les populations vulnérables et marginalisées.**

03.

Analyse des perspectives géographiques

Analyse des perspectives géographiques _____

Principales perspectives

- Les commissaires à l'information et à la protection de la vie privée (CIPVP) et les bureaux d'accès à l'information et de protection de la vie privée (AIPVP) gouvernementaux des 13 provinces et territoires, ainsi que huit dirigeants principaux du numérique (DPN), ont été invités à émettre des commentaires pour le présent rapport.
    - Les répondants provenaient de 5 bureaux de CIPVP, 12 bureaux d'AIPVP gouvernementaux et 5 bureaux de DPN qui ont accepté de rencontrer ou de fournir une rétroaction par écrit.
- **Parmi les intervenants qui ont répondu :**

  Plus de 50 % n'étaient au courant d'aucun ministère ou organisme provincial qui surveille officiellement l'acceptation par le public de l'utilisation des données par le gouvernement.

  Moins de 50 % mesurent l'opinion publique sur l'utilisation des données d'un projet à l'autre.

  Plus de 50 % ont indiqué que la confiance du public dans le gouvernement (en général) a augmenté depuis le début de la pandémie. Toutefois, **plus de 33 %** ont indiqué que la méfiance du public à l'égard de l'utilisation des données par le gouvernement pendant la pandémie s'est accrue.

  Environ 25 % des répondants ont indiqué que la perception selon laquelle le gouvernement utilise les données pour des utilisations secondaires sans consentement était une préoccupation majeure pour le public.

  Environ 20 % ont indiqué que la population en a assez d'avoir à fournir ses renseignements à plusieurs reprises au gouvernement.

- Les consultations et les recherches menées dans le cadre du présent rapport ont permis de dégager 11 perspectives, regroupées selon cinq thèmes :

Thème 1 : Sensibilisation du gouvernement à l'acceptation par le public

1.1 Plus de la moitié des intervenants que nous avons interviewés n'étaient pas au courant que les organismes gouvernementaux surveillaient officiellement l'acceptation par le public de l'utilisation de ses données.

1.2 Malgré un manque généralisé de surveillance formelle, la plupart des administrations recueillent tout de même des renseignements sur la perception du public auprès de diverses sources.

1.3 Certaines administrations envisagent d'instaurer une surveillance de l'acceptation par le public.

Thème 2 : Enjeux les plus préoccupants pour le public

2.1 Il semble y avoir deux enjeux qui préoccupent grandement le public : une perception selon laquelle le gouvernement utilise les renseignements publics à des fins secondaires non communiquées, et une frustration quant à l'obligation de fournir les mêmes renseignements à plusieurs reprises au gouvernement.

2.2 La technologie de reconnaissance faciale est une préoccupation publique dans certaines administrations, mais pas dans d'autres.

Thème 3 : Changement au niveau d'acceptation par le public

3.1 Les effets de la pandémie de la COVID-19 variaient considérablement, allant de l'acceptation accrue de l'utilisation des renseignements par le gouvernement à une perte de confiance envers le gouvernement.

Thème 4 : Tendances géographiques

- **4.1** Les préoccupations du Commissariat à l'information et de la protection de la vie privée (CIPVP) varient d'un endroit à l'autre au pays.
- **4.2** Les citoyens qui se font le plus entendre au sujet des préoccupations relatives à la protection de la vie privée varient d'une administration à l'autre et à l'intérieur des administrations.
- **4.3** L'intérêt du public pour la protection des renseignements personnels s'est accru dans l'ensemble du pays au cours des dernières années.

Thème 5 : Obstacles

- **5.1** Il peut s'avérer difficile d'établir des initiatives d'échange de données au sein du gouvernement.
- **5.2** La volonté politique est essentielle au succès des initiatives de données ouvertes.

Ces 11 perspectives sont expliquées en détail ci-dessous, ainsi que le soutien de la recherche documentaire.

Approche

Un examen des approches et des projets des administrations canadiennes portant sur l'acceptation par le public de l'utilisation des données et de l'échange de renseignements personnels afin d'améliorer la prestation des services a été effectué.

Le groupe initial d'intervenants désignés pour une consultation directe, en fonction de leur exposition prévue au public, était constitué des commissaires à l'information et à la protection de la vie privée (CIPVP) et des bureaux d'accès à l'information et de protection de la vie privée (AIPVP) gouvernementaux des 13 provinces et territoires. Vers la fin de la période de recherche, les bureaux de huit dirigeants principaux du numérique (DPN) à l'échelle du Canada ont reçu un sondage en fonction des questions posées lors de consultations directes afin d'aider à renforcer les résultats de cette analyse.

Dans l'ensemble, cinq des treize CIPVP, tous sauf un bureau d'AIPVP gouvernemental, et cinq DPN ont accepté de nous rencontrer ou de fournir une rétroaction par écrit. Sur les cinq DPN qui ont répondu, deux étaient disponibles pour une consultation de suivi. (Une liste complète d'administrations qui participent aux consultations figure à l'annexe B.)

Afin de faciliter une mobilisation uniforme et complète, un ensemble de questions standards a été préparé et utilisé pour toutes les entrevues. Cette série de questions a également servi de fondement au sondage envoyé aux DPN. Cet ensemble de questions visait à déterminer si le public acceptait l'utilisation par le gouvernement des types de données ou de renseignements suivants :

- l'échange de renseignements personnels à des fins administratives comme pour l'authentification ou la vérification à l'appui de la prestation de services aux clients;
- l'utilisation de données et de renseignements relatifs aux services à des fins non administratives, comme l'évaluation de programme ou l'analyse statistique, y compris l'utilisation de nouvelles technologies et méthodes de l'intelligence artificielle.

En plus des administrations canadiennes consultées, d'autres recherches sur le Web ont été menées sur des initiatives entreprises par des administrations canadiennes et certaines administrations internationales pour améliorer la confiance du public dans l'utilisation des données et faciliter un meilleur échange des données au sein du gouvernement et par celui-ci. Le critère de sélection des administrations internationales était opportuniste : il incluait celles spécifiquement relevées par l'ISAC lors des premières étapes du projet, ainsi que celles qui ont attiré l'attention de l'équipe de projet au cours de ses recherches pour le présent rapport.

Une liste complète de toutes les sources utilisées pour effectuer l'analyse géographique figure à l'annexe C.

Perspectives

Les consultations et les recherches menées dans le cadre du présent rapport ont permis de dégager 11 perspectives clés, organisées selon cinq thèmes :

Thème 1 : Sensibilisation du gouvernement à l'acceptation par le public

1.1 Plus de la moitié des intervenants que nous avons interviewés n'étaient pas au courant que les organismes gouvernementaux surveillaient officiellement l'acceptation par le public de l'utilisation de ses données.

Un intervenant a cité l'insuffisance des ressources comme facteur déterminant dans la décision de ne pas surveiller la perception du public au sein de son organisation. Un autre intervenant a indiqué qu'il n'était pas certain de la façon dont il allait sonder les citoyens. Bien que certaines administrations suivent le nombre de plaintes déposées au sujet du gouvernement, cela ne met pas nécessairement en corrélation directe avec l'acceptation du public.

Bien qu'il ne s'agisse pas d'un exemple de surveillance de l'acceptation de l'utilisation des données en soi, la Nouvelle-Zélande est un gouvernement qui surveille officiellement la confiance du public.

Exemple : Nouvelle-Zélande

Le gouvernement néo-zélandais surveille activement les niveaux de confiance envers le gouvernement — à la fois par la collecte de données longitudinales continue et des études à un instant précis. Le sondage Kiwis Count sur la confiance du public mesure la confiance des Néo-Zélandais dans le gouvernement. Le sondage est mené tous les trimestres auprès de 1 000 personnes et aide le gouvernement à améliorer les services qu'il offre. Les résultats sont communiqués au public et sont transmis aux organismes afin de les aider à cerner les domaines où des problèmes pourraient se poser et où des mesures correctives pourraient être nécessaires. Le sondage donne au gouvernement un aperçu utile des opinions des Néo-Zélandais, de leur confiance envers le gouvernement et du rôle de celui-ci dans la société.

En avril 2021, les principales mesures étaient les suivantes :

- 79 % des Néo-Zélandais font confiance aux services publics en fonction de leur expérience personnelle.
- La confiance envers l'image de marque du secteur public est de 63 %, en baisse par rapport à son dernier sommet de 69 %.
- La confiance envers l'image de marque du secteur privé est de 50 %, en hausse par rapport à 48 % et un nouveau sommet.

(Source : http://publicservice.govt.nz/our-work/kiwis-count-survey/ with historical reporting available at https://www.publicservice.govt.nz/our-work/kiwis-count-survey/kiwis-count-archive-including-the-survey-methodology/)

1.2 Malgré un manque généralisé de surveillance formelle, la plupart des administrations recueillent tout de même des renseignements sur la perception du public auprès de diverses sources.

Près de la moitié des intervenants interrogés ont indiqué qu'ils mesuraient l'opinion publique en fonction des projets, par exemple, lors de consultations publiques sur une politique ou une initiative législative. De plus, un intervenant nous a également dit qu'il surveillait formellement la perception du public sur l'utilisation par les entreprises privées de ses données et qu'il tirait des conclusions sur ce que cela pourrait signifier pour le gouvernement.

Parmi les autres tactiques courantes, mentionnons l'analyse secondaire de la correspondance publique et des questions présentées au gouvernement, et la surveillance des communiqués de presse et d'autres publications. Le rapport annuel du Commissariat à l'information et de la protection de la vie privée s'avère particulièrement utile.

Exemple : Colombie-Britannique

La Colombie-Britannique a réalisé des activités publiques périodiques au cours des dernières années concernant l'accès à l'information et la protection des renseignements personnels. Voici des exemples de participation du public :

- Été 2021 — Les Britanno-Colombiens ont été invités à donner leur avis sur les lois provinciales sur la protection des renseignements personnels dans le secteur public concernant la résidence, les frais et d'autres enjeux.
- Été 2021 — Les dirigeants des Premières Nations ont été invités à remplir un questionnaire en ligne afin d'obtenir les points de vue propres aux Autochtones sur l'accès à l'information et la protection de la vie privée.
- Printemps et été 2021 – Le ministre responsable de la *Freedom of Information and Protection of Privacy Act* (FOIPPA) a tenu un certain nombre de tables rondes avec des groupes d'intervenants.
- Été 2021 — Nous avons tenu une activité de discussion ciblée avec des intervenants et des titulaires de droits sur la collecte de données fondées sur la race par le gouvernement.
- Automne 2019 – Nous avons tenu une table ronde des citoyens sur l'utilisation par le gouvernement des renseignements personnels sur la santé (animée par PopData BC).
- 2018 — Nous avons invité les Britanno-Colombiens à contribuer à la conception des prochaines étapes du gouvernement en ce qui concerne la FOIPPA et avons demandé aux personnes de discuter d'enjeux comme les pénalités pour les contraventions à la FOIPPA, les frais d'accès à l'information et les genres d'information qu'ils aimeraient voir le gouvernement rendre disponible sans qu'ils aient à présenter une demande officielle d'accès à l'information.
- Printemps 2018 – Le ministre responsable de la FOIPPA a tenu un certain nombre de tables rondes avec des groupes d'intervenants.

1.3 Certaines administrations envisagent d'instaurer une surveillance de l'acceptation par le public

Plusieurs administrations cherchent activement à mettre en place des mécanismes pour surveiller l'acceptation par le public de l'utilisation des données gouvernementales. Les exemples comprennent un comité de citoyens peut être utilisé pour mener des recherches proactives, un conseil municipal intelligent composé de membres du public et des sondages d'opinion publique courants. Ces mécanismes pourraient également appuyer l'élaboration d'initiatives stratégiques et aider à évaluer la confiance du public envers le gouvernement en général.

Thème 2 : Enjeux les plus préoccupants pour le public

2.1 Il semble y avoir deux enjeux qui préoccupent grandement le public : une perception selon laquelle le gouvernement utilise les renseignements publics à des fins secondaires non communiquées et une frustration quant à l'obligation de fournir les mêmes renseignements à plusieurs reprises au gouvernement.

De toutes les préoccupations du public dont nous ont parlé les intervenants, il y en avait deux qui se sont distinguées parce qu'elles sont communes à toutes les administrations.

Environ un quart des intervenants que nous avons interrogé ont indiqué que l'une des principales préoccupations de leur administration est la perception selon laquelle le gouvernement utilise l'information à des fins secondaires, ce à quoi le public n'a pas consenti. Parmi les perceptions, mentionnons celle selon laquelle l'information publique est librement partagée entre les ministères, ou même avec le secteur privé. Les intervenants nous ont dit que les collectivités marginalisées de certaines provinces et de certains territoires peuvent être particulièrement préoccupées par cette question et qu'elles éprouvent certains des plus faibles niveaux de confiance envers le gouvernement. Dans l'ensemble, nous avons entendu dire que le public aimerait davantage de transparence gouvernementale, notamment l'approche « ouverte par défaut » concernant les fins en vertu de l'autorisation de la collecte des renseignements.

Un intervenant nous a également signalé que le public semble plus préoccupé par l'utilisation de l'information par le gouvernement que le secteur privé. Certains citoyens peuvent ne pas comprendre les avantages que l'échange de données peut offrir, y compris une meilleure prestation de services.

Une autre préoccupation importante, exprimée par environ le cinquième des intervenants, est que le public ne veut pas fournir plusieurs fois au gouvernement les mêmes renseignements. Les intervenants nous ont dit que le public réclame une meilleure intégration des données et l'approche « Une fois suffit ».

Ces deux préoccupations peuvent être perçues comme paradoxales — et répondre aux deux pourrait s'avérer difficile. D'une part, le public cherche à obtenir l'assurance que leurs renseignements ne sont utilisés que par le gouvernement à des fins précises, et d'autre part, les gens veulent une meilleure intégration des données et sont disposés à consentir à un plus grand échange de renseignements entre les ministères. La transparence du gouvernement sera essentielle pour répondre à ces deux préoccupations et les réconcilier.

D'autres préoccupations du public dont on nous a fait part, qui étaient moins communes dans l'ensemble des administrations, se divisent en trois catégories principales : la gestion de l'information publique, la confiance et la responsabilisation, et la pandémie de la COVID-19 :

1. Gestion de l'information publique

- Comment la sécurité de l'information publique est assurée.
- Comment les gens peuvent accéder à leurs propres renseignements.
- Demandes d'accès tardif à l'information tardive.

2. Confiance et responsabilisation

- Méfiance à l'égard des forces de l'ordre, en particulier à la suite de certains incidents violents.
- Souveraineté des données autochtones
- Méfiance à l'égard de l'utilisation par le gouvernement de la technologie de reconnaissance faciale.

Exemple : Ontario

La souveraineté des données autochtones a toujours suscité des préoccupations quant à l'utilisation de l'information publique — ou même de données agrégées — pour appuyer la prestation des services. Les populations qui ont été historiquement exclues ou ciblées négativement avaient des préoccupations quant aux effets de la prise de décisions automatisée. En Ontario, une autorité de données qui suit les lignes directrices du Centre de gouvernance de l'information des Premières Nations est en voie d'être créée pour superviser la collecte et l'utilisation des données. Elle aidera également à faire en sorte que les technologies axées sur les données profitent aux populations autochtones.

- Préoccupations quant à la possibilité d'identifier les citoyens à partir de données qui devraient être anonymisées.

3. Pandémie de la COVID-19

- La réponse du gouvernement à la pandémie de la COVID-19, qui, selon certaines personnes, a été précipitée et n'a pas tenu compte des considérations liées à la protection de la vie privée.
- Passeports vaccinaux et question de savoir s'ils enfreignent les considérations de confidentialité.
- Mauvais traitement des citoyens et des employés dans les établissements de soins de longue durée.
- Applications de suivi de contacts qui surveillent le mouvement des personnes.

Exemple : Nouveau-Brunswick

Puisque le Nouveau-Brunswick est une petite province, les régions rurales et les codes postaux ont le potentiel de localiser les participants. Des citoyens se sont dits préoccupés de voir leur point de vue associé à leur lieu de résidence, par exemple en fournissant un code postal avec une réponse au sondage.

2.2 La technologie de reconnaissance faciale est une préoccupation publique dans certaines administrations, mais pas dans d'autres.

Les intervenants de deux administrations ont mentionné expressément que la technologie de reconnaissance faciale est une préoccupation publique clé, particulièrement en ce qui concerne la délivrance des permis de conduire et la façon dont les données de reconnaissance faciale sont stockées et utilisées. Un intervenant estimait que la préoccupation résulterait probablement d'une méconnaissance de la technologie, de son fonctionnement et de ce à quoi elle peut servir.

En revanche, les intervenants de trois administrations nous ont signalé que la reconnaissance faciale n'est pas un sujet de préoccupation pour le public ou qu'elle n'est qu'une question secondaire. Ces administrations peuvent être moins avancées que d'autres dans leur utilisation de la technologie, ce qui entraîne une exposition et une prise de conscience du public moindres. D'autre part, les gens de ces administrations peuvent être plus habitués à la technologie de reconnaissance faciale et donc moins préoccupés.

Thème 3 : Changement au niveau d'acceptation par le public

La vaste majorité des intervenants ont discuté du changement quant à l'acceptation du public dans le contexte de la pandémie de la COVID-19. Cette acceptation peut s'expliquer par le fait que la plupart des administrations ne surveillent pas officiellement les niveaux d'acceptation, en plus du fait que la pandémie a entraîné des répercussions si importantes sur le gouvernement et le public en général.

3.1 Les effets de la pandémie de la COVID-19 variaient considérablement, allant de l'acceptation accrue de l'utilisation des renseignements par le gouvernement à une perte de confiance envers le gouvernement.

Plus de la moitié des intervenants que nous avons interviewés nous ont signalé que la confiance du public dans le gouvernement s'est accrue dans leur administration depuis le début de la pandémie de la COVID-19. Ils nous ont dit que les citoyens veulent maintenant interagir davantage avec le gouvernement en ligne, y compris pour

ce qui est des exigences en matière de délivrance des permis de conduire, de l'accès aux services de santé, de l'inscription en tant que donneur d'organismes et de tissus et de la mise à jour administrative de leurs renseignements personnels.

Les intervenants nous ont également dit que le public s'intéresse de plus en plus à une intégration plus transparente des données dans l'ensemble des ministères, par exemple par une identité numérique unique. Plusieurs intervenants ont cité un large soutien à l'égard d'un passeport vaccinal électronique dans leur administration.

Exemple : Nouveau-Brunswick

Le public du Nouveau-Brunswick n'a guère eu de réticence à l'égard de la collecte de renseignements supplémentaires pendant la pandémie. Bien que les enregistrements obligatoires des voyageurs à la frontière aient d'abord suscité l'attention du public, la principale préoccupation était les inconvénients plutôt que le manque de confiance. Cette réaction est peut-être attribuable à une population plus âgée et plus obéissante qui fait plus confiance au gouvernement que les jeunes.

D'autre part, plus d'un tiers des intervenants nous ont indiqué que la méfiance envers le gouvernement s'est accrue depuis la pandémie. Ils nous ont dit que les préoccupations du public se sont accrues en général et que la confiance s'est érodée, en partie en raison de la collecte accrue d'information gouvernementale pour les registres de vaccins et les passeports vaccinaux. Un intervenant nous a dit que les habitants de leur administration estimaient que l'approche du gouvernement à l'égard de la pandémie était trop précipitée et qu'elles craignaient que des changements majeurs aient été apportés aux politiques dans une situation d'urgence. Un autre intervenant a discuté des enjeux éthiques perçus concernant l'utilisation des centres d'isolement liés à la COVID-19.

De plus, nous avons appris que, bien que le public souhaite que les services du gouvernement correspondent à leur façon de vivre, il s'inquiète de la facilité qu'il y aura à violer leur vie privée. En réponse à ces préoccupations, une administration ralentit l'utilisation de l'analyse pour éclairer les décisions stratégiques et une autre a fait de la protection de la vie privée un élément prioritaire à l'échelle du gouvernement.

Même au sein d'une seule administration, les intervenants nous ont dit que le public avait des attitudes très divergentes à l'égard du gouvernement. Les passeports vaccinaux ont été cités comme un exemple d'un sujet particulièrement polarisant.

Exemple : Saskatchewan

Selon un récent sondage, une minorité de résidents de la Saskatchewan sont disposés à échanger leurs renseignements personnels en ligne afin de simplifier leur expérience de service. Les répondants étaient également très préoccupés que leurs renseignements personnels puissent être compromis en ligne.
En outre, deux groupes de répondants sont extrêmement préoccupés par la compromission de l'information : ceux qui sont très disposés à échanger des renseignements et ceux qui sont très opposés à l'échange de l'information. Cette constatation laisse entendre que les résidents qui communiquent librement leur information pour des raisons de commodité reconnaissent les risques de le faire, mais qu'ils sont tout de même disposés à les accepter pour éviter les tracas.

Environ 7 Canadiens sur 10 (69 %) ont indiqué que leur point de vue sur la protection de la vie privée et de leurs renseignements personnels n'avait pas changé depuis le début de la pandémie de la COVID-19, en mars 2020. En revanche, 1 personne sur 3 (29 %) a déclaré que son point de vue avait changé depuis mars 2020.

Les Canadiens du Canada atlantique (59 %) et de l'Ontario (55 %) étaient plus susceptibles de se dire plus préoccupés par la protection des renseignements personnels maintenant qu'ils ne l'étaient avant la pandémie de la COVID-19. Cependant, les résidents du Québec (49 %) et des Prairies (50 %) étaient plus susceptibles de se dire plus sensibilisés au moment de communiquer des renseignements personnels.

Figure 1 : *Les préoccupations des citoyens canadiens au sujet de la protection des renseignements personnels pendant la pandémie de la COVID-19*[1].

Thème 4 : Tendances géographiques

4.1 Les préoccupations du Commissariat à l'information et de la protection de la vie privée (CIPVP) varient d'un endroit à l'autre au pays

Nous avons entendu parler d'un éventail de préoccupations différentes du CIPVP, qui varient à l'échelle du pays. Aucune préoccupation n'a été exprimée par la majorité ou une proportion importante des personnes interrogées. Voici les préoccupations que nous avons entendues :

[1] *Source :* Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée de 2020-2021 — Commissariat à la protection de la vie privée du Canada, https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2021/por_2020-21_ca/

- Partialité à l'égard de l'intelligence artificielle, de l'analyse prédictive, des algorithmes, en particulier lorsqu'ils désavantagent les groupes minoritaires.
- Méfiance envers les entreprises privées et leur utilisation de l'information publique.
- Utilisation des dossiers de vaccination dans les passeports vaccinaux.
- L'effet mosaïque, où sont agrégées des sources de données disparates, provenant en grande partie de l'extérieur du secteur public, afin de désanonymiser des personnes anonymisées autrement.
- Tactiques de surveillance de l'État, y compris la vidéo, l'utilisation de la caméra d'intervention, la notification de l'exposition, la technologie de reconnaissance faciale et la biométrie.
- Manque de clarté et de transparence du gouvernement, y compris les avis en langage clair et les formulaires de consentement.

Malgré le fait que les gouvernements peuvent recueillir trop d'information publique, nous avons observé une reconnaissance générale que cela ne sera probablement pas à des fins malveillantes.

4.2 Les citoyens qui se font le plus entendre au sujet des préoccupations relatives à la protection de la vie privée varient d'une administration à l'autre et à l'intérieur des administrations.

Dans une juridiction, on nous a dit que les groupes soucieux de la protection de la vie privée sont plus susceptibles de correspondre avec le gouvernement que les citoyens individuels, qui prennent rarement contact. Dans une autre administration, les personnes d'âge moyen sont responsables de la plus grande partie de la correspondance avec le gouvernement. Un troisième intervenant nous a indiqué que, dans son administration, les populations rurales sont plus susceptibles d'exprimer des préoccupations concernant les questions de vie privée que les citadins.

Exemple : Ontario

Le CIPVP a demandé que 26 mesures concernant la vie privée, la sécurité, l'accès et la responsabilisation soient intégrées dans un cadre de gouvernance robuste pour les caméras d'intervention. Le Conseil et le Service ont abordé complètement ou de façon importante la plupart de ces recommandations et ont convenu de donner suite aux points restants. Le cadre qui s'est dégagé permettra de répondre aux besoins du public en matière de transparence et de responsabilisation tout en respectant les attentes raisonnables en ce qui concerne la protection de la vie privée. En s'appuyant sur cette expérience et sur l'apport d'autres intervenants clés, le CIPVP est à élaborer un cadre de gouvernance complet des caméras d'intervention, qui pourrait servir de modèle à tous les autres services de police qui utilisent ou envisagent d'utiliser les programmes de caméras d'intervention en Ontario, contribuant ainsi à assurer l'uniformité dans l'ensemble de la province.

4.3 L'intérêt du public pour la protection des renseignements personnels s'est accru dans l'ensemble du pays au cours des dernières années

Les intervenants de toutes les administrations ont observé une augmentation de l'intérêt du public envers la protection de la vie privée, y compris une augmentation exponentielle des demandes de renseignements au cours des dernières années. Ce phénomène peut être attribuable au développement de nouvelles technologies entraînant des répercussions sur la vie privée et à l'augmentation de la couverture médiatique sur les questions de protection de la vie privée. Malgré l'intérêt public croissant, nous avons aussi appris que la plupart des

citoyens semblent mal comprendre les complexités de la législation sur la protection de la vie privée, notamment ce que le gouvernement peut et ne peut pas faire de l'information publique.

En complément de cette idée, le rapport « Étude canadienne sur l'identité numérique 2020 » établi par le Conseil canadien de l'identification et l'authentification numériques (CCIAN) a révélé que la familiarité avec l'identité numérique est plus élevée en Ontario, au Manitoba et en Saskatchewan. Les Albertains étaient ceux qui étaient les plus favorables au concept d'identité numérique. Comparativement à d'autres régions, le Québec demeure le moins préoccupé en ce qui a trait à la communication en ligne de renseignements personnels qui les concernent, et il est plus probable que les résidents considèrent qu'il est très important que leur gouvernement provincial passe rapidement à l'identité numérique[2].

À l'échelle nationale, l'Institut canadien de recherches avancées (ICRA) dirige la Stratégie pancanadienne d'intelligence artificielle (IA) du gouvernement du Canada, qui s'élève à 125 millions de dollars, en partenariat avec trois instituts provinciaux de l'IA, l'Alberta Machine Intelligence Institute, Mila à Montréal et l'Institut Vector à Toronto. Annoncée dans le budget fédéral de 2017, la stratégie a quatre grands objectifs : 1) accroître le nombre de chercheurs exceptionnels et de diplômés compétents dans le domaine de l'IA au Canada; établir des nœuds d'excellence scientifique interconnectés dans les trois principaux centres d'IA; créer un leadership intellectuel mondial sur les répercussions économiques, éthiques, stratégiques et juridiques des percées en IA; appuyer une collectivité nationale de recherche en IA. Les implications de cette initiative sur l'utilisation des renseignements personnels par le gouvernement sont importantes. À mesure que s'accroîtra le leadership éclairé et la capacité de travailler dans le domaine de l'IA, les applications de l'IA aux programmes et services offerts par le gouvernement évolueront. Ainsi, un besoin accru de données et d'information sera nécessaire pour l'élaboration et le peaufinage d'algorithmes et d'autres principes de l'IA. Proportionnellement à cette innovation, il sera nécessaire que les lois évoluent pour réglementer le développement et l'utilisation de l'IA sur les renseignements personnels.

Thème 5 : Obstacles à l'échange des données

5.1 Il peut s'avérer difficile d'établir des initiatives d'échange de données au sein du gouvernement

[2] *Source :* Étude canadienne sur l'identité numérique 2020, réalisée par le CCIAN

Les intervenants de quatre administrations nous ont indiqué que les initiatives d'échange de données sont généralement difficiles à mettre en place au gouvernement, malgré l'acceptation généralisée qu'elles sont essentielles à la prestation de services publics sans faille. L'ambiguïté autour de la définition des autorisations, ainsi que de la capacité à surmonter les restrictions législatives et les cloisonnements structurels des gouvernements, ont été désignés comme des défis qui y contribuent. Nous avons également appris que les administrations qui n'assurent pas de surveillance ou de leadership centralisés en matière de protection de la vie privée estiment que l'échange de données entre les ministères particulièrement est difficile.

Des intervenants de quatre administrations nous ont aussi signalé qu'il peut s'avérer difficile de savoir combien de temps dure le consentement à l'information publique ou le moment où le consentement global a été donné. Cette situation a une incidence sur la façon dont on peut les échanger au sein des ministères et entre eux, surtout si de nouvelles initiatives sont mises en place après la collecte des données.

Example : Nunavut

La collecte de données et la communication significative auprès de la population peuvent s'avérer difficiles au Nunavut, où les collectivités sont dispersées géographiquement sur une grande superficie. À certains endroits, la mauvaise connexion à Internet est une contrainte de plus. Cette situation peut se traduire par un manque de données ou une représentation inexacte des enjeux clés, qui peut influer sur la qualité des données disponibles.

5.2 La volonté politique est essentielle au succès des initiatives de données ouvertes

Nous avons appris que les initiatives relatives aux données ouvertes et à l'échange de données nécessitent un appétit politique continu pour réussir. Un intervenant a précisé que le changement politique au cours des cycles électoraux a perturbé les progrès d'une initiative de données ouvertes.

Autre recherche documentaire

La section suivante présente un résumé de la recherche documentaire qui met en lumière les mesures prises par le gouvernement, le secteur privé et les organismes sans but lucratif pour accroître la confiance du public envers l'utilisation des données. Elle porte principalement sur les administrations canadiennes, mais comprend également plusieurs pratiques internationales de premier plan exercées en Australie, en Estonie, au Royaume-Uni et en Nouvelle-Zélande.

Amélioration des possibilités de relèvement des compétences relatives au gouvernement numérique

Le relèvement des compétences dans le domaine du gouvernement numérique s'accroît partout au Canada, comme en témoignent les trois exemples ci-dessous. C'est essentiel pour encourager une confiance accrue du public envers le gouvernement.

1. **École de la fonction publique du Canada**

   L'École de la fonction publique du Canada élabore actuellement un plan directeur pour l'Académie du numérique qui peut être recréée dans les régions canadiennes en mettant fortement l'accent sur les partenariats avec les gouvernements provinciaux et municipaux, les établissements d'apprentissage (universités et collèges) et le secteur privé. Elle collabore également avec le Bureau des partenariats

de la Communauté des politiques afin de déterminer la littératie en matière de numérique et de données au sein des collectivités de la TI et des politiques.

2. **Affaires mondiales Canada**

   Affaires mondiales Canada a mis au point un programme pilote de formation en analyse des données dans le cadre de sa stratégie globale en matière de données afin d'accroître la capacité des employés à utiliser davantage les données dans l'élaboration de politiques fondées sur des données probantes.

3. **Statistique Canada**

   Statistique Canada travaille en étroite collaboration avec 12 établissements d'enseignement qui ont mis sur pied des programmes de chercheurs et de spécialistes en données afin de rechercher des scientifiques en données dans le cadre de leur stratégie ministérielle de ressources humaines. L'organisme offre également des centres de données de recherche comme lieu de collaboration avec la collectivité des sciences des données pour expérimentation et innovation. (Rapport au greffier du Conseil privé : Feuille de route de la Stratégie en matière de données pour la fonction publique fédérale)[3]

Adoption d'une approche pancanadienne de l'identité numérique sûre et sécuritaire

Le Secrétariat du Conseil du Trésor du Canada (SCT) travaille avec Innovation, Sciences et Développement économique Canada (ISDE) et d'autres ministères et administrations afin d'élaborer une approche pancanadienne à l'égard de l'identité numérique et de l'acceptation d'identités numériques de confiance dans l'ensemble des administrations et du gouvernement. L'objectif est de permettre aux Canadiens et aux entreprises canadiennes d'ouvrir une session avec leur identité numérique provinciale fiable afin d'accéder aux services du gouvernement fédéral en temps opportun et de façon sécuritaire. Le SCT a de plus élaboré une d'évaluation de l'incidence algorithmique pour aider à évaluer et à atténuer les risques associés au déploiement d'un système décisionnel automatisé[4].

La *Directive sur la prise de décisions automatisée* du Conseil du Trésor est un instrument de politique obligatoire qui s'applique à la plupart des institutions fédérales. Elle énonce les exigences auxquelles doivent satisfaire les institutions fédérales pour assurer l'utilisation responsable et éthique des systèmes décisionnels automatisés, y compris celles qui utilisent l'IA[5]. Des normes permettant l'interopérabilité et la reconnaissance entre les ministères fédéraux, les provinces, les territoires, les municipalités et les partenaires de l'industrie rendront cela possible.

Interopérabilité et normes

Le Cadre de confiance pancanadien (CFP) établit un ensemble de critères et de lignes directrices afin de veiller à ce que les secteurs public et privé se conforment à des règles communes, mutuellement acceptées pour faire confiance et accepter les identités numériques des uns et des autres[6]. Les gouvernements fédéral, provinciaux et territoriaux continuent de travailler ensemble à l'élaboration du Profil du secteur public du CFP afin d'évaluer les programmes d'identité numérique et d'accepter les identités numériques fiables émises par ces

[3] Source : https://www.canada.ca/fr/conseil-prive/organisation/greffier/publications/strategie-donnees.html
[4] *Source :* Trusted Digital Transformation Considerations for Canadian Public Policy, janvier 2019
[5] *Source :* https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592
[6] *Source :* Digital-ID-General-with-CIOSC-Standard-Draft (EN)

programmes d'identité numérique, ce qui améliorera la prestation des services aux Canadiens. De plus, le Conseil canadien de l'identification et l'authentification numériques (CCIAN) continue de déployer des outils et des processus du PCF pour appuyer plus largement l'ensemble de l'économie. En outre, des cadres fiables dans d'autres contextes nationaux, comme l'Union européenne, le Royaume-Uni et ailleurs, continuent d'émerger.

L'établissement de normes d'identité numérique a progressé au Canada. En juillet 2020, le Conseil canadien des normes (CCN) a approuvé la première édition de CAN/CIOSC 103-1 : Confiance numérique et de l'identité en tant que norme volontaire nationale pour le Canada. En février 2021, le CCN a lancé une demande de proposition (DP) visant à élaborer une spécification technique nationale pour les justificatifs d'identité numériques et les portefeuilles numériques.

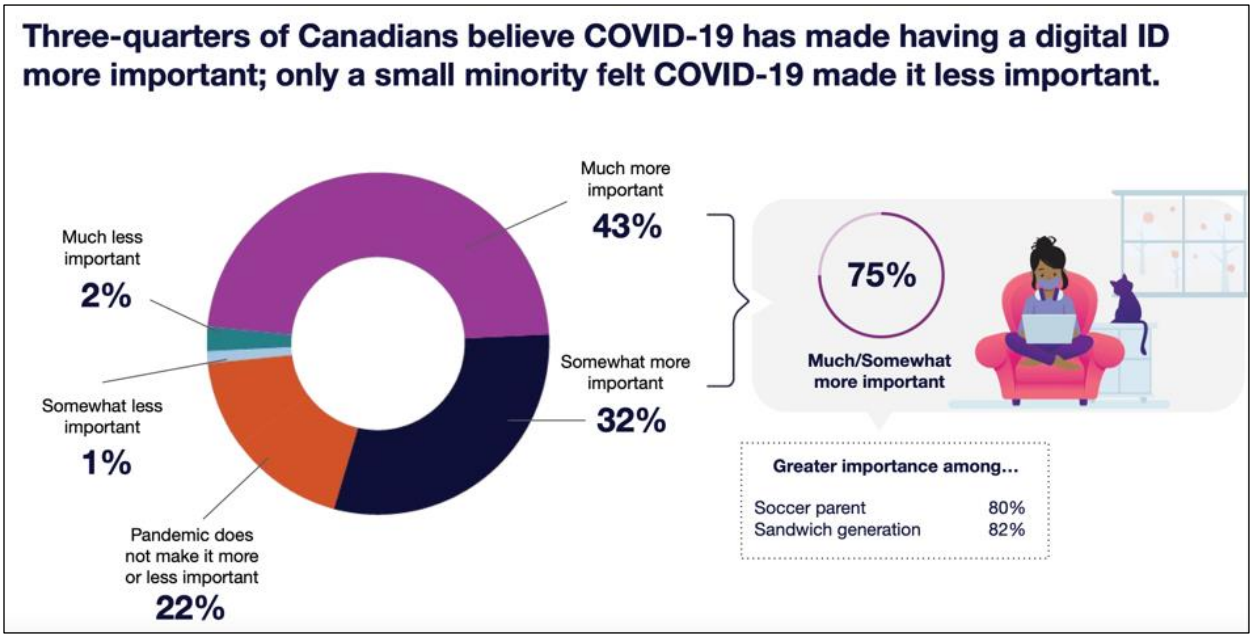


Figure 2 : *L'intérêt des citoyens canadiens d'avoir une carte d'identité numérique*[7]

Australie

Trois millions d'Australiens et la moitié de toutes les entreprises australiennes utilisent maintenant l'identité numérique. Elle est intégrée dans toutes les administrations dans le système d'identité numérique de la Nouvelle-Zélande, et d'autres pays comme Singapour suivront. Pour établir la confiance du public, l'Australie s'est concentrée sur le fait que l'identité numérique est volontaire, qu'elle exige un consentement éclairé et avisé et que la minimisation des données est envisagée partout.

Le Digital Transformation Office (DTO) a également appliqué une approche de conception de services axée sur l'utilisateur à ce travail, ce qui a consisté entre autres à prendre le point de vue de quelqu'un de l'extérieur

[7] *Source :* Étude canadienne sur l'identité numérique 2020, réalisée par le CCIAN

pour refondre le projet comme une expérience humaine. En observant, en glanant, en expérimentant, en comprenant ce que les gens font, pensent et utilisent réellement dans leur vie et en sympathisant avec eux, l'ODM crée des services que les citoyens utiliseront et établit une relation plus confiante avec le public.

Estonie

En Estonie, chaque citoyen possède une identité numérique et une signature électronique. L'Estonie a adopté une loi pour que l'accès à Internet soit un droit de la personne, et plus de 90 % de sa population est en ligne. L'exemple estonien porte à croire que la gouvernance électronique est plus acceptée dans les petits pays, surmontant les infrastructures de communication dysfonctionnelles ou difficiles, avec une population jeune qui a toute une grande confiance envers les institutions.

Royaume-Uni

Le Data Advisory Board du Royaume-Uni, dirigé par le chef de direction de la fonction publique et le secrétaire permanent du Cabinet, coordonnent les efforts afin de faire le meilleur usage possible des données dans l'ensemble du gouvernement, comme les initiatives visant à maintenir la sécurité des données sensibles, à assurer des normes de sécurité communes, à faciliter pour les citoyens la consultation et la correction des données sur eux-mêmes et à perfectionner les principes éthiques des techniques de science des données.

Le Royaume-Uni s'est également engagé à réaliser les avantages de l'identité numérique, sans créer de carte d'identité. Plus tôt cette année, il a publié une version préliminaire du UK Digital Identity and Attributes Trust Framework, l'équivalent du Cadre de confiance pancanadien.

Le cadre montre comment les organisations peuvent être accréditées pour fournir des services d'identité numérique sécurisés; elles devront suivre un processus d'évaluation avec un organisme d'accréditation. Il indique également comment les données peuvent être échangées entre les organisations et annonce que le gouvernement commencera à mettre à l'essai le cadre en partenariat avec les fournisseurs de services[8].

De plus, il élabore et met à l'essai le nouveau système « One Login for Government » (Une seule connexion pour le gouvernement » qui facilitera l'accès de tous aux services gouvernementaux, les utilisateurs n'ayant qu'à fournir des données pour prouver leur identité une fois et protéger la vie privée tout au long du processus[9].

Amélioration de la prestation de services sans faille

L'amélioration de la prestation des services est l'un des moyens les plus importants d'accroître la confiance du public envers le gouvernement — simplement en démontrant un rendement élevé.

Initiative d'échange de renseignements sur l'adresse et le dépôt direct

Un projet conjoint du gouvernement du Canada, l'Initiative d'échange de renseignements sur l'adresse et le dépôt direct, vise à permettre l'expérience « Une fois suffit » en échangeant l'information de base dans l'ensemble des organisations afin de simplifier pour les Canadiens le processus de mise à jour de leurs renseignements, ce qui réduit le temps et la confusion, et qui assure l'uniformité. Avec consentement, les renseignements bancaires des Canadiens seront mis à jour pour tous les programmes de prestations et de

[8] *Source:* https://www.gov.uk/government/news/next-step-in-plans-to-govern-use-of-digital-identities-revealed--2
[9] *Source :* https://www.gov.uk/government/groups/data-advisory-board-and-data-leaders-network

crédit de l'Agence du revenu du Canada, comme le crédit pour la TPS/TVH, l'Allocation canadienne pour enfants, l'Allocation canadienne pour les travailleurs et leur remboursement d'impôt sur le revenu. Ces renseignements sont communiqués à Emploi et Développement social Canada afin de mettre à jour les renseignements sur le Régime de pensions du Canada[10].

Calgary

La Ville de Calgary a intégré des données provenant de sources nouvelles, y compris le système de télévision en circuit fermé (TVCF) de Calgary Transit, dans ses données globales sur les incidents liés aux opioïdes. Selon la Ville, [TRADUCTION] *« le signalement des surdoses correspond aux endroits où les troubles sociaux sont élevés, principalement le long des lignes du C-Train ».*

Lorsqu'un incident survient sur la propriété de Calgary Transit, environ un tiers des cas sont signalés au moyen du système téléphonique HELP et environ 50 % sont signalés par des opérateurs de véhicule de transport en commun ou la surveillance de TVCF au Centre des opérations du transport en commun. En réponse à ce problème croissant, Calgary Transit et Alpha House mettent à l'essai une approche visant à jumeler un travailleur d'approche de l'équipe du programme Downtown Outreach Addictions Partnership (DOAP) à un agent de la paix de Calgary Transit. Cette équipe se déploiera dans le réseau du C-Train et surveillera de façon proactive les endroits où il y a des troubles sociaux élevés et des surdoses signalées[11].

Bloomberg Philanthropies

Bloomberg Philanthropies (BT) s'efforce d'assurer une vie meilleure et plus longue pour le plus grand nombre de personnes en se concentrant sur cinq domaines clés : les arts, l'éducation, l'environnement, l'innovation gouvernementale et la santé publique. Bloomberg a lancé le programme *What Works Cities* (WWC) en 2015 dans le cadre de son secteur clé de l'innovation gouvernementale. Avant 2015, seules quelques villes américaines avaient adopté une approche axée sur les données pour améliorer la prise de décisions; beaucoup croyaient que le gouvernement axé sur les données ne s'adressait qu'aux villes à forte population[12].

WWC fournit un réseau national de villes en croissance, avec une norme d'excellence pour les administrations locales axées sur les données (la norme WWC), une assistance technique de chacun de ses organismes partenaires experts, des possibilités d'apprentissage par les pairs pour appuyer et élargir l'adoption d'approches axées sur les données pour les problèmes urgents et les activités gouvernementales, et une série de formations en ligne et de webinaires conçus pour renforcer les capacités du personnel municipal. Toute ville d'une population comptant au moins 30 000 habitants peut accéder aux ressources de WWC.

Les villes inscrites au programme et accréditées par BT ont obtenu les résultats suivants :

- Gestion du rendement : Le pourcentage de villes qui surveillent et analysent leurs progrès vers les objectifs clés a plus que doublé (passant de 30 % à 75 %).

[10] *Source :* Rapport au greffier du Conseil privé : Feuille de route de la Stratégie relative aux données pour la fonction publique fédérale
[11] *Source :* The Opioid Crisis and Response: Update to Council and Senior Administration, Ville de Calgary, 21 juin 2018
[12] *Source :* https://www.bloomberg.org/

- Participation du public : Le pourcentage de villes qui s'engagent avec les résidents sur un objectif et qui communiquent les progrès a plus que triplé (passant de 19 % à 70 %).
- Diffusion des données : Le pourcentage de villes disposant d'une plateforme et d'un processus de diffusion des données aux résidents a plus que triplé (passant de 18 % à 67 %).
- Prise de mesures : Le pourcentage de villes qui modifient les programmes existants en fonction de l'analyse des données a plus que doublé (passant de 28 % à 61 %).

Environ 70 % ont indiqué que leur ville utilise systématiquement des processus décisionnels axés sur des données pour répondre à la crise de la COVID-19, et près de 90 % des villes déclarent mieux utiliser les données pour mobiliser les résidents et/ou les intervenants communautaires.

Lorsque le réseau de WWC a été établi pour la première fois, il y avait une ou deux personnes dans chaque administration municipale qui étaient désignées pour appuyer des projets axés sur les données à l'aide de l'assistance technique fournie par WWC. Au cours des six dernières années, il y a eu un changement radical dans l'étendue et la profondeur des compétences en données dans l'ensemble des villes. Aujourd'hui, WWC travaille à des projets en moyenne avec plus de 11 dirigeants municipaux dans chaque ville. De plus, les villes sont passées de centres d'expertise en données limitée, cantonnés dans un rôle ou un service précis, à une utilisation généralisée. Dans l'enquête auprès des dirigeants municipaux, plus de la moitié des villes participantes ont déclaré avoir diffusé des données pratiques à au moins huit services ou organismes[13].

Initiative des Nations numériques

Les Nations numériques sont un forum collaboratif des principaux gouvernements numériques du monde qui vise à utiliser la technologie pour améliorer les services aux citoyens au Canada et dans le monde. Le Canada est actuellement l'un des dix pays membres. Les autres membres sont les pays suivants : l'Estonie, Israël, la République de Corée, la Nouvelle-Zélande, le Royaume-Uni, l'Uruguay, le Mexique, le Portugal et le Danemark. Ils dirigent la transformation du gouvernement numérique au profit des citoyens des façons suivantes :

- élaborer des politiques et des pratiques numériques;
- communiquer ces approches et pratiques exemplaires avec d'autres pays membres;
- faire progresser l'influence internationale de tous les pays membres;
- renforcer les relations, bâtir l'expertise et établir des liens entre les dirigeants numériques à l'échelle mondiale.

Chaque année, les pays membres des Nations Unies numériques se réunissent pour échanger leurs connaissances et expertises lors de réunions au niveau des opérations, au niveau du dirigeant principal de l'information et au niveau des ministères. Le Canada participe actuellement aux groupes thématiques des Nations numériques sur l'intelligence artificielle, l'identité numérique et les données. Le Canada préside le groupe thématique sur l'écologisation de la TI gouvernementale.

[13] *Source :* Rapport de Deloitte « Closing the Data Gap: How Cities Are Delivering Better Results for Residents A Monitor Institute », en collaboration avec What Works Cities, juin 2021

Estonie

L'Estonie gère l'assistant virtuel du citoyen, qui est un outil interactif vocal qui peut relier une personne à des services. Cet outil a permis de faciliter des activités du gouvernement, puisque celui-ci reçoit plus de 30 000 demandes par an concernant seulement la police et les mesures de contrôle frontalières[14].

En raison de toutes ces initiatives et innovations, la confiance des Estoniens dans leur Parlement et leur gouvernement est beaucoup plus élevée que la moyenne de l'Union européenne (UE). L'Eurobaromètre montre que plus de la moitié de la population estonienne, 51 %, fait confiance au gouvernement, qui est 1 % plus bas que l'année dernière. Dans l'Union européenne en moyenne, seulement 29 % de la population fait confiance au gouvernement d'État.

Le niveau de confiance dans le gouvernement national parmi les États membres de l'UE est plus élevé seulement aux Pays-Bas (52 %), en Suède (54 %) et à Malte (56 %)[15].

Renforcement de la souveraineté des données autochtones

En novembre 2019, le gouvernement provincial a adopté la *Declaration on the Rights of Indigenous Peoples Act* (*Declaration Act*). La *Declaration Act* établit la Déclaration des Nations Unies comme le cadre de réconciliation de la province, comme le demandent les *appels à l'action* de la Commission de la vérité et réconciliation. Cette loi historique a été élaborée en collaboration et en consultation avec les partenaires autochtones et vise à créer une voie à suivre qui respecte les droits de la personne des peuples autochtones tout en instaurant une plus grande transparence et une plus grande prévisibilité dans le travail que le gouvernement partage avec eux. Il est nécessaire d'élaborer un plan d'action pour réaliser cette harmonisation au fil du temps et présenter régulièrement des rapports annuels sur les progrès à l'Assemblée législative, en assurant la transparence et la responsabilisation pour suivre les progrès. De plus, la loi permet à la Province de conclure des accords avec un plus large éventail de gouvernements autochtones, et elle fournit un cadre pour la prise de décisions entre les gouvernements autochtones et la province sur les questions qui touchent leurs citoyens.

Participation des citoyens à la prise de décisions

Service Alberta a lancé une consultation en ligne afin de recueillir les commentaires des intervenants sur un certain nombre de questions liées à la protection de la vie privée, notamment :

- l'accès aux renseignements personnels et le contrôle de ceux-ci d'une personne lorsqu'elle interagit avec des organisations du gouvernement et du secteur privé;
- l'importance d'un consentement clair et éclairé, de la transférabilité des données et du droit à l'oubli;
- la nécessité d'une plus grande transparence, comme des déclarations de confidentialité en langage clair;
- le désir d'exigences juridiques pour la collecte, l'utilisation et la communication de données anonymisées;

[14] *Source : https://www.ria.ee/en.html*

[15] Source : Eurobaromètre — Opinion publique dans l'Union européenne 2014 https://europa.eu/eurobarometer/screen/home

- le renforcement de la surveillance gouvernementale afin de veiller à ce que les organisations des secteurs public et privé protègent les renseignements personnels au fur et à mesure que de nouvelles technologies émergent[16].

La province de la Saskatchewan a accompli beaucoup de travail avec la participation du public et a cherché de façon proactive à obtenir des commentaires des citoyens. Elle souhaite ainsi à accroître la confiance envers le gouvernement, puisque les consultations ont révélé que près de trois citoyens sur quatre s'inquiétaient quelque peu ou beaucoup de la compromission en ligne de leur information[17].

Surveillance de l'acceptabilité sociale

Une étude réalisée en 2018 par Statistics New Zealand, le principal ministère responsable de la collecte de données dirigé par l'intendant principal des données, a examiné l'acceptabilité sociale du gouvernement pour prendre des décisions concernant la gestion et l'utilisation des données publiques. Elle visait à assurer aux Néo-Zélandais la confiance dans la façon dont leurs données sont gérées.

L'étude a révélé ce qui suit :

- La plupart des personnes qui connaissent Statistics New Zealand ont un certain niveau de confiance dans ce que cette organisation fait, puisque 85,5 % des gens qui connaissaient son travail ont au moins une certaine confiance dans l'organisation.
- Moins les gens connaissaient Statistics New Zealand, moins ils avaient confiance dans l'organisation. Seulement 16,3 % de ceux qui avaient « un peu de connaissances » sur Statistics New Zealand avaient également une grande confiance envers l'organisation.
- 39,9 % des gens ne connaissent pas suffisamment Statistics New Zealand pour donner leur confiance éclairée à l'organisation[18].

Une étude menée en 2016 par le gouvernement néo-zélandais sur les attitudes du public à l'égard de l'intégration des données a révélé que :

- les participants s'attendaient généralement à ce que l'information fournie aux ministères soit échangée avec d'autres ministères;
- les gens semblaient juger de l'acceptabilité surtout en fonction du besoin d'information, autrement dit, la façon dont les données seraient utilisées et les personnes qui y auraient recours;
- les gens s'intéressaient à la valeur de l'intégration des données, voulaient savoir si les avantages l'emporteraient sur les coûts et les risques, et souhaitaient connaître la façon dont les risques d'atteinte à la vie privée et d'autres risques pourraient être atténués;
- les gens estimaient que les systèmes de données intégrés pouvaient être plus fiables, à jour et exacts que ceux qui sont actuellement utilisés et qu'ils pouvaient déboucher sur une prise de décisions et une prestation de services plus éclairés, plus équitables, plus efficaces et plus efficients[19].

[16] *Source :* https://www.jdsupra.com/legalnews/everybody-is-jumping-on-the-privacy-1873356/
[17] *Source :* Étude canadienne sur l'identité numérique 2020, réalisée par le CCIAN
[18] *Source :* https://www.stats.govt.nz/corporate/a-social-licence-approach-to-trust
[19] *Source :* https://www.stats.govt.nz/corporate/public-attitudes-to-data-integration

04.

Revue de la littérature

Revue de la littérature

La section suivante résume les principales constatations d'une revue de la littérature universitaire et grise qui porte sur l'acceptation et la confiance du public à l'égard de l'utilisation des données et des sujets connexes, en mettant l'accent sur l'utilisation des données dans le contexte du secteur public.

Principales perspectives

- Il existe actuellement peu de littérature universitaire et grise pour étudier les niveaux de soutien à l'utilisation des données par le gouvernement. La littérature disponible suggère que les niveaux de soutien et de confiance au Canada varient assez considérablement selon le but ou l'avantage de l'échange de données, avec des niveaux d'acceptation beaucoup plus élevés pour détecter la fraude et prendre des décisions stratégiques, par rapport à l'aisance à utiliser les données pour la collecte du renseignement.
- Dans les études qualitatives menées en Ontario et en Colombie-Britannique, on s'est généralement inquiété du risque de conséquences néfastes ou d'utilisation abusive des données, en particulier pour les membres vulnérables de la collectivité, notamment les membres de la collectivité LGBTQ et les populations autochtones.
- Les recherches menées dans des régions géographiques internationales révèlent que les Canadiens sont moins enclins à appuyer l'échange de données par le gouvernement et les professionnels de la santé que les habitants du Royaume-Uni. D'autres études portent à croire que les Canadiens ont moins confiance en l'utilisation et l'échange de données par le gouvernement que les résidents de l'Australie et des États-Unis.
- En général, le soutien à l'échange de données est plus important dans le but d'améliorer la sécurité personnelle, les soins de santé, la recherche médicale et la santé publique. En général, le soutien est légèrement inférieur aux fins de l'élaboration des politiques et de la prise de décisions du gouvernement, et il est nettement inférieur aux fins à but lucratif, comme le marketing.
- Les données probantes appuient la « théorie du calcul de la protection de la vie privée », qui laissent entendre que les personnes approuvent l'échange de renseignements personnels lorsqu'ils estiment que les avantages positifs l'emportent sur les résultats négatifs de cette démarche. Cela a été démontré dans le contexte du soutien à l'utilisation et à l'échange de données personnelles dans le but de rechercher les contacts pour ralentir la propagation de la COVID-19.
- Bien qu'il existe un vaste ensemble de documents internationaux qui explorent les influences sur la confiance et l'appui à l'échange de données, il existe d'importantes lacunes dans la recherche qui devraient être explorées pour établir une compréhension générale de l'acceptation par le public de l'échange de données dans le contexte canadien. En particulier, il existe des lacunes dans les données sur les niveaux de confiance entre les différentes régions géographiques et les différents groupes démographiques.

Approche

Cette revue de la littérature portait sur la recherche de la littérature universitaire et grise qui traite de l'acceptation et de la confiance du public à l'égard de l'utilisation des données et des sujets connexes, dont l'accent est mis sur l'utilisation des données dans le contexte du secteur public. Pour s'assurer du spectre le plus grand de publications pertinentes provenant d'un éventail de sources et de publications, une recherche documentaire a été effectuée dans diverses bibliothèques électroniques, dont Science Direct, Springer Link, SAGE Journals, ScienceOpen, SSRN : Réseau de recherche en sciences sociales, JSTOR : Journal Storage ainsi que Google Scholar (pour assurer le repérage des sources évaluées par les pairs et d'autres sources). Dans le cadre des stratégies de recherche, nous avons utilisé des termes d'en-tête de sujet appropriés pour chaque base de données et des mots clés pertinents à l'acceptation publique et à la confiance envers l'utilisation et l'échange de données personnelles par le gouvernement. Les sources ont été choisies pour être incluses dans cette revue en fonction de leur capacité à fournir des indications précieuses et uniques sur le sujet d'intérêt, ainsi que de la robustesse des méthodes de recherche appliquées. Ces ressources ont été examinées et analysées afin de fournir une revue concise de la littérature qui existe actuellement sur l'acceptation par le public de l'échange de données par le gouvernement. Les connaissances tirées de ces ressources ont été regroupées par thèmes dans la revue qui suit. Il s'agit notamment de l'acceptation par le public selon la région géographique, l'objectif de l'échange de données et les facteurs démographiques (comme l'acceptation parmi les populations vulnérables). Bien que ces thèmes se recoupent, ce regroupement thématique fournit une structure pour certains des principaux enseignements tirés de la documentation relevée. De plus, nous avons également cerné certaines lacunes de la recherche qui ont été relevées au cours de la présente revue de la littérature.

Acceptation par le public de l'utilisation et de l'échange des données dans l'ensemble des régions géographiques

Bien qu'aucune source n'ait été déterminée pour permettre une comparaison complète de l'acceptation par le public de l'échange de données dans l'ensemble des régions géographiques, plusieurs études ont été relevées pour comparer les attitudes d'un petit nombre de pays ou d'un seul pays. La section qui suit vise à résumer les études les plus pertinentes afin de donner l'occasion de comparer les niveaux relatifs de confiance et d'acceptation de la collecte, de l'utilisation et l'échange de données par le gouvernement.

Acceptation publique de l'échange de données selon le but au Canada

Le *Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée de 2020-2021*, commandé au Commissariat à la protection de la vie privée du Canada, fournit des renseignements récents et utiles sur l'opinion publique concernant la collecte de données par le gouvernement au Canada (Commissariat à la protection de la vie privée du Canada, 2021). L'étude portait sur le niveau d'acceptation des Canadiens à l'égard de la collecte et de l'utilisation de données selon la méthode et le but, ainsi que sur les facteurs démographiques comme l'âge. Elle a révélé que les Canadiens sont plus à l'aise avec la collecte de renseignements personnels à partir de sources en ligne, comme les publications sur les médias sociaux, dans le but d'enquêter sur une fraude potentielle, 57 % d'entre eux ayant déclaré qu'ils seraient « à l'aise » ou « très à l'aise » avec cette approche. Ce résultat n'a baissé que pour se situer à 45 % si les données étaient recueillies dans le but de prendre des décisions au sujet des programmes et des services gouvernementaux. Pourtant,

cette différence est très significative selon l'âge, 62 % des répondants âgés de 16 à 24 ans déclarant qu'ils l'appuyaient, comparativement à 38 % des répondants âgés de plus de 55 ans.

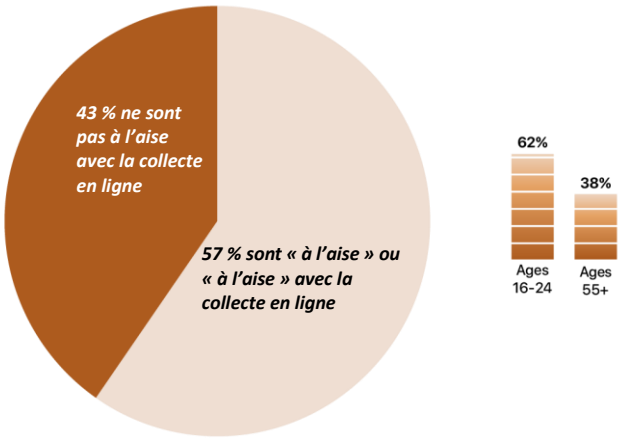


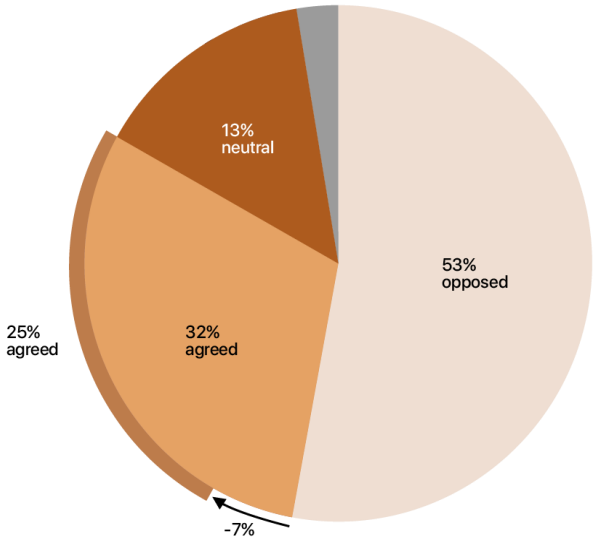
Figure 3 : Niveau d'aisance des Canadiens avec la collecte d'information en ligne

Les Canadiens sont plus à l'aise avec la collecte de renseignements personnels à partir de sources en ligne, comme les publications sur les médias sociaux, dans le but d'enquêter sur une fraude potentielle.

Ce résultat n'a laissé que passer seulement à 45 % si les données étaient recueillies dans le but de prendre des décisions au sujet des programmes et des services gouvernementaux.

Les niveaux d'aisance diffèrent de façon assez importante selon l'âge, 62 % des répondants âgés de 16 à 24 ans déclarant qu'ils l'appuyaient, comparativement à 38 % des répondants âgés de plus de 55 ans.

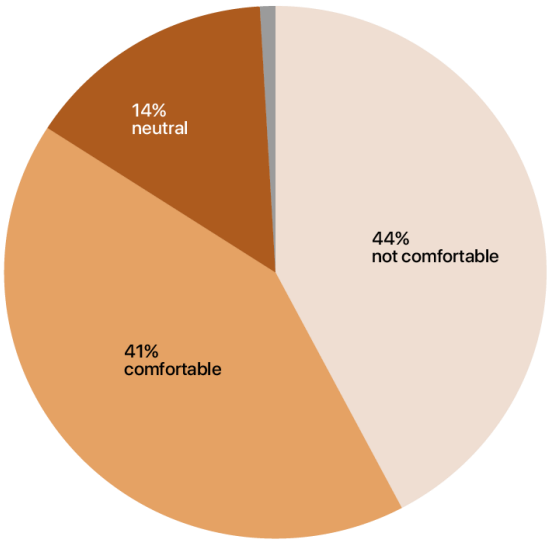
L'étude a également révélé que la collecte de données à caractère personnel à des fins de collecte dans le cadre d'activités de renseignement a peu de soutien. Lorsqu'on a demandé si *« le gouvernement du Canada devrait pouvoir recueillir et utiliser les renseignements personnels des Canadiens dans le cadre de ses activités de renseignement »,* la plupart des répondants (53 %) étaient opposés à l'énoncé, tandis que 32 % étaient d'accord et que 13 % avaient une opinion neutre à cet égard. Le pourcentage de ceux qui étaient d'accord avec l'énoncé a diminué pour se situer seulement à 25 % lorsqu'il était précisé que ces activités signifieraient que *« les Canadiens doivent céder une partie de leur vie privée ».* Il n'y avait pas non plus de consensus quant à l'acceptation de la collecte de renseignements personnels auprès des institutions financières par le gouvernement pour la prise de décisions économiques, notamment en matière de fiscalité et de dépenses. Dans l'ensemble, 44 % des Canadiens n'étaient pas à l'aise avec cette utilisation, 41 % ont déclaré qu'ils étaient à l'aise et 14 % avaient une opinion neutre. Fait significatif, 63 % des Canadiens ont déclaré qu'ils avaient confiance que le gouvernement fédéral respecte leur vie privée, ce qui représente une hausse par rapport au taux de 55 % en 2018. Ce taux était plus élevé que la confiance envers les entreprises, qui se situait à 45 %. Fait intéressant, une majorité (69 %) des répondants ont déclaré que leur opinion sur la protection de la vie privée et des renseignements personnels n'avait pas changé depuis le début de la pandémie. Parmi les 29 % qui ont déclaré que leurs opinions *avaient* changé, 48 % ont déclaré qu'ils étaient plus préoccupés par la protection des renseignements personnels.



Lorsque nous avons demandé si *« le gouvernement du Canada devrait pouvoir recueillir et utiliser les renseignements personnels des Canadiens dans le cadre de ses activités de renseignement »,* la plupart des répondants (53 %) étaient opposés à l'énoncé, tandis que 32 % étaient d'accord et que 13 % avaient une opinion neutre à cet égard.

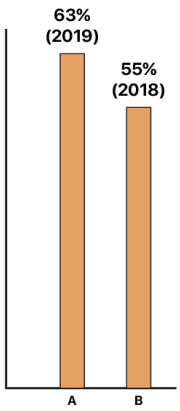
Le pourcentage de ceux qui étaient d'accord avec l'énoncé a diminué pour se situer seulement à 25 % lorsqu'il était précisé que ces activités signifieraient que *« les Canadiens doivent céder une partie de leur vie privée ».*

Figure 4 : « Le gouvernement du Canada devrait-il pouvoir recueillir et utiliser les renseignements personnels des Canadiens dans le cadre de ses activités de renseignement? »



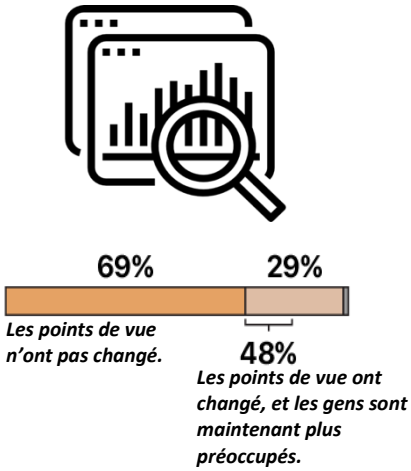
Il n'y avait pas non plus de consensus quant à l'acceptation de la collecte de renseignements personnels auprès des institutions financières par le gouvernement pour la prise de décisions économiques, notamment en matière de fiscalité et de dépenses. Dans l'ensemble, 44 % des Canadiens n'étaient pas à l'aise avec cette utilisation, 41 % ont déclaré qu'ils étaient à l'aise et 14 % avaient une opinion neutre.

Figure 5 : « Dans quelle mesure êtes-vous à l'aise avec le fait que le gouvernement recueille des renseignements auprès des institutions financières afin de prendre des décisions concernant l'économie »



63 % des Canadiens ont déclaré qu'ils avaient confiance que le gouvernement fédéral respecte leur vie privée, ce qui représente une hausse par rapport au taux de 55 % en 2018. Ce taux était plus élevé que la confiance envers les entreprises, qui se situait à 45 %.

Figure 6 : Confiance des Canadiens à l'égard du respect de la vie privée par le gouvernement du Canada



Une majorité (69 %) des répondants ont déclaré que leur opinion sur la protection de la vie privée et des renseignements personnels n'avait pas changé depuis le début de la pandémie.

Parmi les 29 % qui ont déclaré que leurs opinions *avaient* changé, 48 % ont déclaré qu'ils étaient plus préoccupés par la protection des renseignements personnels.

Figure 7 : L'opinion des Canadiens sur la protection de la vie privée et de leurs renseignements personnels.

Colombie-Britannique

En 2018, des recherches qualitatives ont été entreprises à Vancouver, en Colombie-Britannique, afin de recueillir des avis et des idées du public sur l'utilisation et l'échange de données couplées pour la recherche, en mettant l'accent sur les processus et les règlements nécessaires à la diffusion des données (Teng, Bentley, Burgess, O'Doherty et McGrail, 2019). Dans ce contexte de recherche, les auteurs ont défini les données comme des jeux de données liés à des sources, dont l'information déclarée par le patient, l'information génomique, les données provenant de dispositifs portables et des médias sociaux. La recherche a été menée par Population Data BC, en collaboration avec des chercheurs de l'Université de Guelph et de l'Université d'Édimbourg. La recherche visait à assurer une large représentation de la collectivité de la Colombie-Britannique et à tenir des consultations en personne au cours d'une activité de plusieurs jours réunissant 28 participants. Cette recherche a révélé qu'en général, les habitants de la Colombie-Britannique étaient favorables à la recherche à l'aide de données couplées en raison de leur valeur potentielle pour la société. Ce point a été en particulier solidement appuyé dans le contexte de la recherche sur les urgences en santé publique. L'un des principaux sujets de préoccupation concernant le couplage des données pour la recherche était le risque d'effets nocifs sur les populations étudiées, en particulier dans le cas des populations vulnérables et marginalisées (p. ex., les enfants, les collectivités autochtones). Dans la gestion de ces risques, les

répondants ont estimé qu'il fallait une gouvernance proportionnée qui équilibrait les risques et la nécessité d'une prise de décisions efficace. Les participants ont proposé qu'une plus grande transparence de l'accès aux données accroisse la fiabilité des processus d'accès aux données. Il y avait également des préoccupations quant à la participation des entreprises privées à la recherche et des facteurs de motivation pour que la recherche ne cadre pas avec le bien public. Dans l'ensemble, les participants ont indiqué qu'ils souhaitaient améliorer l'efficacité de l'information sur les demandes de données afin d'appuyer davantage de recherches, en précisant que des protections suffisantes sont en place pour protéger la sécurité et la vie privée.

Ontario

En 2015 et 2017, huit groupes de discussion ont été organisés avec 65 membres du public en Ontario pour en apprendre davantage sur les attitudes du grand public envers les utilisateurs et l'utilisation des données couplées administratives sur la santé détenues par l'Institut de recherche en services de santé (IRSS). (Parica, Nunes du Melo et Schull, 2019). L'IRSS est une société à but non lucratif qui mène des recherches sur les résultats en santé à l'aide de données recueillies par l'entremise du système de soins de santé financé par l'État de l'Ontario. Plus précisément, il [TRADUCTION] *« travaille avec des jeux de données qui sont créés en reliant les données au niveau des personnes provenant de différents ensembles de données (p. ex., médicaments d'ordonnance, hospitalisations, mortalité), puis en supprimant ou en codant l'information d'identification afin que la recherche et les analyses puissent être effectuées tout en protégeant la vie privée ».* Compte tenu des constatations de la recherche réalisée en Colombie-Britannique, cette étude a permis de dégager un soutien général à l'utilisation de données couplées administratives sur la santé aux fins de la recherche en santé, même si cette acceptation générale était conditionnelle au contexte. Les auteurs ont indiqué que l'une des principales conditions d'acceptation de l'utilisation des données couplées était la nécessité d'assurer la confidentialité et la sécurité. Plus précisément, bien que l'anonymisation des données ait été appréciée et qu'elle constitue une étape importante dans la protection de la vie privée et la sécurité, l'augmentation du nombre de parties pouvant accéder aux données accroissait était toujours considéré comme une augmentation du risque de violation de la vie privée et d'atteinte à la sécurité. En outre, le soutien à l'utilisation des données était plus solide lorsque les répondants avaient convenu qu'un avantage public tangible y était associé. En revanche, l'appui était plus faible lorsqu'on voyait que les résultats pouvaient être utilisés à mauvais escient ou désavantager les populations vulnérables. De même, le soutien de l'inclusion du secteur privé dans les études de recherche utilisant des données personnelles couplées a été considérablement moindre, certains participants n'approuvant cette proposition que lorsqu'il y aurait des avantages réciproques pour le public de leur participation (p. ex., des prix des médicaments plus bas). Notamment, il n'y a pas eu de consensus sur la nécessité d'obtenir le consentement lorsque les données sur la santé ont été anonymisées, et il y a eu des opinions divergentes sur la nécessité d'obtenir le consentement dans ce contexte. Dans le cadre de cette recherche, les auteurs concluent que si les chercheurs se concentrent sur la réalisation d'études qui [TRADUCTION] *« ont un avantage public évident, qui respectent préoccupations du public quant à la protection des renseignements personnels et à la participation du secteur privé et qui y répondent, le soutien du public est susceptible d'augmenter, ce qui renforcera l'impact et la viabilité de la recherche fondée sur des données couplées administratives sur la santé ».*

Canada et Royaume-Uni

Une étude récente portait sur la fiabilité perçue de certains acteurs sociaux au Canada et au Royaume-Uni, et l'incidence de ces facteurs sur la volonté du public de consentir à donner des données à utiliser et à échanger

pour la recherche en santé (Savic-Kallescoe, Middleton et Milne, 2021). Cette recherche a révélé qu'en général, les Canadiens avaient un niveau de confiance moindre à l'égard de l'utilisation et de l'échange de données que les Britanniques. En effet, 54 % des citoyens du Royaume-Uni ont précisé qu'ils faisaient généralement confiance à au moins deux des utilisateurs potentiels de données suivants : leur médecin de famille, les médecins du pays, le gouvernement de leur pays, ou bien les chercheurs nationaux d'organisme à but lucratif ou à but non lucratif. Par comparaison, seulement 48 % des Canadiens ont indiqué qu'ils avaient confiance à au moins deux de ces utilisateurs potentiels de données. Il est intéressant de prendre note que, malgré des niveaux de confiance inférieurs du public, les Canadiens étaient *plus* disposés à faire don de leurs données sur la santé à ces utilisateurs potentiels. Au Canada, 46 % des Canadiens étaient prêts à donner leurs données génomiques, comparativement à 40 % des répondants britanniques. Les auteurs avancent que ces constatations indiquent que [TRADUCTION] *« des niveaux élevés de confiance du public ne garantissent pas des niveaux élevés de volonté de donner; les gens sont prêts à faire des dons même s'ils ne font pas confiance, et on ne peut pas garantir que ceux qui font confiance seront également prêts à faire des dons. La confiance du public n'est pas suffisante pour qu'ils soient disposés à donner ».* Ils proposent que des facteurs tels que la confiance envers les acteurs sociaux individuels, comme les médecins et les chercheurs, qui participent à la collecte, à la gestion, au stockage et à l'application des données d'une personne puissent être plus importants que la confiance globale du public.

Canada, Royaume-Uni, États-Unis et Australie

Compte tenu de la possibilité que la confiance puisse jouer un rôle dans l'élaboration des attitudes du public à l'égard de l'échange de données génomiques et des initiatives de mégadonnées, une étude en ligne a été entreprise auprès de 8 967 membres du grand public au Canada, au Royaume-Uni, aux États-Unis et en Australie. (Milne et coll., 2019). Cette recherche a révélé que, dans tous les pays, les participants étaient plus susceptibles de faire confiance à leur médecin avec leurs données médicales anonymisées, 75 % des répondants ayant déclaré qu'ils feraient confiance à leur médecin. Les gens étaient moins susceptibles de faire confiance à un médecin (40 %) ou à un chercheur d'une université de leur pays (34 %), et beaucoup moins susceptibles de faire confiance au gouvernement de leur pays (19 %). À l'aide de ces résultats, les chercheurs ont classé les répondants en trois catégories : faible confiance globale (41 %), confiance variable (43 %) et grande confiance (16 %). Les personnes ayant une faible confiance sont constituées de celles qui ont une confiance modérée envers leur propre médecin et aucune confiance à l'égard d'autres organisations. La confiance variable sous-entend des niveaux élevés de confiance envers les professionnels de la santé, avec une confiance modérée aux chercheurs universitaires et une faible confiance à l'égard des chercheurs d'entreprises et de son propre gouvernement. Les personnes ayant une grande confiance globale sont composées de celles qui ont une grande confiance envers toutes les personnes ou organisations. À l'aide de ces classifications, les chercheurs ont déterminé que les participants de la catégorie « faible confiance » étaient les plus susceptibles d'être des habitants du Royaume-Uni, suivis du Canada et des États-Unis. Les Australiens étaient les moins susceptibles de rentrer dans cette catégorie. Les personnes qui font partie du groupe ayant une grande confiance étaient les plus susceptibles d'être originaires des États-Unis, puis du Royaume-Uni et du Canada. La recherche a également permis de déterminer que les personnes qui se sont identifiées comme des hommes étaient plus susceptibles de tomber dans la catégorie de la grande confiance, ainsi que celles qui étaient très scolarisées. Les personnes âgées de moins de 50 ans étaient plus susceptibles de tomber dans la catégorie « grande confiance », tandis que celles de plus de 50 ans ou plus étaient plus enclines à faire partie des catégories « faible confiance » ou « confiance variable ». En raison du faible taux de réponse des répondants

non blancs, aucune conclusion n'a pu être tirée des niveaux de confiance. Les auteurs concluent que, dans l'ensemble des pays, la mesure dans laquelle le grand public accepte l'échange de données sur la santé varie selon la confiance à l'égard du bénéficiaire, les niveaux les plus élevés de confiance étant envers son propre médecin et les plus bas niveaux de confiance à l'égard des entreprises et du gouvernement.

Royaume-Uni et États-Unis

Une autre étude a porté sur les attitudes publiques comparatives envers l'échange de données et l'accès aux données dans le domaine des soins de santé au Royaume-Uni et aux États-Unis (Ghafur, Van Dael, Leis, Darzi et Aziz, 2020). Les deux pays ont été choisis pour comparaison parce qu'ils sont tous deux des pays à revenu élevé qui ont fait des investissements importants dans l'échange de renseignements sur la santé et l'utilisation des données, mais qui ont des modèles de prestation des soins de santé nettement différents. En conséquence, l'étude visait à comprendre la mesure dans laquelle ces différences influent sur les attitudes du public à l'égard de l'utilisation et de l'échange de données. Notamment, cette recherche a révélé qu'en général, la volonté de communiquer des données était plus grande au Royaume-Uni qu'aux États-Unis. Comme le montre la *Figure 2*, la volonté de communiquer des renseignements anonymisés sur la santé différait considérablement selon l'entité qui recevrait les données. Dans les deux pays, la volonté de communiquer des données anonymisées sur la santé était plus forte lorsqu'elles étaient à un médecin individuel (Royaume-Uni, 75,4 %; États-Unis, 60,6 %), une institution universitaire ou médicale (Royaume-Uni, 50,3 %; États-Unis : 25,5 %), ou un pharmacien (Royaume-Uni, 40,4; États-Unis, 41,2 %). La volonté de communiquer des données sur la santé à son gouvernement était relativement faible dans les deux pays, bien que beaucoup plus faible aux États-Unis (6,6 %) qu'au Royaume-Uni (21,8 %). Les auteurs postule que [TRADUCTION] *« le fait que la méfiance aux États-Unis, qui ont un système largement privatisé, était plus grande qu'au Royaume-Uni, qui a un système socialisé à payeur unique, pourrait indiquer que les patients craignent que les données ne soient pas protégées contre une utilisation commerciale finale ».* Conformément à la littérature précédente, cette étude suggère que les gens sont moins à l'aise avec l'échange de données à des fins commerciales (Gostin, Halabi et Wilson, 2018). Autant aux États-Unis qu'au Royaume-Uni, moins de 20 % des répondants étaient prêts à communiquer des renseignements personnels anonymisés sur la santé à des sociétés pharmaceutiques, des compagnies d'assurance et des sociétés technologiques, même lorsque ces sociétés devaient utiliser ces données pour améliorer les soins de santé.

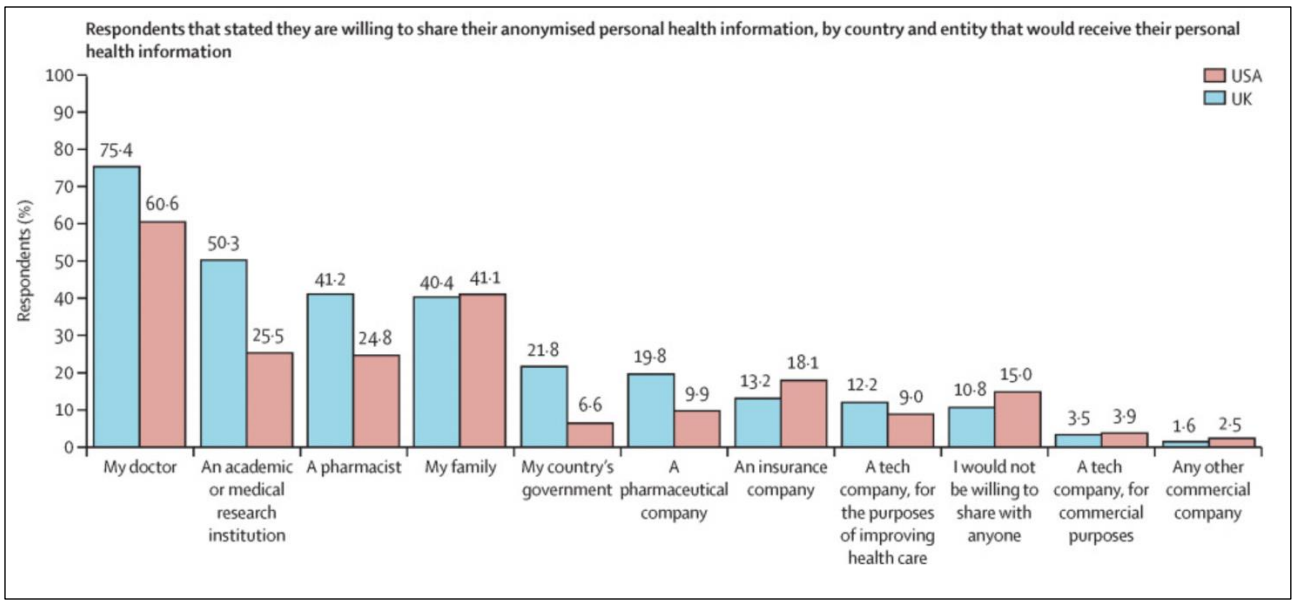


Figure 8 : *Volonté de communiquer des données sur santé selon l'entité au Royaume-Uni et aux États-Unis*[20]

Europe

Une étude comparative des attitudes à l'égard de l'échange de données personnelles dans un certain nombre de pays européens a été réalisée en 2018 (Open Data Institute, 2018). Dans le cadre de l'étude en ligne, on a interrogé des personnes de la Belgique, de la France, de l'Allemagne, des Pays-Bas et du Royaume-Uni. L'étude a révélé que, dans tous les pays, la grande majorité des répondants ont déclaré qu'il était important qu'ils fassent confiance à une organisation ou à une institution pour être disposés à communiquer des données à caractère personnel. La proportion la plus faible de répondants ayant exprimé ce point de vue provenait de France, 87 % des répondants ayant déclaré que la confiance était importante pour l'échange de données, et la plus forte proportion se situait au Royaume-Uni, à 94 %. Cette recherche a également mis en évidence de grandes différences dans la volonté de communiquer des données à différentes entités, comme le montre le *tableau 1*. Dans l'ensemble des pays étudiés, les gens étaient plus susceptibles de faire confiance aux fournisseurs et aux services de soins de santé avec leurs renseignements, suivis par les banques et les institutions financières, ainsi que les gouvernements locaux et centraux. Compte tenu des constatations tirées de l'étude américaine et britannique, les personnes étaient moins disposées à faire confiance aux entités commerciales, notamment les sociétés de marketing et de publicité, les compagnies d'assurance et les détaillants. Il y avait notamment une différence significative entre les niveaux de confiance des mêmes entités entre les différents pays. Par exemple, les niveaux de confiance dans l'échange de données avec les gouvernements centraux étaient relativement plus élevés aux Pays-Bas (48 %), au Royaume-Uni (37 %) et en Belgique (36 %) qu'en France (17 %) et en Allemagne (16 %).

[20] *Source :* Ghafur, S., Van Dael, J., Leis, M., Darzi, A. et Aziz, S. (2020). Public perceptions on data sharing : key insights from the UK and the USA. *The Lancet: Digital Health*.

Institution ou organisation	Belgique	France	Allemagne	Pays-Bas	Royaume-Uni	Moyenne
Gouvernement central	36 %	17 %	16 %	48 %	37 %	31 %
Administrations locales (p. ex., les organismes des conseils locaux)	36 %	19 %	26 %	53 %	41 %	35 %
Service de santé national et fournisseurs de soins de santé	60 %	35 %	37 %	71 %	64 %	53 %
Détaillants hors ligne (magasins physiques)	12 %	8 %	8 %	11 %	10 %	10 %
Détaillants en ligne (p. ex., Amazon)	12 %	11 %	15 %	21 %	22 %	16 %
Banques, organismes d'épargne et de crédit et sociétés de cartes de crédit (p. ex., Halifax, Barclays, etc.)	48 %	31 %	34 %	50 %	57 %	44 %
Organismes de recherche médicale (p. ex., Cancer Research UK, MS Society, etc.)	39 %	15 %	20 %	43 %	24 %	28 %
Sociétés de marketing et de publicité (p. ex., Saatchi & Saatchi, etc.)	5 %	2 %	2 %	4 %	2 %	3 %
Compagnies d'assurance (p. ex., Aviva, Direct Line, etc.)	41 %	27 %	22 %	40 %	32 %	32 %
Organismes de médias sociaux (p. ex., LinkedIn, Facebook, Instagram, etc.)	8 %	5 %	3 %	8 %	10 %	7 %
Universités	28 %	14 %	15 %	21 %	25 %	21 %
Famille et amis	62 %	55 %	60 %	61 %	57 %	59 %
Aucun de ces éléments	8 %	16 %	14 %	8 %	13 %	12 %
Je ne sais pas	8 %	10 %	7 %	6 %	7 %	8 %

Tableau 1. *Volonté de faire confiance à des organisations ou institutions avec des données personnelles selon le pays*[21]

De plus, dans cette étude, on a également demandé aux répondants de déterminer les fins pour lesquelles ils considéraient les données comme utiles. Comme le souligne le *tableau 1*, la principale réponse de tous les pays était que [TRADUCTION] *« les données sont les plus utiles lorsqu'elles contribuent à me protéger ».* Ce qui a été suivi de près par le soutien à la déclaration selon laquelle [TRADUCTION] *« les données sont utiles lorsque les gouvernements les utilisent pour comprendre et mieux servir la société avec des services publics améliorés ».* Il est intéressant de prendre note que les attitudes à l'égard de cet énoncé variaient considérablement selon les pays, les répondants au Royaume-Uni, en Belgique et aux Pays-Bas étant d'accord avec la déclaration à un taux de 51 %, 41 % et 37 % respectivement, tandis que le soutien en France et en Allemagne était plus faible, soit à 29 % et à 24 %. Ces différences montrent que les attitudes du public à l'égard l'échange des données gouvernementales en vue de l'amélioration des services publics peuvent varier considérablement selon le contexte géographique, politique et social précis.

Acceptation publique de l'échange de données entre les secteurs public, privé et tiers en Écosse

En 2012, le gouvernement écossais a commandé des recherches visant à étudier l'acceptabilité publique du couplage de données intersectorielles à des fins de recherche et de statistiques afin de comprendre les niveaux d'acceptation de l'échange de données entre les secteurs public, privé et sans but lucratif (Pagliari et coll.,

[21] *Source :* Open Data Institute. (2018). *Attitudes towards data sharing - Europe.* Open Data Institute.

2013). À l'aide de méthodes qualitatives, la recherche a permis de constater que le public était, en principe, généralement en faveur du couplage des données, même si ce soutien était conditionnel à l'objectif pour lequel les données seraient utilisées et avec qui elles étaient échangées. D'abord, la recherche a fait ressortir des préoccupations importantes concernant la confidentialité et la sécurité des données, et en particulier la prévention de l'échange de données personnelles avec des acteurs commerciaux, comme les entreprises privées. Des préoccupations persistaient même lorsque les données échangées entre les intervenants devaient être anonymisées. De plus, on était d'avis que la recherche utilisant des données échangées ne devrait être menée que dans les cas où il y a un avantage public. En conséquence, l'échange de données avec les organisations du secteur privé s'est opposé au fait que les entreprises privées n'agiraient pas dans l'intérêt public. De même, l'échange avec le secteur sans but lucratif a été considéré avec scepticisme en raison du potentiel d'intérêts catégoriels (c'est-à-dire les intérêts d'un groupe ou d'une organisation en particulier). L'une des principales préoccupations soulevées par la consultation publique était la possibilité que l'échange de données crée des résultats négatifs pour les membres déjà marginalisés de la collectivité écossaise. Par exemple, les participants LGBT étaient très préoccupés par le fait que les données sur l'orientation sexuelle pourraient être utilisées à mauvais escient, en particulier en cas d'atteinte à la protection des données. En tirant des conclusions de la recherche, les auteurs ont souligné l'importance [TRADUCTION] d'*« aborder la consultation comme un processus continu plutôt que de la considérer comme une stratégie ponctuelle visant à déterminer les attitudes et l'acceptabilité du public ».*

Singapour

En 2019, une étude portait sur le niveau de confiance des habitants de Singapour et leur volonté de permettre au gouvernement de recueillir des données, par rapport à leurs niveaux comparatifs de confiance envers les entreprises (Ong et Ling Loo, 2021). Constatant des niveaux élevés de confiance à l'égard de leur gouvernement, l'étude a révélé que les habitants de Singapour étaient toujours « modérément préoccupés » par la collecte de données tant par le gouvernement que par les entreprises. Toutefois, ils se préoccupaient moins notamment de l'échange de données avec le gouvernement que les entreprises. En effet, ils étaient beaucoup plus à l'aise avec leurs gouvernements que les entreprises qui recevaient des coordonnées personnelles, des coordonnées du travail, des renseignements sur les cartes de crédit, des renseignements démographiques, des pièces d'identité émises par le gouvernement, les antécédents médicaux, l'emplacement, les renseignements sur les amis des réseaux sociaux et l'historique des communications. Parmi ces catégories de données, les résidents étaient moins à l'aise avec l'accès du gouvernement aux renseignements sur leur carte de crédit, aux coordonnées personnelles et aux historiques de communication. Lorsqu'on a examiné les niveaux d'acceptation par les facteurs démographiques, l'étude a révélé que l'augmentation du revenu et de la scolarisation était associée à une préoccupation accrue concernant la collecte de données par le gouvernement. Il a également constaté que le vieillissement était associé à une préoccupation moindre à l'égard de l'accès du gouvernement aux données de localisation, mais n'était pas lié à l'inquiétude concernant les données sur la santé et les réseaux sociaux. Les auteurs avancent que ce niveau de préoccupation préexistant en matière de collecte de données par le gouvernement pourrait avoir contribué à l'inquiétude du public et à l'adoption relativement faible de la technologie de recherche des contacts du gouvernement de Singapour, TraceTogether, pendant la réponse à la pandémie de la COVID-19.

Acceptation de l'échange de données selon le but

En plus des différences géographiques quant à l'échange des données, la recherche sur l'acceptation publique de l'échange de données a aussi porté sur les différences en ce qui concerne l'acceptation publique de l'échange des données à différentes fins. Les contextes les plus pertinents aux objectifs de cette littérature, ainsi que ceux qui ont été étudiés de manière plus approfondie, sont résumés ci-dessous.

Échange de données pour la santé publique

Avant l'émergence de la crise sanitaire liée à la COVID-19, la santé publique était déjà l'un des principaux domaines de recherche pour l'acceptation publique de l'échange de données. En particulier, les facteurs qui influent sur la volonté du public de transmettre des données génomiques aux biobanques et à d'autres organismes de recherche ont été bien étudiés. Il s'agit de l'échange de données personnelles sur la santé (comme l'ADN) pour établir une « banque » de données génomiques qui sera utilisée pour développer la compréhension scientifique de la santé humaine et des maladies (Saskia C. Sanderson, 2017). Le succès et la valeur des biobanques reposent sur l'accès à de grands jeux de données et, par conséquent, sur le consentement des participants à fournir un « large consentement ». Cet accès renvoie à l'autorisation accordée aux chercheurs et aux établissements d'utiliser les données des participants non seulement pour atteindre des objectifs de recherche ponctuels et précis (consentement étroit), mais aussi pour des possibilités de recherche en santé à long terme (Richter et coll., 2017). En conséquence, une vaste recherche a été réalisée sur les facteurs qui influent sur la volonté du public d'accorder un large consentement à l'utilisation et à l'échange de données génomiques entre les institutions, y compris les organismes gouvernementaux.

Une étude importante sur la volonté du public de donner des données génomiques à une biobanque a mené une enquête auprès de 36 262 personnes dans 22 pays et en 15 langues, dans l'intention de [TRADUCTION] *« comprendre comment les membres du public, en tant que donateurs de données, considèrent et soutiennent le processus d'échange de données »* (Middleton et coll., 2020). La recherche a révélé que, dans l'ensemble de l'échantillon, la majorité des participants n'étaient pas disposés à donner anonymement des renseignements sur leur ADN et des renseignements médicaux à des fins d'utilisation par les chercheurs ou n'en étaient pas certains. En outre, ils étaient les plus disposés à fournir des renseignements à un médecin, et les moins disposés à les transmettre à un chercheur à but lucratif, en particulier en Pologne, au Portugal et en Allemagne (quoiqu'avec une différence beaucoup plus faible en Égypte, en Inde et au Pakistan). Dans l'ensemble des échantillons, sauf en Inde, la confiance envers la transmission de renseignements médicaux à plus d'un utilisateur (médecin, chercheur, gouvernement, entreprise) et la volonté de donner des données étaient étroitement corrélées. Au Canada, cette association entre la confiance entre plusieurs acteurs et la volonté de faire des dons était l'une des plus fortes associations, comme le montre la *Figure 2*. Les auteurs ont conclu que la variation entre la confiance et la volonté de donner des données génomiques porte à croire que la confiance envers les utilisateurs de données peut ne pas signifier la même chose partout en raison de différences culturelles et/ou circonstancielles. Ils ont également découvert une forte association entre la familiarité avec la recherche génomique ainsi que la connaissance des avantages associés à la recherche biobanque (en raison de la présence d'un trouble de santé hérité, par exemple).

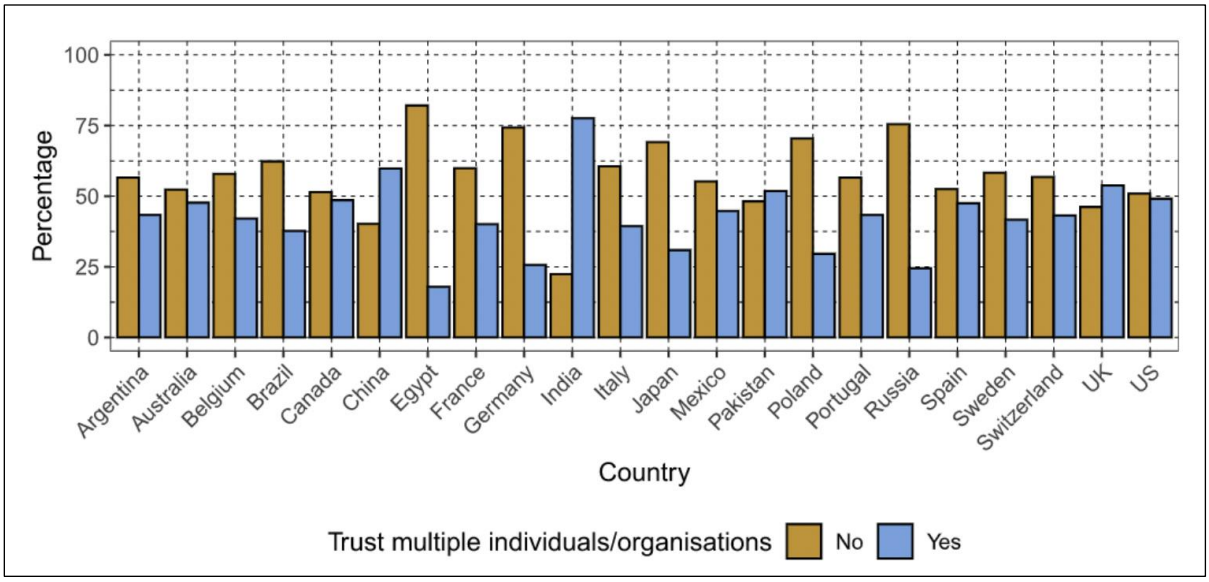


Figure 9 : *Confiance dans le don de renseignements sur l'ADN et de renseignements médicaux à plus d'un utilisateur, stratifiée par pays*[22]

Une série d'autres études ont porté sur les facteurs qui influent sur la volonté d'accorder son « large » consentement dans divers contextes et régions. Par exemple, une revue systématique de la littérature portant sur les points de vue des personnes sur le large consentement et les données aux États-Unis a révélé qu'une minorité de répondants étaient favorables à une option du large consentement lorsqu'il y avait une option d'accorder un consentement étroit (p. ex., le consentement à une étude à la fois) (Garrison et coll., 2016). La volonté d'accorder un large consentement s'est accrue si les données étaient anonymisées et lorsque les données n'étaient échangées qu'entre les chercheurs universitaires. Il y avait une volonté moindre d'accorder un large consentement lorsque les données pouvaient être échangées entre les bases de données fédérales. L'étude a également mis en évidence le fait que les minorités raciales et ethniques étaient souvent plus préoccupées par le fait de donner un large consentement, bien que cette information soit incomplète. De même, l'étude a mis en évidence le manque de renseignements sur l'influence des facteurs sociodémographiques, tels que le statut socioéconomique et la scolarisation, sur les attitudes à l'égard du large consentement et de l'échange de données. Une autre étude a porté sur les perspectives d'un large consentement à la recherche génomique et aux biobanques dans les pays à faible et à moyen revenu (Tindana et de Vries, 2016). D'après ces recherches, les auteurs ont recommandé que l'élaboration d'un cadre de gouvernance solide pour la génomique et les biobanques nécessite cinq éléments clés : respect, mobilisation communautaire authentique et renforcement de la confiance, préservation de la vie privée et de la confidentialité, rétroaction sur les résultats et renforcement des capacités.

[22] *Source :* Middleton, A., Milne, R., Almarri, A., Anwer, Atutornu, J., Baranova, E. E., . . . Critchley, C. (2020). Global Public Perception of Genomic Data Sharing : What Shapes the Willingness to Donate DNA and Health Data? *The American Journal of Human Genetics, 107*, 723-752.

Échange de données dans la poursuite du suivi des contacts pendant la crise de la COVID-19

Au cours de la dernière année, la crise de la COVID-19 a suscité l'intérêt des chercheurs pour la nécessité d'équilibrer les avantages pour la santé publique et les préoccupations quant à la protection de la vie privée. Cet intérêt a été particulièrement motivé par la possibilité d'utiliser les technologies de téléphone intelligent pour recueillir des données afin d'aider les efforts de santé publique à suivre, à retracer et à réduire au minimum la propagation de la COVID-19 (Yasaka, Lhrich et Sahyouni, 2020). En effet, les gouvernements de plusieurs pays, dont Singapour, l'Allemagne, le Royaume-Uni et l'Australie, ont lancé des applications de « suivi » de téléphone intelligent au cours de la dernière année (Lewandowsky, Dennis, Kashima, White et Garrett, 2021). Ces « applications » recueillent des données sur les contacts d'une personne afin de pouvoir suivre et d'informer les personnes qui pourraient être entrées en contact avec le virus. Bien que ces initiatives aient donné de nombreuses occasions d'aider les gouvernements à repérer et à réduire au minimum la transition vers la maladie, elles ont déclenché de vastes discussions sur la vie privée et l'acceptation par les citoyens de l'échange de données (French et Monahan, 2020). En conséquence, plusieurs études récentes se sont concentrées sur la compréhension de la perception des citoyens et de l'acceptation de la collecte et de l'échange de données aux fins du suivi des contacts liés à la COVID-19.

Dans le même ordre d'idées, une étude menée en Irlande visait à déterminer comment la perception de la vie privée des citoyens et les perceptions des avantages sociaux influent sur l'acceptation par les citoyens de l'échange de données aux fins du suivi des contacts (Fox, Clohessy, Van der Werff, Rosati et Lynn, 2021). Dans le cadre de l'étude, les auteurs ont recueilli des données tant avant qu'après le lancement à l'échelle du pays provenant d'une application de suivi des contacts du gouvernement, en examinant des facteurs tels que l'influence sociale, les avantages perçus et les préoccupations relatives à la protection de la vie privée. L'étude a révélé que l'influence sociale, la réciprocité sociale et la perception qu'a une personne des avantages pour la santé avaient influencé son intention d'utiliser l'application avant son lancement, et les avantages réciproques avaient influé sur l'utilisation au fil du temps. Il est intéressant de prendre note que les préoccupations relatives à la protection de la vie privée ne semblent pas influer sur les intentions d'utilisation avant ou après le lancement. Cela ne veut pas dire que les considérations relatives à la protection de la vie privée ne préoccupaient pas les citoyens. Les auteurs de l'étude avancent plutôt que cela indique que les avantages réciproques et personnels pour la santé de l'application, combinés à l'influence sociale, les ont *emportés* sur les préoccupations des citoyens à l'égard de la protection de la vie privée dans le contexte de l'application nationale de suivi de contacts de l'Irlande. En conséquence, ils font valoir que lorsqu'on instaure des politiques, des programmes et des technologies qui reposent sur l'échange de données, les décideurs devraient communiquer clairement les avantages (personnels et réciproques), ainsi que mettre en évidence sur les mesures de protection de la vie privée et la nécessité de communiquer des renseignements pour atteindre les objectifs énoncés. En conséquence, les citoyens peuvent évaluer les coûts et les avantages perçus du consentement à l'utilisation de leurs données, compte tenu du poids qu'ils accordent aux avantages sociaux et à leurs considérations de confidentialité.

Des études similaires ont également été réalisées dans d'autres régions. Une étude menée en Allemagne a révélé que les taux d'utilisation des applications de suivi des contacts étaient significativement plus élevés chez ceux qui faisaient confiance au gouvernement national, au système de santé et à la science en général, que parmi ceux qui avaient peu confiance envers ces institutions (Munzert, Selb, Gohdes, Stoetzer et Lowe, 2021).

Ces constatations concordent avec les recherches menées en France qui ont montré que la volonté d'utiliser une application de suivi des contacts est fortement corrélée avec les niveaux de confiance à l'égard du gouvernement (Guillon et Kergall, 2020). Au Royaume-Uni, une étude semblable a révélé que l'acceptation publique des technologies de collecte de données de suivi de contact et de suivi se situait entre 60 % et 70 % en avril 2020 (Lewandowsky, Dennis, Kashima, White et Garrett, 2021). La différence entre ces deux niveaux déclarés était fondée sur l'étendue à laquelle des mesures de protection de la vie privée étaient incluses dans les politiques proposées, comme l'option de refuser la collecte de données pour le suivi des contacts. Cette recherche a révélé que l'association la plus importante avec l'acceptation des technologies du suivi des contacts est la confiance d'une personne envers le gouvernement, et plus particulièrement sa confiance à l'égard de la capacité du gouvernement à protéger la vie privée.

Échange de données dans le contexte d'un « passeport vaccinal »

Le passeport vaccinal s'entend d'un document numérique ou physique qui permet au détenteur de démontrer qu'il a reçu le vaccin contre la COVID-19 et qu'il est ainsi en mesure de participer à des activités telles que les voyages internationaux (Dye et Mills, 2021). Déjà, l'Union européenne, le Danemark, Israël et New York ont instauré des passeports vaccinaux qui permettent l'accès à une gamme d'activités, et au Canada, le gouvernement fédéral s'est engagé à élaborer un passeport vaccinal pour les voyages internationaux. Même avant la disponibilité d'un vaccin contre la COVID-19, les chercheurs ont étudié les considérations éthiques, pratiques, juridiques et de confidentialité des passeports vaccinaux, ainsi que l'opinion publique sur leur utilisation (Schlagenhauf, Patel, Rodriguez-Morales, Gautret et Grobusch, 2021). Au Canada, un sondage d'Ipsos mené au début de mai 2021 a révélé que le public était fortement favorable à l'utilisation de passeports vaccinaux afin de permettre l'accès à une gamme d'activités (Simpson, 2021). Par exemple, 74 % des Canadiens étaient favorables à l'utilisation de passeports vaccinaux pour se rendre dans un établissement pour personnes âgées. Ce pourcentage est demeuré à 72 % pour les voyages en avion et à 71 % pour les vols à l'étranger. Même pour des activités comme les concerts en plein air et dans des stades, plus de 66 % des personnes interrogées ont appuyé quelque peu ou fortement l'exigence de passeports vaccinaux.

Les Canadiens étaient favorables à 74 % à l'utilisation de passeports vaccinaux pour se rendre dans un établissement pour personnes âgées. *Ce pourcentage est demeuré à 72 % pour les voyages en avion et à 71 % pour les vols à l'étranger. Même pour des activités comme les concerts en plein air et dans des stades, plus de 66 % des personnes interrogées ont appuyé quelque peu ou fortement l'exigence de passeports vaccinaux.*

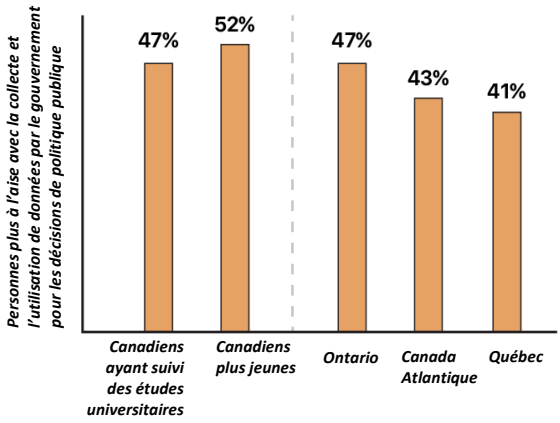
(Source : Simpson, S. (2021). Majority of Canadians Support Vaccine Passports for Variety of Indoor and Outdoor Activities. Toronto : Ipsos Public Affairs)

Une autre étude a permis d'effectuer une revue de la littérature rapide sur l'acceptabilité publique des passeports vaccinaux à l'aide de 33 revues de littérature provenant d'un large éventail de pays, dont l'Allemagne, le Royaume-Uni, les États-Unis, l'Australie, le Canada, le Nigeria, la Pologne, la Roumanie, l'Espagne et la Suisse (Drury et coll., 2021). Notamment, ces études portaient sur l'utilisation de passeports vaccinaux non seulement pour atténuer la propagation de la COVID-19, mais pour une gamme de différentes maladies transmissibles. La recherche reflète les constatations canadiennes sur les attitudes à l'égard de l'utilisation des passeports vaccinaux pour les voyages internationaux : l'attitude du public était généralement

favorable. Cependant, l'étude permet de penser que l'opinion publique est défavorable à leur utilisation dans le contexte de l'accès au travail et d'autres activités. Dans une étude semblable du Royaume-Uni, on a observé une attitude similaire et a étudié les facteurs qui agissent comme des prédicteurs de l'acceptation des passeports vaccinaux (Lewandowsky, Dennis, Kashima, White et Garrett, 2021). Cette étude a révélé qu'une plus grande confiance envers le gouvernement, l'augmentation de l'âge et le risque perçu de la maladie étaient associés à des attitudes plus favorables. Les auteurs avancent que ces constatations portent à croire que le public britannique est disposé, dans une certaine mesure, à « faire un compromis » entre leur vie privée et les intérêts de la santé publique. Fait important, la recherche a également démontré que les détails de la politique ont eu une incidence relativement faible sur le niveau d'acceptation par le public d'une politique de passeport vaccinal. Les auteurs ont fait valoir que même si cette constatation [TRADUCTION] « *est surprenante à la lumière des réponses des répondants aux sondages d'opinion qui accordent une grande importance à la vie privée […], elle est conforme au fait que les gens ont tendance à révéler des renseignements personnels pour des récompenses relativement faibles, contrairement à leur opinion exprimée.* » (Kokolakis, 2017) (Norberg, Horne et Horne, 2007) (Wang, Duong et Chen, 2016).

Confiance parmi les populations vulnérables

Comme l'a souligné la revue de la littérature jusqu'à présent, de nombreuses études ont mis en évidence que les niveaux de confiance et d'acceptation dans l'échange des données varient selon les groupes démographiques. Par exemple, le *Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée de 2020-2021* du Commissariat à la protection de la vie privée du Canada a révélé que les Canadiens ayant suivi des études universitaires (47 %) et les Canadiens plus jeunes (52 %) étaient plus à l'aise avec la collecte et l'utilisation de données par le gouvernement pour les décisions de politique publique.



Par exemple, selon le Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée de 2020-2021, les Canadiens ayant suivi des études universitaires (47 %) et les Canadiens plus jeunes (52 %) étaient plus à l'aise avec la collecte et l'utilisation de données par le gouvernement pour les décisions politiques publiques. Ces points de vue étaient aussi plus prépondérants en Ontario (47 %), au Canada Atlantique (43 %) et au Québec (41 %).

(Source : Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée de 2020-2021 — Commissariat à la protection de la vie privée du Canada)

Figure 10 : « Je suis à l'aise avec la collecte et l'utilisation de données par le gouvernement pour les décisions de politique publique »

Ces points de vue étaient aussi plus prépondérants en Ontario (47 %), au Canada Atlantique (43 %) et au Québec (41 %). En revanche, une étude évaluant la confiance des Canadiens à l'égard de l'échange de données génomiques a révélé plusieurs différences dans les niveaux d'acceptation selon l'âge, en concluant que les personnes de plus de 60 ans avaient des niveaux de confiance beaucoup plus élevés envers l'échange de ces données que les autres groupes d'âge.

La recherche reflète également les préoccupations de la collectivité canadienne selon lesquelles l'échange de données pourrait avoir des effets négatifs pour les membres de la société déjà marginalisés. Comme l'a souligné la recherche qualitative menée en Colombie-Britannique et en Ontario, l'une des principales hésitations à recueillir et à utiliser les données sur la santé à des fins secondaires est la possibilité d'une mauvaise utilisation ou d'une perpétuation de résultats négatifs pour des populations déjà marginalisées (Teng, Bentley, Burgess, O'Doherty et McGrail, 2019) (Parica, Nunes du Melo et Schull, 2019). Les groupes identifiés dans cette recherche comprennent les enfants, les personnes âgées et les populations autochtones. Malheureusement, aucune recherche n'a été relevée dans le cadre de cette revue, qui visait à quantifier les niveaux relatifs de confiance et d'acceptation de l'échange de données gouvernementales parmi les populations vulnérables et marginalisées, notamment les Autochtones et les personnes qui s'identifient comme LGBTQ2S+. Toutefois, des recherches récentes ont porté sur l'utilisation des données des Autochtones au cours de la pandémie de la COVID-19 au-delà des frontières internationales, y compris au Canada (Carroll et coll., 2021). Cette recherche a révélé que les politiques systémiques et la « marginalisation historique et continue » à l'échelle internationale ont entraîné des limitations quant à la qualité, à la quantité, à l'accès et à l'utilisation des données sur la COVID-19 des Autochtones.

À l'échelle internationale, un certain nombre de revues de littérature systémiques ont permis de déterminer des niveaux de confiance et d'acceptation variables de l'échange de données parmi les différents groupes démographiques et populations, en particulier ceux qui sont vulnérables ou marginalisés. L'une de ces études comprend une revue systématique et une synthèse thématique de plus de 25 études menées, principalement en Amérique du Nord et au Royaume-Uni. L'analyse thématique a mis en évidence plusieurs facteurs démographiques qui ont réduit la volonté de consentir à l'échange de données sur la santé. L'un de ces facteurs était l'origine ethnique identifiée des répondants (Hutrchings, Loomes, Butow et Boyle, 2021). Au Royaume-Uni, les répondants blancs étaient beaucoup moins susceptibles (59 %) de consentir à l'échange de données que les participants non blancs (72 %). De même, au Royaume-Uni et aux États-Unis, les personnes qui se disaient de Britanniques ou des Irlandais de race blanche avaient un consentement plus élevé que les autres groupes. Aux États-Unis, les personnes identifiées comme Afro-Américains étaient également moins susceptibles de consentir à l'utilisation des données. D'autres facteurs associés à l'acceptation accrue du partage de données étaient des niveaux d'éducation plus élevés, le sexe (les hommes étaient, dans certains cas, plus susceptibles de consentir à l'échange de données) et l'âge, en ce sens que les participants plus âgés étaient plus disposés à consentir à l'échange de données et aux données couplées que les populations plus jeunes.

Le « calcul de la protection de la vie privée », un facteur contribuant à l'acceptation publique de l'échange de données

À mesure que la technologie de collecte et d'analyse de données a progressé au cours des dernières décennies, on a exploré les facteurs qui contribuent aux préoccupations des particuliers en matière de protection de la vie privée et à l'acceptation de l'utilisation des données. L'une des principales théories utilisées pour comprendre les facteurs qui influent sur le niveau d'acceptation de la vie privée des citoyens et l'échange de données est la théorie du calcul de la protection de la vie privée (TCPVP) (Wolfe et Laufer, 1977). La théorie repose sur l'idée centrale que le comportement des gens est fondé sur un compromis entre les coûts et les avantages potentiels que le comportement créera. En conséquence, selon la TCPVP, les particuliers prennent des décisions en matière de protection de la vie privée pour communiquer les renseignements personnels et permettre

l'échange lorsqu'ils perçoivent que les avantages positifs l'emportent sur les résultats négatifs de la communication de renseignements personnels. La recherche a démontré une vaste gamme de facteurs que les personnes utilisent dans leur calcul des coûts et des avantages d'un résultat. Par exemple, les effets négatifs comprennent ce qu'on appelle les « croyances sur le risque », et la recherche a démontré qu'il y a un sentiment d'intrusion, de surveillance et de préoccupations relatives à la protection de la vie privée dans les renseignements sur la santé. Les résultats positifs sont liés aux avantages perçus de la technologie en question, dont les avantages pour la santé et la perception des avantages de la collecte et de l'échange de données par le gouvernement (Dinev, 2014) (Fox, 2020). Ces théories ont été appuyées dans un éventail de contextes, y compris récemment dans les niveaux d'acceptation publique des applications de suivi des contacts avec des personnes ayant contracté la COVID-19 (Lewandowsky, Dennis, Kashima, White et Garrett, 2021). En fait, une étude récente dans ce contexte conclut que les gens [TRADUCTION] *« se livrent à un calcul de la protection de la vie privée facilement compréhensible. Plus précisément, les gens échangent les préjudices perçus de la politique concernée (applications de suivi ou passeports d'immunité) contre le risque perçu de la COVID-19 : une perception accrue du risque augmente l'acceptation des politiques, et une crainte accrue des conséquences des politiques réduit le soutien.* »

Lacunes des recherches

Comme l'a souligné la présente revue, la majorité de la documentation relative au degré d'acceptation par le public de l'échange de données se rapporte à la collecte et à l'échange de données sur la santé. Même avant 2020, les études se portaient principalement sur les niveaux de confiance envers la collecte et l'échange de données sur la santé, comme les renseignements génomiques et médicaux. Il est intéressant de prendre note que le besoin d'outils tels que le suivi des contacts pendant la pandémie de la COVID-19 a mené à l'élargissement de la recherche sur l'acceptation du public dans des contextes plus vastes, comme la collecte et l'échange de données sur le lieu et l'administration. Néanmoins, à l'heure actuelle, il manque toujours de recherche sur les niveaux d'acceptation par le public de l'échange de données gouvernementales à des fins autres que la collecte et l'échange de données sur la santé. Cette réalité n'est pas unique aux niveaux provincial et national du Canada, mais aussi à l'échelle internationale. En conséquence, une lacune existe actuellement dans la littérature sur les niveaux d'acceptation de l'échange de données à des fins telles que l'échange intergouvernemental de données administratives pour une meilleure prestation des services sociaux. De même, il manque de recherches pour déterminer si les niveaux d'acceptation diffèrent selon les intervenants qui auront accès à ces données et l'association avec les niveaux de confiance à l'égard de ces intervenants.

Il convient également de signaler qu'il y a un manque de recherche sur l'acceptation par le public de l'échange de données dans un contexte canadien dans son ensemble, et particulièrement à l'échelle provinciale. Par exemple, aucune recherche canadienne qui porte précisément sur les niveaux de confiance envers le gouvernement et les niveaux connexes d'acceptation de l'échange de données intergouvernemental partout au Canada n'a été relevée. En conséquence, aucune recherche n'offre un aperçu exhaustif des niveaux de confiance et d'acceptation potentiellement variés de l'échange de données dans différents segments de la population canadienne, comme les différences entre les régions géographiques ou les populations minoritaires. Cette question pose des défis considérables aux décideurs lorsqu'ils prennent des décisions sur l'échange de données dans un contexte canadien, en particulier pour assurer un échange sécuritaire et éthique des données pour les populations marginalisées et vulnérables. La compréhension de la nature des différences entre les régions et les centres urbains, ruraux et les petits centres partout au Canada ainsi que de la différence

d'âge pour combler ces lacunes mènera à une compréhension plus complète de l'acceptation par le public de l'échange de données.

05.

Aperçu des principales lois

Aperçu des principales lois

Voici un résumé des principales constatations découlant d'un examen des lois relatives aux secteurs public et privé au Canada, ainsi que de discussions avec les commissaires à la protection de la vie privée, les bureaux d'accès à l'information et de la protection de la vie privée du gouvernement et les bureaux de dirigeant principal du numérique partout au Canada :

Principales perspectives

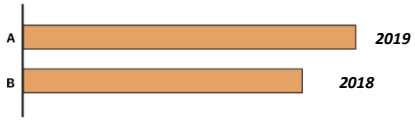
- Le public est au courant de la législation qui régit la protection des renseignements personnels, l'utilisation de ces renseignements et estime que le gouvernement fédéral, en général, respecte ses droits à la vie privée.
  De plus, les Canadiens font un peu plus confiance au secteur privé qu'au gouvernement pour les protéger contre les menaces de cybersécurité. *(Source : Sondages réalisés par Citoyens en tête de l'ISAC, 2018 et 2020)*
- Les thèmes qui ont émergé du public sont les suivants :
  - la grande préoccupation quant à l'utilisation de l'intelligence artificielle et de la reconnaissance faciale;
  - l'érosion du consentement;
  - l'utilisation de données à des fins non administratives ne cadre pas toujours avec les lois en vigueur.
- Pour tirer pleinement parti des avantages de l'économie numérique, beaucoup de provinces et de territoires canadiens ont entrepris des réformes législatives pour :
  - stimuler l'innovation en ouvrant le cloisonnement de données entre les ministères;
  - faciliter l'échange de données pour permettre au gouvernement d'offrir de meilleurs services aux citoyens;
  - empêcher les citoyens d'avoir à communiquer leurs renseignements personnels à plusieurs reprises;
  - rendre les données disponibles pour orienter les décisions, là où elles pourraient devenir plus motivées politiquement.
- Il y a eu une augmentation de l'adoption de lois sur la protection à la vie privée concernant le secteur privé au Canada.
- La volonté politique, un examen obligatoire intégré de la législation et un commissariat à l'information et à la protection de la vie privée actif ont aidé certaines administrations à apporter des changements substantiels à leur législation liée au secteur public.
- De nombreuses administrations internationales (en particulier les États-Unis) ont promulgué ou apporté des modifications analogues à leurs lois sur la protection de la vie privée ou sont sur le point de le faire.

Introduction

Un examen de la législation relative aux secteurs public et privé au Canada a indiqué que pour tirer pleinement parti de l'économie numérique et partager des données à des fins administratives et non administratives, une

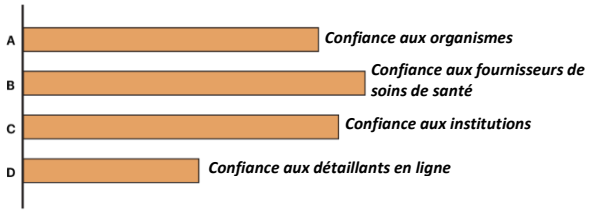
réforme législative est nécessaire. La volonté politique, un examen obligatoire intégré de la législation et un commissariat à l'information et à la protection de la vie privée actif ont aidé certaines administrations à apporter des changements substantiels à leur législation liée au secteur public.

Le public est au courant des lois qui régissent la protection des renseignements personnels et a bon niveau de confiance à leur égard[23].



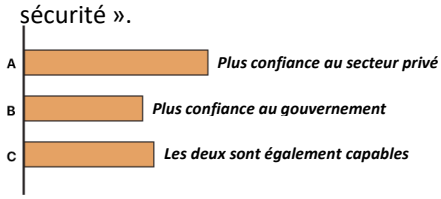
Plus de six Canadiens sur dix (63 %, en hausse par rapport à 55 % en 2018) estiment que le gouvernement fédéral, en général, respecte leurs droits à la protection des renseignements personnels.

Figure 11 : « Je pense que le gouvernement fédéral respecte mes droits à la protection des renseignements personnels. »



Près de six citoyens sur dix (57 %) disent faire confiance aux organismes gouvernementaux pour protéger les renseignements personnels. Ce pourcentage est légèrement inférieur à celui des fournisseurs de soins de santé (66 %) ou des institutions financières (62 %), mais il est bien supérieur à celui des détaillants en ligne comme Amazon (37 %).

Figure 12 : « Je fais confiance à certaines organisations pour que mes renseignements personnels demeurent en sécurité ».



Les Canadiens font légèrement plus confiance (37 %) au secteur privé qu'au gouvernement (25 %) pour les protéger contre les menaces de cybersécurité, alors que 23 % estiment que les deux sont également capables de le faire.

Figure 13 : Les Canadiens font confiance que les organisations des secteurs privé et public protégeront les renseignements personnels.

(Source pour les trois tableaux : Sondages réalisés par Citoyens en tête de l'ISAC, 2018 et 2020)

Approche

Une analyse de la législation fédérale, provinciale, territoriale et municipale (FPTM) du Canada a été effectuée. Elle comportait des recherches sur l'utilisation des données par les gouvernements FPTM afin d'améliorer la

[23] Source : Sondages réalisés par Citoyens en tête de l'ISAC, 2018 et 2020.

prestation des services et le niveau d'acceptation par les Canadiens de ces différentes utilisations et divulgations, y compris les niveaux d'acceptation par le public de :

- l'échange de renseignements personnels à des fins administratives;
- l'utilisation de données et de renseignements sur les services à des fins non administratives;
- les types de données et de renseignements personnels sont actuellement échangés, en vertu de quelles autorisations et à quelles fins.

Une analyse législative d'autres approches d'administration (en particulier les États-Unis, le Royaume-Uni, l'Estonie et l'Australie) a également été effectuée.

Une analyse des principaux accords internationaux relatifs à la protection des renseignements personnels et à l'échange de données (p. ex., provenant de l'OCDE et d'autres organismes internationaux) auxquels le Canada souscrit n'a pas été incluse dans la portée du présent rapport. Toutefois, cette analyse et l'examen des liens entre le présent rapport et ces accords internationaux seraient pertinents à d'autres discussions découlant du présent rapport et pourraient être inclus dans une phase future de ces travaux.

Entrevues avec les commissaires canadiens à l'information et à la protection de la vie privée du Canada et les bureaux gouvernementaux de l'accès à l'information et de la protection des renseignements personnels.

Tous les commissaires à l'information et à la protection de la vie privée du Canada et des bureaux provinciaux et territoriaux d'accès à l'information et de protection de la vie privée ont été invités à y participer. On espérait que cela fournirait un échantillon représentatif des renseignements recueillis par le gouvernement, de la façon dont ils sont utilisés, stockés, échangés ou supprimés et des régimes législatifs qui les appuient. On croyait aussi que ces entités comprendraient la perception du public quant à l'utilisation par le gouvernement de leurs données.

Commissaire à l'information et à la protection de la vie privée, et ombudsman

Un ensemble de questions standards a été préparé et utilisé pour toutes les entrevues.

Les thèmes qui ont émergé de ces consultations ont montré :

- une grande préoccupation quant à l'utilisation de l'intelligence artificielle et de la reconnaissance faciale;
- l'érosion du consentement;
- l'utilisation de données à des fins non administratives qui est contraire aux lois en vigueur.

Très peu de commissariats à l'information et à la protection de la vie privée effectuent des recherches proactives sur les perceptions du public et ne procèdent qu'à un processus fondé sur les plaintes.

Bureaux d'AIPVP gouvernementaux

En général, les gouvernements ne cherchent pas de façon proactive à obtenir des perceptions du public sur l'utilisation des données ou la confiance envers ce processus. La participation du public a été limitée partout au Canada et elle est généralement liée à un enjeu ou à une initiative en particulier.

Les gouvernements qui ont répondu ou qui ont été consultés dans le cadre d'un sondage ont indiqué un manque de ressources ou de capacité et des défis géographiques comme principaux obstacles à la participation du public. Parmi les autres commentaires dont ils ont fait part, mentionnons les suivants :

- des modifications législatives étaient nécessaires pour favoriser l'innovation;

- les frustrations à l'égard de la création de cloisonnements de données entre les ministères;
- les gouvernements devraient mieux échanger les renseignements personnels et les données à l'interne afin d'offrir de meilleurs services aux citoyens;
- les résidents n'estiment pas qu'ils devraient faire part de leurs renseignements personnels à maintes reprises et préfèrent que le gouvernement trouve des moyens d'intégrer l'accès à ces renseignements;
- il n'y avait pas assez de données pour orienter les décisions, et elles étaient donc souvent motivées pour des raisons politiques.

Recherche Web de la législation provinciale, territoriale et fédérale

Cette recherche portait sur la législation fédérale, provinciale et territoriale (FPT) et ses répercussions sur la confiance du public envers l'échange de données et l'acceptation de celui-ci.

Plus de consultations publiques se déroulent lentement :

- L'Ontario a fait une vaste consultation publique sur son gouvernement numérique et ses stratégies en matière de données[24].
- Le ministère Service Alberta a lancé une consultation en ligne qui se poursuivra jusqu'au 20 août 2021 afin de recueillir les commentaires des intervenants sur plusieurs enjeux liés sur la protection de la vie privée, notamment les suivants :
  - l'accès aux renseignements personnels et le contrôle de ceux-ci d'une personne lorsqu'elle interagit avec des organisations du gouvernement et du secteur privé;
  - l'importance d'un consentement clair et éclairé, de la transférabilité des données et du droit à l'oubli;
  - la nécessité d'une plus grande transparence, comme des déclarations de confidentialité en langage clair;
  - le désir d'exigences juridiques pour la collecte, l'utilisation et la divulgation de données anonymisées;
  - le renforcement de la surveillance gouvernementale afin de veiller à ce que les organisations des secteurs public et privé protègent les renseignements personnels au fur et à mesure que de nouvelles technologies émergent.

Sondage auprès des dirigeants principaux de l'information et des données

Les consultations avec les commissaires à l'information et à la protection de la vie privée et les bureaux gouvernementaux de l'accès à l'information et de la protection de la vie privée partout au Canada n'ont pas donné autant de réponses que prévu, de sorte qu'un sondage a été conçu et envoyé au dirigeant principal du numérique (DPN) ou au dirigeant principal de l'information (DPI) dans certaines administrations.

---

[24] *Source :* https://www.ontario.ca/fr/page/consultations-sur-la-strategie-ontarienne-pour-le-numerique-et-les-donnees
https://www.ontario.ca/fr/document/strategie-ontarienne-relative-aux-donnees

Aperçu des principales lois

Un aperçu des principales lois régissant la collecte, l'utilisation et la communication de renseignements personnels dans les provinces, territoires et le gouvernement du Canada. Il avait pour but de cerner les principales similitudes et les différences notables des approches, notamment en ce qui concerne la collecte, l'utilisation de renseignements et leur échange avec d'autres administrations ou gouvernements au Canada, aux fins de la prestation de services.

Il existe 41 lois distinctes, chacune ayant son propre règlement, qui traitent de la protection de la vie privée aux niveaux fédéral, provincial et territorial (FPT). Seules trois administrations ont une loi distincte pour les municipalités : l'Ontario, la Saskatchewan et la Nouvelle-Écosse. Toutes les autres municipalités relèvent de leur loi provinciale respective sur *l'accès à l'information et la protection des renseignements personnels.*

Lois fédérales

Le Canada a deux lois fédérales qui constituent le fondement de l'échange de données dans l'ensemble du gouvernement. Ces deux lois sont la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la protection des renseignements personnels*.

Loi sur la protection des renseignements personnels et les documents électroniques

La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) est entrée en vigueur en 2000 et s'applique aux transactions commerciales d'organisations qui exercent des activités dans le secteur privé canadien.

Plus précisément, la LPRPDE s'applique aux organisations sous réglementation fédérale relevant de la compétence du Parlement canadien, comme l'industrie des télécommunications et de la radiodiffusion, et toutes les entreprises locales du Yukon, du Nunavut et des Territoires du Nord-Ouest.

La LPRPDE s'applique au secteur privé de chaque province, à moins qu'une province n'ait promulgué sa propre loi sur la protection des renseignements personnels qui est sensiblement semblable à la LPRPDE. Les organisations assujetties à une loi provinciale sur la protection des renseignements personnels essentiellement similaires sont généralement exemptées de la LPRPDE en ce qui concerne la collecte, l'utilisation ou la communication de renseignements personnels qui se font dans cette province. À l'heure actuelle, seuls l'Alberta, la Colombie-Britannique et le Québec ont une loi « essentiellement similaire » en matière de protection de la vie privée.

La LPRPDE continue de s'appliquer aux organisations mènent des activités dans des ouvrages, des installations, des entreprises et des secteurs d'activités fédéraux dans ces provinces ainsi qu'à toutes les transactions interprovinciales et internationales effectuées par toutes les organisations assujetties à la LPRPDE au cours de leurs activités commerciales.

Les organismes qui exercent des activités interprovinciales ou internationales sont tenus de respecter les lois provinciales et fédérales sur la protection des renseignements personnels.

Loi sur la protection des renseignements personnels

La *Loi sur la protection des renseignements personnels* est entrée en vigueur en 1983, et elle régit les pratiques de traitement des renseignements personnels des institutions fédérales. Cette loi s'applique à tous les renseignements personnels que le gouvernement fédéral recueille, utilise et communique, qu'ils proviennent des particuliers ordinaires ou des employés fédéraux. Cette loi s'applique directement à tout organisme

fédéral. La Loi donne également aux gens le droit d'accéder aux renseignements personnels détenus par les institutions fédérales et de demander des corrections à ces renseignements.

Lois pour le secteur privé

Il y a une augmentation de l'adoption de lois sur la protection à la vie privée concernant le secteur privé au Canada. Comme nous l'avons mentionné précédemment, la Colombie-Britannique, l'Alberta et le Québec ont leur propre loi sur la protection des renseignements personnels relative au secteur privé. Ces textes législatifs sont jugés sensiblement similaires à la LPRPDE.

L'Ontario et le Manitoba ont récemment mis en place leur propre loi sur la protection des renseignements personnels dans le secteur privé et ont tenu des consultations publiques.

Principales similitudes des lois

Toutes les lois sur l'accès à l'information et la protection de la vie privée au Canada protègent et englobent le *Code type sur la protection des renseignements personnels* élaboré par l'Association canadienne de normalisation (CSA). Ce Code type a été élaboré par l'Association canadienne de normalisation en 1996, avec un comité de 45 membres composé de représentants du gouvernement, d'entreprises, d'universitaires, de consommateurs et d'experts en technologie de l'information et en sécurité[25]. Ces principes constituent également le fondement de la LPRPDE et sont définis à l'annexe D.

La législation canadienne sur la protection de la vie privée dans le domaine des soins de santé comprend 14 administrations gouvernementales (le gouvernement fédéral, 10 provinces et 3 territoires), chacune ayant son propre cadre législatif pour la protection des renseignements personnels (RP) ou des renseignements personnels sur la santé (RPS).

Toutes les lois sur l'accès à l'information et la protection des renseignements personnels dans le secteur public (qu'elles soient fédérales, provinciales ou territoriales) conservent une liste de droits pour le public[26]. Ces droits comprennent les suivants :

DROIT D'ACCÈS	En vertu des lois canadiennes sur la protection des renseignements personnels, les organisations doivent, sur demande et sous réserve d'exemptions limitées, informer les personnes de l'existence, de l'utilisation et de l'échange de leurs renseignements personnels et leur y donner accès, y compris une liste des organisations tierces avec lesquelles les renseignements ont été communiqués.
RECTIFICATION DES ERREURS	Les lois canadiennes sur la protection de la vie privée exigent généralement que, lorsqu'une personne démontre l'inexactitude ou la non-exhaustivité des renseignements personnels qu'elle détient, l'organisation corrige les inexactitudes et/ou y ajoute une note, selon le cas.
SUPPRESSION/DROIT À L'OUBLI	Bien que les lois sur la protection de la vie privée des provinces et des territoires (PT) du Canada accordent aux particuliers le droit de retirer leur consentement

[25] *Source :* https://www.privacysense.net/10-privacy-principles-of-pipeda/
[26] *Adapté du site* https://www.osler.com/osler/media/Osler/reports/privacy-data/Data-Protection-Laws-in-Canada-2018.pdf

	et de contester l'exactitude, l'exhaustivité et l'actualité de leurs données personnelles, elles n'accordent pas le droit précis d'exiger des organisations qu'elles « effacent » ou suppriment leurs renseignements personnels en soi. (Bien qu'il ne s'agisse pas d'un droit précis, les règlements sur la protection des renseignements personnels permettent l'élimination anticipée des renseignements personnels dans certaines circonstances.)
OBJET/TRAITEMENT RESTREINT	Les personnes accordent leur consentement à l'utilisation ou à la divulgation de leurs renseignements personnels au-delà de ce qui est requis pour remplir l'objet explicite et légitime de la collecte. De plus, une personne doit pouvoir retirer son consentement à tout moment, sous réserve de restrictions juridiques ou contractuelles et d'un préavis raisonnable. Dès réception de tout retrait, les personnes doivent être informées des conséquences de ce retrait.
PORTABILITÉ DES DONNÉES	Bien que les lois canadiennes sur la protection des renseignements personnels comprennent un droit d'accès aux renseignements personnels (voir ci-dessus), elles n'incluent pas le droit à la portabilité des données.
RETRAIT DU CONSENTEMENT	En vertu des lois canadiennes sur la protection des renseignements personnels des PT, une personne doit pouvoir retirer son consentement à tout moment, sous réserve de restrictions juridiques ou contractuelles et d'un préavis raisonnable. Les personnes doivent être informées des conséquences de ce retrait.
OBJET DU MARKETING	Le consentement est requis pour l'utilisation ou la communication de renseignements personnels à des fins de marketing. La forme de consentement requise (adhésion ou désistement) varie selon les circonstances, la sensibilité de l'information et les attentes raisonnables de la personne.
PLAINTE AUX ORGANISMES RESPONSABLES DE LA PROTECTION DES DONNÉES PERTINENTS	Les personnes ont le droit de porter plainte auprès de l'organisme responsable de la protection des données pertinent. À l'échelle provinciale et territoriale, les organisations doivent avoir des procédures faciles d'accès et simples à utiliser pour répondre aux plaintes ou aux demandes de renseignements et doivent prendre des mesures pour répondre efficacement aux plaintes en conséquence.

Organismes responsables de la protection des données

Chaque administration canadienne — fédérale, provinciale et territoriale — a son propre commissaire à l'information et à la protection de la vie privée ou son ombudsman indépendant qui relève de leur assemblée législative respective et qui supervise les lois pertinentes en matière de protection des données applicables dans cette administration.

Points de vue et différences notables pour l'échange avec d'autres administrations ou gouvernements au Canada

Lorsque des différences ont été constatées, elles étaient fondées sur la prémisse qu'une personne possède les renseignements les concernant. La volonté politique, un examen obligatoire intégré de la législation et un commissariat à l'information et à la protection de la vie privée actif ont aidé certaines administrations à apporter des changements substantiels à leur législation liée au secteur public.

Plusieurs changements ont été apportés au Canada en ce qui a trait à la mise à jour et à la modification des lois existantes qui ne permettaient pas l'échange de données à des fins non administratives.

Colombie-Britannique

En Colombie-Britannique, un comité spécial[27] de l'Assemblée législative a été mis sur pied pour examiner sa loi sur la protection des renseignements personnels, étudier les commentaires à ce sujet et publier des rapports. Ce comité facilite les discussions en vue d'examiner les modifications à y apporter, et certains des enjeux comprennent les suivants :

- la production obligatoire de rapports sur les atteintes;
- les consentements;
- rendre cette loi essentiellement semblable à la loi fédérale (la LPRPDE).

Il mène également des consultations publiques de diverses façons (consultations publiques et en ligne) pour faire progresser leurs initiatives en matière de souveraineté des données sur les Autochtones.

Declaration Act

Le gouvernement provincial a adopté la *Declaration on the Rights of Indigenous Peoples Act* (Declaration Act). La *Declaration Act* établit la Déclaration des Nations Unies comme le cadre de réconciliation de la province, comme le demandent les *appels à l'action* de la Commission de la vérité et réconciliation. Cette loi historique a été élaborée en collaboration et en consultation avec les partenaires autochtones. La Colombie-Britannique. est le premier province ou territoire au Canada à adopter une loi visant à mettre en œuvre la Déclaration des Nations Unies, qui reconnaît, en droit, les droits de la personne des peuples autochtones.

La *Declaration Act* vise à créer une voie à suivre qui respecte les droits de la personne des peuples autochtones tout en instaurant une plus grande transparence et une plus grande prévisibilité dans le travail que le gouvernement partage avec eux. Il est nécessaire d'élaborer un plan d'action pour réaliser cette harmonisation au fil du temps, ce qui assure la transparence et la responsabilisation des objectifs de la Déclaration des Nations Unies. De plus, elle exige la production régulière de rapports annuels sur les progrès à l'Assemblée législative, en assurant la transparence et la responsabilisation pour suivre les progrès.

De plus, la loi permet à la Province de conclure des accords avec un plus large éventail de gouvernements autochtones, et elle fournit un cadre pour la prise de décisions entre les gouvernements autochtones et la province sur les questions qui touchent leurs citoyens.

Manitoba

Le 2 novembre 2020, le gouvernement du Manitoba a présenté le projet de loi 49, *Loi modifiant la Loi sur l'accès à l'information et la protection de la vie privée*. Les organismes publics sont autorisés à communiquer des renseignements personnels pour fournir des services communs ou intégrés selon des conditions précises

[27] Vous trouverez de plus amples renseignements sur le Comité spécial à l'adresse suivante : https://www.leg.bc.ca/parliamentary-business/committees/42ndParliament-2ndSession-pipa

et à communiquer des renseignements personnels pour évaluer ou surveiller leurs programmes, ou pour effectuer des activités de recherche et de planification à leur sujet.

Le gouvernement du Manitoba a également présenté le projet de loi 54, *Loi modifiant la Loi sur les renseignements médicaux personnels*, et deux caractéristiques applicables sont qu'un syndic peut utiliser des renseignements médicaux personnels tout en éduquant les employés, les agents, les étudiants et les professionnels de la santé pour fournir des soins de santé.

Territoires du Nord-Ouest

La *Loi sur l'accès à l'information et la protection de la vie privée* des Territoires du Nord-Ouest est entrée en vigueur le 30 juillet 2021. La *Loi* permettra maintenant d'améliorer la reddition de comptes au public en donnant accès à l'information gouvernementale, ainsi que de mieux protéger la façon dont les renseignements personnels sont recueillis, utilisés et divulgués par des organismes publics.

Terre-Neuve

Depuis 2011, Terre-Neuve a modifié à deux reprises sa loi sur l'accès à l'information et la protection de la vie privée (AIPRP) afin de faciliter et de sécuriser l'utilisation administrative et non administrative des données dans l'ensemble du gouvernement.

Ontario

Le gouvernement de l'Ontario a présenté un livre blanc expliquant les nouvelles lois sur la protection des renseignements personnels dans le secteur privé à l'intention des entreprises et du secteur non gouvernemental.

Québec

En juin 2020, le gouvernement du Québec a présenté le projet de loi 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels.* Voici certaines caractéristiques :

- Modifier la *Loi sur la protection des renseignements personnels dans le secteur privé* afin de créer la fonction d'une personne chargée de la protection des renseignements personnels au sein des entreprises et d'exiger des entreprises qu'elles veillent à ce que les paramètres des produits ou services technologiques qu'elles utilisent pour recueillir des renseignements personnels fournissent par défaut le plus haut niveau de confidentialité, sans aucune intervention de la personne concernée.
- Le projet de loi exige que les organismes publics et les entreprises fournissent certains renseignements à la personne concernée lorsqu'ils recueillent des renseignements personnels au moyen d'une technologie qui comprend des fonctions permettant à la personne d'être identifiée, localisée ou profilée, ou lorsqu'ils utilisent des renseignements personnels pour rendre une décision fondée exclusivement sur le traitement automatisé de ces renseignements. Il établit le droit d'une personne d'accéder à des renseignements personnels informatisés la concernant dans un format technologique

structuré et couramment utilisé ou d'exiger que ces renseignements soient communiqués à une tierce personne.

Le 9 juin 2021, le projet de loi 95, *Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives*, a été adopté. Ce texte législatif établit un nouveau cadre pour la gestion des données numériques gouvernementales détenues par des organismes publics et exigera des ministères et organismes gouvernementaux qu'ils planifient et entreprennent des initiatives pour numériser les renseignements personnels des citoyens du Québec. La loi vise également à rationaliser l'échange de renseignements personnels numérisés au sein du gouvernement.

Yukon

L'Assemblée législative du Yukon a adopté le projet de loi 24, la nouvelle *Loi sur l'accès à l'information et la protection de la vie privée*, qui est entrée en vigueur le 1er avril 2021. Voici certaines caractéristiques de la Loi :

- remplacer l'approche fondée sur les antécédents de la Loi par une nouvelle approche fondée sur l'information;
- établir trois catégories normatives d'organismes publics et d'entités visées par règlement;
- enchâsser des principes de protection de la vie privée par conception la prestation d'activités de services de programmes et l'exécution d'activités de programmes par des organismes ministériels en exigeant que ceux-ci procèdent à une évaluation des facteurs relatifs à la vie privée dans certains cas;
- autoriser les organismes publics à :
    - fournir des services intégrés en collaboration avec des organismes partenaires,
    - fournir un service d'identité personnelle à l'échelle du gouvernement,
    - mener des activités de couplage de données.

Pratiques exemplaires internationales

Australie

.

Data Availability and Transparency Act

L'Australie a rédigé, mais n'a pas promulgué la *Data Availability and Transparency Act*. Il y a eu de nombreuses difficultés à échanger des données en vertu de sa loi sur la protection des renseignements personnels, rédigée dans les années 1980. Cette nouvelle loi autorise les gardiens de données du secteur public à échanger des données avec les utilisateurs accrédités, conformément à des autorisations, objectifs, principes et accords spécifiques.

Consumer Data Rights Act (CDR)

La RDC Act permettra aux consommateurs d'avoir un meilleur accès à leurs données et de mieux les contrôler, et elle améliorera la capacité des consommateurs à comparer les produits et services et à les changer.

En vertu de la RDC Act, les résidents australiens peuvent choisir que leurs données soient communiquées à un fournisseur accrédité de leur choix à l'aide d'un système en ligne sécurisé.

Estonie

La protection des données personnelles de l'Estonie provient de la loi de 1996 sur la protection des données personnelles (LPDP). La LPDP s'est adaptée au fil du temps à l'évolution des technologies et aux pratiques, mais un élément central est demeuré le même : le consentement.

Les renseignements personnels sensibles (attribut biométrique, ethnicité, vie sexuelle, adhésion à un syndicat, état de santé, par exemple) ne peuvent être ouverts par un organisme gouvernemental que si le sujet consent volontairement à leur utilisation. Pour donner plus de précisions, la LPDP ne considère pas le « silence ou l'inactivité » comme un consentement et accorde aux citoyens le droit de donner leur consentement « partiel et conditionnel ». En élargissant le concept de consentement, les citoyens estoniens sont protégés contre le traitement de leurs renseignements personnels sans autorisation. Il permet également aux citoyens de choisir de manière flexible le service électronique qui convient le mieux à leurs besoins.

L'Estonie est à la fine pointe de l'échange de renseignements grâce à son système X Road, qui est utilisé par plus de 3 000 entités publiques et privées, effectuant plus de 1,3 milliard de transactions par an.

Royaume-Uni

Le UK Digital Identity and Attributes Trust Framework, qui est semblable au Cadre de fiducie pancanadien du Canada, a été mis en place en juillet de cette année. Le cadre montre comment les organisations peuvent être accréditées pour fournir des services d'identité numérique sécurisés; elles devront suivre un processus d'évaluation avec un organisme d'accréditation. Il indique également comment les données peuvent être échangées entre les organisations et annonce que le gouvernement commencera à mettre à l'essai le cadre en partenariat avec les fournisseurs de services. À la suite de consultations avec diverses organisations publiques et privées l'an dernier, le gouvernement a produit une version préliminaire (ou « Alpha ») du document, sur laquelle il a invité les organisations et les citoyens à formuler des observations.

États-Unis d'Amérique

Des développements significatifs en matière de confidentialité des données ont été observés depuis 2020 aux États-Unis.

Californie

La *California Consumer Privacy Act* (CCPA) est entrée en vigueur cette année, donnant aux consommateurs californiens le droit d'exercer plus de contrôle sur leurs données.

Cette loi historique garantit aux consommateurs californiens de nouveaux droits à la vie privée, y compris les droits suivants :

- connaître les renseignements personnels qu'une entreprise recueille à leur sujet et la façon dont ils sont utilisés et communiqués;
- supprimer les renseignements personnels recueillis pour eux (à quelques exceptions près);
- se soustraire à la vente de leurs renseignements personnels;

- éviter la discrimination pour l'exercice de leurs droits prévus dans la CCPA.

La *California Privacy Rights Act* (CPRA) sert d'addenda à la CCPA : le renforcement des droits des résidents de Californie, le resserrement de la réglementation commerciale sur l'utilisation des renseignements personnels et la mise sur pied d'un nouvel organisme gouvernemental pour l'application de la protection de la vie privée des données à l'échelle de l'État, appelé California Privacy Protection Agency (CPPA).

La LPRP entrera entièrement en vigueur le 1er janvier 2023. L'application de la loi devrait débuter le 1er juillet 2023, avec une soi-disant période de retour en arrière jusqu'au 1er janvier 2022; ainsi les données recueillies à partir de cette date doivent y être conformes.

Delaware

.

Le 1er janvier 2016, la *Delaware Online Privacy and Protection Act* (« DOPPA ») est entrée en vigueur. Il s'agit d'une loi qui assure aux résidents de l'État une solide protection de la vie privée en ligne, y compris l'exigence que le gouvernement de l'État se défasse des données des consommateurs après une période déterminée.

Connecticut

.

L'*Insurance Data Security Law* du Connecticut est entrée en vigueur le 1er octobre 2020. Cette loi établit des normes applicables aux titulaires de licence du Département d'assurance du Connecticut pour la sécurité des données, l'enquête sur un incident de cybersécurité et la notification au Département de cet événement.

Nevada

.

Le Nevada a été le premier État à accorder aux consommateurs le droit de se soustraire à la vente de leurs renseignements personnels en vertu de son projet de loi 220 du Sénat, en octobre 2019. Le projet de loi 220 du Sénat exige des entreprises qu'elles honorent les demandes des consommateurs de ne plus vendre leurs données dans les 60 jours. Le procureur général du Nevada peut intenter une action en justice contre les entreprises pour avoir enfreint cette loi et infliger des amendes pouvant atteindre 5 000 dollars par infraction. Les entreprises sont toujours autorisées à échanger des renseignements personnels identifiables avec leurs propres filiales et, pour qu'une personne puisse s'y soustraire, une entreprise doit avoir l'intention de vendre les données.

New York

.

Une proposition de modification de la loi sur les droits civils de New York créerait une responsabilité pénale pour certaines atteintes à la vie privée, et le projet de loi *It's Your Data Act* créerait des droits de protection de la vie privée des consommateurs semblables à ceux de la CCPA, mais avec un droit d'action privé élargi.

La *Stop Hacks and Improvement Electronic Data Security Act* (SHIELD Act), qui a modifié la loi sur la notification des infractions de New York et qui exigeait que les entreprises visées mettent en œuvre et maintiennent des mesures de sécurité raisonnables, est entrée en vigueur en mars 2020.

Orégon

.

L'Oregon ne dispose pas de loi complète sur la confidentialité des données, mais il enchâssera la protection de la vie privée à une combinaison de dispositions de la common law, comme l'invasion de la vie privée et des lois sectorielles. En 2019, l'Oregon a mis à jour sa loi sur la notification d'atteintes à la protection des données, devenue maintenant l'*Oregon Consumer Protection Act*.

Virginie

.

L'adoption de la *Virginia Consumer Data Protection Act* (CDPA) plus tôt cette année offrira une gamme de nouveaux droits aux résidents de l'Old Dominion. Tout comme la *California Consumer Privacy Act*, la CDPA comprend un seuil clair où les entreprises sont couvertes si elles traitent les données personnelles de :

- 100 000 résidents de Virginie annuellement;
- 25 000 habitants de Virginie annuellement et que plus de 50 % de leurs recettes brutes sont tirées de la vente de données personnelles.

La CDPA s'appliquera à compter du 1er janvier 2023.

Washington

.

Le projet de loi 5062 du Sénat, la *Washington Privacy Act*, a eu un chemin cahoteux vers l'acceptation. Pendant trois années consécutives, ses législateurs ont tenté de l'adopter sans succès parce qu'ils n'ont pas pu s'entendre sur un mécanisme d'application.

06.
Recommandations

Recommandations

À la lumière de la recherche présentée, les Conseils mixtes de l'ISAC doivent étudier huit recommandations pour les prochaines étapes à suivre en vue de faire avancer les constatations du présent rapport. Les recommandations ont été classées en trois thèmes, à savoir les suivants :

Thème 1 : Comprendre les niveaux de confiance du public

- **Recommandation A** : Communiquer avec le public de partout au Canada afin de mieux comprendre les niveaux d'acceptation de l'utilisation des données par le gouvernement.
- **Recommandation B :** Encourager les gouvernements à établir une surveillance officielle et continue des niveaux d'acceptation par le public de l'utilisation et du partage des données par les Canadiens (en mettant l'accent sur la détermination des différences dans les niveaux d'acceptation entre les différentes régions géographiques, les centres urbains, ruraux, les petits centres et les groupes démographiques).

Thème 2 : Renforcement des relations entre le gouvernement et le public

- **Recommandation C :** Appuyer le gouvernement à prendre des mesures précises pour promouvoir la transparence en vue de gagner ou de regagner la confiance.
- **Recommandation D :** Encourager les gouvernements à permettre aux citoyens d'adopter l'approche « Une fois suffit », où les données peuvent être partagées avec d'autres ministères pour un ensemble d'utilisations convenues, conformément aux contextes législatifs du secteur public au Canada.
- **Recommandation E :** Plaider pour que les organisations gouvernementales donnent la priorité à la souveraineté des données autochtones.

Thème 3 : Amélioration des opérations internes du gouvernement

- **Recommandation F :** Encourager les gouvernements à établir des autorités centralisées responsable des données, en conformité avec les contextes législatifs du secteur public au Canada.
- **Recommandation G :** Éduquer les fonctionnaires sur les renseignements qu'ils peuvent et ne peuvent pas échanger (utilisation secondaire) et les exigences en matière de consentement, conformément à la loi sur la protection des renseignements personnels de leur administration.
- **Recommandation H** : Encourager et appuyer la réforme législative FPTM afin de permettre l'utilisation secondaire des données qui ne sont pas actuellement autorisées.

On a attribué un *niveau* estimé *de complexité et d'effort de mise en œuvre* à chacune des huit recommandations, ainsi qu'à une série d'activités précises qui pourraient être entreprises pour les faire avancer. À l'exception de la recommandation A, qui peut être dirigée et mise en œuvre entièrement par l'ISAC, notre estimation de la complexité et du niveau d'effort se rapporte à ce que les organisations gouvernementales devront faire pour suivre une recommandation donnée.

	Recommendation	Suggested Activities	Complexity	Effort
A	*Communiquer avec le public de partout au Canada afin de mieux comprendre les niveaux d'acceptation de l'utilisation des données par le gouvernement.*	a. Tenir des consultations publiques afin de mieux comprendre les niveaux d'acceptation, ainsi que les principaux facteurs et/ou événements qui ont façonné ces attitudes. b. Valider tous points de vue à l'encontre des constatations du présent rapport. c. Au moment de la tenue d'une consultation publique : i. Déterminer et préciser les raisons et les objectifs de la communication avec le public. ii. Assurer une combinaison d'une participation par exemple à l'aide de courts sondages et de consultation approfondie fondée sur la discussion. iii. Veiller à ce que, dans la collecte de ces données, la population échantillonnée soit représentative et saisisse les différences entre les régions géographiques et les groupes démographiques (particulièrement les populations vulnérables).		
B	Encourager les gouvernements à établir une surveillance officielle et continue des niveaux d'acceptation par le public de l'utilisation et du partage des données par les Canadiens (en mettant l'accent sur la détermination des différences dans les niveaux d'acceptation entre les différentes régions géographiques, les centres urbains, ruraux, les petits centres et les groupes démographiques).	a. Promouvoir la collecte d'un jeu de données longitudinales sur les attitudes des Canadiens à l'égard de l'utilisation et de l'échange de données. b. Mettre en commun les pratiques exemplaires des administrations qui commencent (p. ex., la Colombie-Britannique, l'Alberta, l'Ontario) ou qui le font déjà (p. ex., la Nouvelle-Zélande et le sondage public trimestriel *Kiwis Count*) c. Veiller à ce que, dans la collecte de ces données, la population échantillonnée soit représentative et saisisse les différences entre les régions géographiques et les groupes démographiques (particulièrement les populations vulnérables). d. Consigner l'acceptation de l'utilisation prévue des données (p. ex., santé, collecte du renseignement, vaste utilisation, etc.) et l'acceptation par le public dans son ensemble.		

			Complexity	Effort
			 High  Medium-High  Medium  Medium-Low  Low	
Recommendation		**Suggested Activities**		
C	*Appuyer le gouvernement à prendre des mesures précises pour promouvoir la transparence en vue de gagner ou de regagner la confiance.*	a. Encourager le gouvernement à continuer d'être constamment transparent sur les raisons pour lesquelles il recueille des renseignements publics, les fins auxquelles ils seront utilisés, les personnes avec lesquelles ils pourraient être communiqués et le pouvoir en vertu duquel ils sont recueillis. b. Encourager le gouvernement à tirer parti de la recherche sur les facteurs, les événements et les objectifs qui renforcent et diminuent la confiance envers l'échange de données, y compris en favorisant l'accès libre aux données, pour éclairer l'élaboration de politiques d'échange de données pour lesquelles il existe un soutien public. c. Encourager le gouvernement à prioriser et à améliorer continuellement les systèmes qui appuient l'exactitude, l'exhaustivité, la fiabilité et la protection des données. d. Aider le gouvernement à mettre en évidence les programmes et les politiques qui comportent la réussite de l'échange de données afin de fournir des services de haute qualité aux commettants dans l'ensemble des plateformes et des lieux géographiques. e. Collaborer avec des administrations étrangères qui ont entrepris des initiatives de recherche et d'échange de connaissances dans leurs régions respectives, notamment l'Australie, le Royaume-Uni et les États-Unis. f. Analyser les résultats des consultations publiques (recommandation A), et produire un rapport pour mettre en évidence les moyens par lesquels les gouvernements peuvent améliorer la transparence et la valeur de leur utilisation des données des citoyens.		
D	*Encourager les gouvernements à permettre aux citoyens d'adopter l'approche « Une fois suffit », où les données peuvent être partagées avec d'autres ministères pour un ensemble d'utilisations convenues, conformément aux contextes législatifs du secteur public au Canada.*	a. Mettre en commun les pratiques exemplaires des administrations qui le font déjà, comme l'Australie. b. Encourager les administrations PTM canadiennes à participer aux possibilités et groupes internationaux d'échange de connaissances afin de tirer parti des leçons tirées dans d'autres administrations, y compris avec des groupes internationaux d'échange de connaissances existants.		

	Recommendation	Suggested Activities	Complexity	Effort
		c. Aider les gouvernements à tirer parti de la recherche et de l'expertise existantes afin de veiller à ce que les programmes mis en œuvre : i. autorisent les citoyens à adhérer ou à se désister; ii. garantissent l'accessibilité pour les utilisateurs utilisant une technologie rudimentaire; iii. veillent à ce que l'utilisateur estime que ses renseignements sont privés et sécurisés; iv. suivent les lignes directrices disponibles sur consentement significatif du CIPVP du Canada.		
E	*Plaider pour que les organisations gouvernementales donnent la priorité à la souveraineté des données autochtones.*	a. Nouer le dialogue avec la collectivité pour comprendre la perspective autochtone sur la souveraineté des données dans le cadre d'une consultation inclusive et solide, et fournir ces renseignements au gouvernement (des progrès à cet égard peuvent être réalisés en parallèle ou dans le cadre de la recommandation B). b. Veiller à ce que la consultation soit fondée sur la collectivité et sur la nation. c. Encourager les gouvernements à favoriser une collaboration significative et des partenariats réciproques avec les collectivités autochtones. d. Mettre en commun les pratiques exemplaires des administrations qui le font déjà, comme la Colombie-Britannique. e. Promouvoir l'adoption par le gouvernement d'une autorité de données qui suit les lignes directrices du Centre de gouvernance de l'information des Premières Nations pour superviser la collecte et l'utilisation des données, ce qui est en voie d'être fait en Ontario. f. Chercher des points de vue internationaux de pays tels que la Nouvelle-Zélande et l'Australie sur les principales considérations à prendre en compte pour procéder efficacement à la souveraineté des données dans les initiatives d'échange de données.		

	Recommendation	Suggested Activities	Complexity	Effort
				
F	*Encourager les gouvernements à établir des autorités centralisées responsables des données, en conformité avec les contextes législatifs du secteur public au Canada.*	a. Encourager tous les gouvernements à établir un rôle clairement défini (p. exemple, un agent numérique) avec un mandat centralisé pour diriger les activités suivantes, entre autres : i. mettre à jour les politiques et élaborer des protocoles d'échange des données pour faciliter l'échange de données au sein du gouvernement afin d'améliorer la prestation des services; ii. favoriser les connaissances sur les lois en ce qui concerne les données qui peuvent être échangées à des fins secondaires et ce qui ne peut pas l'être; iii. travailler avec les DPI afin de veiller à ce que les données soient sécurisées et prêtes à l'emploi; iv. appuyer les pratiques exemplaires sur l'échange de données pour veiller à ce que l'utilisateur estime que ses renseignements sont privés et sécuriser. b. Tirer parti des enseignements tirés et des pratiques exemplaires des administrations qui détiennent déjà ce rôle, comme l'Ontario, la Colombie-Britannique et l'Île-du-Prince-Édouard.		
G	*Éduquer les fonctionnaires sur les renseignements qu'ils peuvent et ne peuvent pas échanger (utilisation secondaire) et les exigences en matière de consentement, conformément à la loi sur la protection des renseignements personnels de leur administration.*	a. Créer ou aider les gouvernements à créer des programmes de formation qui comblent les lacunes d'apprentissage (veiller à ce que la formation comprenne des séances de recyclage). b. Mettre à jour (ou aider les gouvernements à mettre à jour) le matériel de formation et d'apprentissage afin de refléter à la fois les pratiques actuelles et les ordres/recommandations d'un bureau d'AIPVP ou d'un CIPVP. c. Encourager les gouvernements à rendre les politiques et les procédures en matière de protection de la vie privée facilement accessibles. d. Éduquer le personnel sur les concepts *Ouvert par conception* et *Sécurité par conception* et sur la façon dont leur adoption pourrait contribuer à renforcer la confiance du public envers la collecte et l'utilisation des données du gouvernement.		

		High Medium-High Medium Medium-Low Low		
	Recommendation	**Suggested Activities**	**Complexity**	**Effort**
H	*Encourager et appuyer la réforme législative FPTM afin de permettre l'utilisation secondaire des données qui ne sont pas actuellement autorisées.*	a. Encourager les gouvernements à communiquer avec les administrations visées à l'**article 06**. **Aperçu des lois clés** pour en apprendre davantage sur leur approche de la réforme législative et pour déterminer l'harmonisation avec les réformes législatives souhaitées. b. Faciliter les discussions avec les gouvernements pour les aider à comprendre où ils voudraient poursuivre l'utilisation secondaire des données. c. Encourager les gouvernements à envisager de modifier la loi afin de mieux appuyer l'évolution des pratiques gouvernementales et les attentes des citoyens, y compris les changements qui faciliteraient l'échange des renseignements personnels entre les entités au sein du gouvernement et avec les entités externes approuvées. d. Encourager les gouvernements à mettre davantage l'accent sur la protection des renseignements personnels en modifiant la législation et la réglementation. e. Encourager les gouvernements à harmoniser les lois afin de permettre un échange meilleur et plus efficace des renseignements entre les gouvernements et au-delà des frontières, soit à l'internationale.		

Observations

Voici les principales observations relatives au guide :

1. La recommandation A est hautement prioritaire, relativement peu complexe et d'effort, et relève du contrôle de l'ISAC. Nous recommandons qu'elle soit séquencée en premier.
2. Les recommandations B à H consistent à inciter les gouvernements à prendre des mesures. En conséquence, nous recommandons qu'elles soient entreprises en parallèle. Cela permettra de simplifier les communications du point de vue du gouvernement et d'optimiser les ressources pour l'ISAC.
3. La recommandation H est un élément clé de la recommandation D, car une modification législative permettrait aux gouvernements d'adopter l'approche « Une fois suffit » dans le cadre de laquelle les données peuvent être échangées entre les ministères. Quoi qu'il en soit, le volet de défense de droits contenu dans la recommandation H peut progresser en parallèle avec la recommandation D.

07.
Annexes

Annexe A : Sources de la revue de la littérature

Les sources suivantes ont fourni des renseignements pour la réalisation de la revue de la littérature :

Carroll, S. R., Akee, R., Chung, P., Cormack, D. C., Kukutai, T., Lovett, R., . . . Rowe, R. K. (2021). Indigenous Peoples' Data During COVID-19: From External to Internal. *Frontiers in Sociology, 6*.

Dinev, T. (2014). Why Would We Care Abourt Privacy. *European Journal of Information Systems, 23*, 97-102.

Drury, J., Mao, G., John, A., Kamal, A., Rubin, J. G., Stott, C., . . . Marteau, T. M. (2021). Behavioural responses to COVID-19 health certification: a rapid review. *BMC Public Health*(21).

Dye, C. et Mills, M. C. (2021). COVID-19 vaccination passports. *Science, 371*, 1184.

Fahey, R. A. et Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management*.

Fox, G. (2020). To protect my health or my privacy? A mixed methods investigation of the privacy paradox. *Journal of the Association for Information Science and Technology*, 1-15.

Fox, G., Clohessy, T., van der Werff, L., Rosati, P. et Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behaviour, 121*.

French, M. et Monahan, T. (2020). Dis-ease surveillance : How might suveillance studies address COVID-19? *Surveillance & Society, 18*.

Garrison, N. A., Sathe, N. A., Matheny, A. H., Holm, I. A., Sanderson, S. C., Smith, M. E., . . . Clayton, E. W. (2016). A systematic literature review of individuals' perspectives on broad consent and data sharing in the United States. *Genetics in Medicine, 18*, 663-671.

Ghafur, S., Van Dael, J., Leis, M., Darzi, A. et Aziz, S. (2020). Public perceptions on data sharing : key insights from the UK and the USA. *The Lancet: Digital Health*.

Gostin, L. O., Halabi, S. F. et Wilson, K. (2018). Health Data and Privacy in the Digital Era. *JAMA, 320*, 233-234.

Guillon, M. et Kergall, P. (2020). Attitudes and opinions on quarantine and support for a contact-tracing application in France during the COVID-19 outbreak. *Public Health*, 21-31.

Hutrchings, E., Loomes, M., Butow, P. et Boyle, F. (2021). A systematic literature review of attitudes towards secondary use and sharing of health administrative and clinical trial data: a focus on consent. *Systematic Reviews, 132*.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comsputers & Security, 64*, 122-134.

Lewandowsky, S., Dennis, S., Kashima, Y., White, J. P. et Garrett, P. (2021). Public acceptance of privacy-encroaching policies to address the COVID-19 pandemic in the United Kingdom. *PLoS ONE, 16*.

Middleton, A., Milne, R., Almarri, A., Anwer, Atutornu, J., Baranova, E. E., . . . Critchley, C. (2020). Global Public Perception of Genomic Data Sharing : What Shapes the Willingness to Donate DNA and Health Data? *The American Journal of Human Genetics, 107*, 723-752.

Milne, R., Morley, K. I., Howard, H., Niemiec, E., Nicol, D., Chritchley, C., . . . Middleton, A. (2019). Trust in genomic data sharing among members of the general public in the UK, USA, Canada and Australia. *Human Genetics, 138*, 1237-1246.

Munzert, S., Selb, P., Gohdes, A., Stoetzer, L. F. et Lowe, W. (2021). Tracking and Promoting the Usage of COVID-19 Contact Tracing App. *Nature Human Behaviour, 5*, 247-255.

Norberg, P. A., Horne, D. R. et Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*, 100-126.

Commissariat à la protection de la vie privée du Canada. (2021). *Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée de 2020-2021,* Gatineau : Commissariat à la protection de la vie privée du Canada.

Ong, E. et Ling Loo, W. (2021). *Gauging the Acceptance of Contact Tracing Technology: An Empirical Study of Singapore Residents' Concerns and Trust in Information Sharing.* Singapore: Regulatory Insights on Artificial Intelligence : Research for Policy 2021.

Open Data Institute. (2018). *Attitudes towards data sharing – Europe.* Open Data Institute.

Pagliari, C., Davidson, S., Cunningham-Burley, S., Laurie, G., Mhariri, A. et Sethi, N. (2013). *Public Acceptability of Data Sharing Between the Public, Private and Third Sectors for Research Purposes.* Gouvernement de l'Écosse.

Parica, A., Nunes du Melo, M. et Schull, M. J. (2019). Social licence and the general public's attitudes toward research based on linked administrative health data: a qualitative study. *CMAJ Open*.

Richter, G., Krawczak, M., Lieb, W., Wolff, L., Schreiber, S. et Buyx, A. (2017). Broad consent for health care–embedded biobanking: understanding and reasons to donate in a large patient sample. *Genetics in Medicine*, 76-82.

Saskia C. Sanderson, K. B. (2017). Public Attitudes toward Consent and Data Sharing in Biobank Research: A Large Multi-site Experimental Survey in the US. *The American Journal of Human Genetics*, 414-427.

Savic-Kallescoe, S., Middleton, A. et Milne, R. (2021). Public Trust and Genomic Medicine in Canada and the UK. *Wellcome Open Research, 6*, 124.

Schlagenhauf, P., Patel, D., Rodriguez-Morales, A., Gautret, P. et Grobusch, M. (2021). Variants, vaccines and vaccination passports: Challenges and chances for travel medicine in 2021. *Travel Medicine Infectious Disease, 40*.

Simpson, S. (2021). *Majority of Canadians Support Vaccine Passports for Variety of Indoor and Outdoor Activities.* Toronto : Ipsos Public Affairs.

Teng, J., Bentley, C., Burgess, M. M., O'Doherty, K. C. et McGrail, K. M. (2019). Sharing linked data sets for research: results from a deliberative public engagement event in British Columbia, Canada. *International Journal of Population Data Science, 4*(1).

Thompson, N., McGill, T., Bunn, A. et Alexander, R. (2020). Cultural Factors and the Role of Privacy Concerns in Acceptance of Government Surveillance. *Journal of the Association for Information and Science Technology*, 1129-1142.

Tindana, P. et de Vries, J. (2016). Broad Consent for Genomic Research and Biobanking: Perspectives from Low- and Middle-Income Countries. *Annual Review of Genomics and Human Genetics, 17*, 375-393.

Wang, T., Duong, T. D. et Chen, C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, 531-542.

Wolfe, M. et Laufer, R. S. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues, 33*, 22-42.

Yasaka, T. M., Lhrich, B. M. et Sahyouni, R. (2020). Peer-to-peer contact tracing : A privacy-preseving smartphone application. *Journal of Medical Internet Research, 8*(4).

Yun, H., Lee, G. et Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs☆. *Information & Management, 56*, 570-601.

Annexe B : Administrations contactées pour l'analyse des perspectives géographiques

Yukon – Les administrations suivantes ont été mobilisées pour la rédaction de la section Analyse des perspectives géographiques du présent rapport :

Administration	Ministère ou organisation source
Alberta	▪ FOIP and Information Management
Colombie-Britannique	▪ Ministère des Services aux citoyens ▪ Dirigeant principal des données ▪ Administration municipale de Maple Ridge
Manitoba	▪ Secrétariat de l'accès à l'information et de la protection des renseignements personnels ▪ Commissariat à l'information et à la protection de la vie privée
Nouveau-Brunswick	▪ Finances et Conseil du Trésor ▪ Dirigeant principal des données
Terre-Neuve	▪ Bureau de l'accès à l'information et de la protection de la vie privée, ministère de la Justice et de la Sécurité publique. ▪ Dirigeant principal des données ▪ Commissariat à l'information et à la protection de la vie privée
Nouvelle-Écosse	▪ Unité de l'accès à l'information et de la protection des renseignements personnels
Territoire du Nord-Ouest	▪ Bureau d'accès à l'information et de protection de la vie privée, Division des politiques et de la planification du ministère de la Justice. ▪ Commissariat à l'information et à la protection de la vie privée
Nunavut	▪ Bureau d'AIPRP, ministère de l'Exécutif et des Affaires intergouvernementales ▪ Commissariat à l'information et à la protection de la vie privée
Ontario	▪ Services gouvernementaux et Services aux consommateurs, Division de l'information, de la protection de la vie privée et des Archives publiques. ▪ Dirigeant principal des données ▪ Commissariat à l'information et à la protection de la vie privée ▪ Smart Cities Mississauga (administration municipale)
Île-du-Prince-Édouard	▪ Sécurité informatique ▪ Commissariat à l'information et à la protection de la vie privée
Saskatchewan	▪ Direction de l'accès et de la protection des renseignements personnels, ministère de la Justice. ▪ Dirigeant principal des données
Yn	▪ Bureau de l'AIPRP, ministère de la Justice.

Appendice C : Sources pour l'analyse des perspectives géographiques

Les sources suivantes ont fourni des renseignements pour la réalisation de l'analyse des perspectives géographiques :

- *Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée de 2020-2021* — https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por_2020-21_ca/
- *Rapports annuels des commissaires à l'information et à la protection de la vie privée provinciaux et territoriaux*
- Bloomberg Philanthropies — https://www.bloomberg.org/
- Building Trust: Lessons from Canada's Approach to Digital Identity Observer Research Foundation Issue Brief 2020 - https://www.orfonline.org/research/building-trust-lessons-from-canadas-approach-to-digital-identity-67360/
- Rapport 2020 du Conseil d'identification et d'authentification numériques du Canada — https://diacc.ca/wp-content/uploads/2021/02/Canadian-Digital-Identity-Research-2020_Report_VF_FR-1.pdf
- Études Citoyens en Tête 2018 et 2020 de l'ISAC — https://citizenfirst.ca/fr/research-and-playbooks/citizens-first/citizens-first-2020
- Closing the Data Gap: How Cities Are Delivering Better Results for Residents A Monitor Institute by Deloitte report, in collaboration with What Works Cities June 2021 – https://www2.deloitte.com/us/en/blog/monitor-institute-blog/2021/closing-the-data-gap.html
- Data Advisory Board and Data Leaders Network – https://www.gov.uk/government/groups/data-advisory-board-and-data-leadersnetwork#:~:text=The%20use%20of%20data%20in,Media%20%26%20Sports%20(DCMS).
- Identité numérique : Mettre l'accent sur le Cadre de confiance pancanadien, RAPPORT EXÉCUTIF MENSUEL DU COMITÉ MISTE (produit du Comité de recherche), mai 2020 — https://citizenfirst.ca/assets/uploads/research-repository/Rapport-Executif-du-Conseil-mixte-mai-2020.pdf
- It's Not Only Size That Matters: Trust and E-Government Success in Europe — https://www.google.com/search?q=estonia+and+trust+in+government&oq=estonia&aqs=chrome.2.69i57j46i20i263i275i433i512j35i39l2j69i59j0i20i263i512j0i433i512j0i512l2j46i512.2425j0j15&sourceid=chrome&ie=UTF-8
- Stats NZ –

  https://www.stats.govt.nz/corporate/public-attitudes-to-data-integration

  https://www.stats.govt.nz/corporate/a-social-licence-approach-to-trust
- Sondage Kiwis Count du gouvernement de la Nouvelle-Zélande – https://publicservice.govt.nz/our-work/kiwis-count-survey/

- Rapport au greffier du Conseil privé : Feuille de route de la Stratégie de données pour la fonction publique fédérale — https://www.canada.ca/fr/conseil-prive/organisation/greffier/publications/strategie-donnees.html
- Autorité des systèmes d'information de la République d'Estonie — https://www.ria.ee/en.html
- The Opioid Crisis and Response: Update to Council and Senior Administration, Ville de Calgary, 21 juin 2018 – https://www.calgary.ca/csps/cns/mental-health-and-addiction.html
- Directive sur la prise de décisions automatisée du Conseil du Trésor — https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592
- Trusted Digital Transformation Considerations for Canadian Public Policy, janvier 2019) – https://www.gov.uk/government/groups/data-advisory-board-and-data-leaders-network
- UK Digital Identity and Attributes Trust Framework – https://www.gov.uk/government/news/next-step-in-plans-to-govern-use-of-digital-identities-revealed--2

Annexe D : Code type de la CSA

Voici les 10 principes qui constituent le fondement du Code type de l'Association canadienne de normalisation (CSA).

Responsabilisation

Une organisation est responsable des renseignements personnels dont elle a la gestion. Elle doit nommer une personne qui devra s'assurer de sa conformité à ces principes relatifs à l'équité.

Détermination des fins de la collecte des renseignements

Les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci.

Consentement

Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

Limitation de la collecte

L'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

Limitation de l'utilisation, de la communication et de la conservation.

À moins que la personne concernée n'y consente ou que la loi ne l'exige, les renseignements personnels ne doivent être utilisés ou communiqués qu'aux fins auxquelles ils ont été recueillis. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour répondre à ces fins.

Exactitude

Les renseignements personnels doivent être aussi exacts, complets et à jour que possible afin de satisfaire aux fins auxquelles ils sont destinés.

Mesures de sécurité

Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

Transparence

Une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles au public.

Accès aux renseignements personnels

Une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'intégralité des renseignements et d'y faire apporter les corrections appropriées.

Possibilité de porter plainte à l'égard du non-respect des principes

Toute personne doit être en mesure de se plaindre du non-respect par une organisation des principes énoncés ci-dessus. La plainte doit être adressée au responsable de la conformité à la LPRPDE au sein de l'organisation concernée, en l'occurrence, le chef de la protection des renseignements personnels.

Annexe E : Sources pour l'aperçu des principales lois

Les sources suivantes ont fourni des renseignements pour donner l'Aperçu des principales lois :

Entités consultées

- Bureaux de l'accès à l'information et protection de la vie privée fédéraux, provinciaux et territoriaux.
- Commissaires à l'information et à la protection de la vie privée et ombudsmans fédéraux, provinciaux et territoriaux.
- Bureau des dirigeants principaux du numérique et DPI.

Sources de la recherche

Commissariat à la protection de la vie privée du Canada

- **Comparaison entre juridictions : Lois de protection de la vie privée, 2020** https://www.priv.gc.ca/media/5435/jurisdictionalcomparison-fra.pdf
- **Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée de 2020-2021** https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2021/por_2020-21_ca/
- **Rapport au greffier du Conseil privé : Feuille de route de la Stratégie relative aux données pour la fonction publique fédérale** https://www.canada.ca/fr/conseil-prive/organisation/greffier/publications/strategie-donnees.html

Conseil du Trésor du Canada

- **Plan stratégique des opérations numériques de 2018 à 2022** https://www.canada.ca/fr/government/system/digital-government/government-canada-digital-operations-strategic-plans/digital-operations-strategic-plan-2018-2022.html
- **Politique sur les services et le numérique** https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32603
- **Politique sur la protection de la vie privée** https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12510
- **Stratégie du gouvernement numérique du Canada**

  The International Comparative Legal Guide to: Data Protection 2018 A practical cross-border insight into data protection law, publié par Global Legal Group, 5e édition, 2018. https://www.osler.com/osler/media/Osler/reports/privacy-data/Data-Protection-Laws-in-Canada-2018.pdf
- **Document d'orientation pour aider à préparer des Ententes d'échange de renseignements personnels** https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/protection-renseignement-personnels/document-orientation-aider-preparer-ententes-echange-renseignements-personnels.html

Annexe F : Résumé des lois canadiennes sur la protection des renseignements personnels

Voici un résumé, par administration, des modifications apportées à la législation et à son but.

Administration	Loi adoptée	Modification et but
Alberta	**SECTEUR PUBLIC** • *Freedom of Information and Protection of Privacy Act* (FOIP Act), 1995. • *Health Information Act*, 2001. **SECTEUR PRIVÉ** • *Personal Information Protection Act*, 2004.	L'Alberta est la dernière province canadienne à envisager des réformes des lois sur la protection de la vie privée dans les secteurs public et privé, puisque le gouvernement de l'Alberta a lancé un sondage en ligne pour recueillir des commentaires sur les protections offertes par la *Personal Information and Protection Act* et la *Freedom of Information and Protection of Privacy Act.*
Colombie-Britannique	**SECTEUR PUBLIC** • *Freedom of Information and Protection of Privacy Act* (FOIPPA), 1996. • *E-Health (Personal Health Information Access and Protection of Privacy Act*, 2008. **SECTEUR PRIVÉ** • *Personal Information Protection Act* (PIPA), 2004.	Un comité spécial de l'Assemblée législative examine des modifications à la PIPA.
Manitoba	• *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP), 1998. • *Loi sur les renseignements médicaux personnels* (LRMP), 1997.	Dernière modification : janvier 2011 Les organismes publics sont autorisés à divulguer des renseignements personnels dans le but de fournir des services communs ou intégrés dans des conditions déterminées, d'évaluer ou de surveiller leurs programmes, ou d'effectuer des recherches et de planifier à leur sujet. Le gouvernement du Manitoba a également présenté le projet de loi 54, *Loi modifiant la Loi sur les renseignements médicaux personnels,* mais il n'a pas encore été adopté. Le 2 novembre 2020, le gouvernement du Manitoba a présenté le projet de loi 49, *Loi modifiant la Loi sur l'accès à l'information et la protection de la vie privée*.

Nouveau-Brunswick	• *Loi sur le droit à l'information et la protection de la vie privée*, 2009. • *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé*, 2009.	Aucune modification.
Terre-Neuve	• *Access to Information and Protection of Privacy Act*, 2005. • *Personal Health Information Act* (PHIA), 2008.	Dernière modification : 2012 Définit les expressions « programme ou service commun ou intégré » et « système décisionnel automatisé ». Définit également les « évaluations d'impact algorithmiques » et exige que tout organisme public qui planifie la mise en œuvre d'un système de décision automatisé en réalise une et, au besoin, en fournisse une au commissaire à l'information et à la protection de la vie privée. Exige des organismes publics qu'ils tiennent des registres des processus décisionnels des systèmes décisionnels automatisés.
Nouvelle-Écosse	• *Freedom of Information and Protection of Privacy Act* (FOIPOP), 1993. • Personal Health Information Act (PHIA)	Aucune modification.
Territoire du Nord-Ouest	• *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP), 1996. • *Loi sur les renseignements sur la santé* (LRS), 2015.	La *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) des Territoires du Nord-Ouest est entrée en vigueur le 30 juillet 2021, et elle couvre maintenant les municipalités. La Loi permettra maintenant d'améliorer la reddition de comptes au public en donnant accès à l'information gouvernementale, ainsi que de mieux protéger la façon dont les renseignements personnels sont recueillis, utilisés et divulgués par des organismes publics. Permet la collecte et la communication de renseignements pour l'exécution de programmes et la prestation de services communs ou intégrés.
Nunavut	• Consolidation de la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP), 1994.	Aucune modification.

Ontario	**SECTEUR PUBLIC** • *Loi sur l'accès à l'information et la protection de la vie privée* (LIMPVP), 1990. • *Loi sur l'accès à l'information municipale et la protection de la vie privée*, 1990. • *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS). **SECTEUR PRIVÉ** • Projet de loi 64 de 2021 visant à promulguer une loi sur la protection des renseignements personnels dans le secteur privé.	La loi provinciale de l'Ontario sur l'accès à l'information et la protection des renseignements personnels a été modifiée en 2019 et en 2020 afin de permettre aux unités d'intégration des données de recueillir et de relier indirectement des renseignements personnels — au sein des ministères et entre eux, et même avec des entités externes désignées — aux fins de l'analyse, de la gestion, de la planification et de l'évaluation des programmes et services gouvernementaux. Les modifications apportées à la LPRPS établissent un cadre exhaustif de protection de la vie privée et de responsabilisation pour le dossier de santé électronique de la province, en répartissant les responsabilités partagées entre plusieurs gardiens qui utilisent le dossier. Pas encore promulgué.
Île-du-Prince-Édouard	• *Freedom of Information and Protection of Privacy Act*, 1988. • *Health Information Act*	Aucune modification.

Québec	• *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, 2006. • *Loi modifiant la Loi sur les services de santé et les services sociaux, la Loi sur l'assurance maladie et la Loi sur la Régie de l'assurance maladie du Québec.* • *Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives.* **<u>SECTEUR PRIVÉ</u>** • *Loi sur la protection des renseignements personnels dans le secteur privé*, 2021.	En juin 2020, le gouvernement du Québec a présenté le projet de loi 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels.* (Pas encore promulgué.) (Sanction reçue, mais non mise en œuvre encore.)
Saskatchewan	• *Freedom of Information and Protection of Privacy Act* (FOIP), 1990. • *Local Authority Freedom of Information and Protection of Privacy Act – municipal public sector*, 1991. • *Health Information Protection Act* (HIPA), 2003.	
Yukon	• *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP), 2018. • *Loi sur la protection et la gestion des renseignements médicaux*, 2013.	L'Assemblée législative du Yukon a adopté le projet de loi 24, la nouvelle *Loi sur l'accès à l'information et la protection de la vie privée*, qui est entrée en vigueur le 1er avril 2021 pour : ▪ fournir des services intégrés en collaboration avec des organismes partenaires; ▪ fournir un service d'identité personnelle à l'échelle du gouvernement; ▪ mener des activités de couplage de données.