

DE : Madame Sonia LeBel
Ministre responsable des Institutions
démocratiques, de la Réforme électorale
et de l'Accès à l'information

Le 25 mai 2020

TITRE : Loi modernisant des dispositions législatives en matière de protection des renseignements personnels

PARTIE ACCESSIBLE AU PUBLIC

1- Contexte

La protection des renseignements personnels est essentielle à l'exercice du droit à la vie privée, lequel constitue un droit fondamental reconnu par la Charte des droits et libertés de la personne (chapitre C-12) et le Code civil. Compte tenu de l'importance de ce droit, le législateur a conféré un statut prépondérant à la Loi sur la protection des renseignements personnels dans le secteur privé (chapitre P-39.1) (ci-après désignée « Loi sur le secteur privé ») ainsi qu'à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) (ci-après désignée « Loi sur l'accès »), c'est-à-dire que leurs dispositions prévalent sur celles d'une loi générale ou spéciale postérieure qui leur seraient contraires, à moins que ces autres lois y dérogent expressément¹.

La Loi sur l'accès encadre la collecte, l'utilisation, la communication, la conservation et la destruction des renseignements personnels détenus par les organismes publics alors que la Loi sur le secteur privé fait de même avec les renseignements personnels détenus par les personnes qui exploitent une entreprise au Québec.

L'évolution technologique des dernières décennies a soulevé des enjeux nouveaux et importants à l'égard de la protection des renseignements personnels des Québécois. L'avènement des entreprises dont le modèle d'affaires repose sur la commercialisation de renseignements personnels, le développement de nouvelles technologies utilisant les renseignements personnels tels que la biométrie et la reconnaissance faciale ainsi que les capacités d'analyse et de traitement d'une quantité toujours plus importante de renseignements personnels, notamment par l'utilisation de l'intelligence artificielle, amènent un lot de défis qui nécessitent une réflexion sur le cadre législatif applicable.

Par ailleurs, les récentes fuites de données qui ont compromis la confidentialité des renseignements personnels de nombreux Québécois ont révélé la nécessité de responsabiliser les entreprises et les organismes publics sur la protection des renseignements personnels. Entre juin et septembre 2019, quatre incidents de confidentialité d'envergure ont touché des Québécois (Mouvement Desjardins, Capital One, Revenu Québec et Industrielle Alliance). Depuis, plusieurs autres incidents ont fait l'objet

¹ Article 94 de la Loi sur le secteur privé et article 168 de la Loi sur l'accès.

de l'actualité. Par exemple, certains renseignements détenus par le ministère de l'Éducation et de l'Enseignement supérieur ont été dérobés. Ainsi, 360 000 enseignants peuvent être des victimes potentielles. Ces incidents soulèvent d'importantes préoccupations dans la population québécoise, dans un contexte où une fuite de données peut mener à un vol d'identité avec des conséquences importantes pour les victimes.

Finalement, le scandale Cambridge Analytica a soulevé de sérieuses questions sur l'utilisation des renseignements personnels des citoyens dans un contexte électoral. Les possibilités de microciblage politique permettant d'influencer indûment l'électorat à partir des renseignements personnels des électeurs ont entraîné une réflexion mondiale sur l'encadrement des renseignements personnels détenus par les partis politiques.

2- Raison d'être de l'intervention

Le contexte numérique et technologique introduit de nouveaux risques de vulnérabilités et de préjudices sérieux autant pour les organismes publics et les entreprises que pour les citoyens. La Loi sur l'accès, qui date de 1982, ainsi que la Loi sur le secteur privé, adoptée en 1993, doivent être modernisées à la lumière des enjeux contemporains.

Aujourd'hui plusieurs services offerts en ligne, tels que les moteurs de recherche et les médias sociaux, sont devenus des services quasi essentiels. Cependant, ces services sont fondés sur une commercialisation des renseignements personnels des usagers, lesquels se trouvent face à une perte de contrôle à l'égard de leur collecte, de leur utilisation et de leur communication. Le déséquilibre des forces entre les entreprises technologiques et le citoyen commande un rehaussement de la protection accordée aux renseignements personnels.

En outre, au Canada en général, mais également au Québec, les conséquences qu'entraîne le non-respect des règles de protection des renseignements personnels sont faibles par rapport au gain potentiel que peuvent en tirer les entreprises. Non seulement l'encadrement doit être rehaussé, mais les conséquences de son non-respect doivent être plus importantes pour en assurer l'effet dissuasif.

Dans le secteur public, les exigences administratives de la Loi sur l'accès peuvent constituer un frein ou ralentir les projets visant la transformation numérique de l'administration publique. La mise en place de services regroupés au bénéfice du citoyen nécessite une révision du cadre applicable aux échanges de renseignements personnels entre les organismes publics afin de favoriser la fluidité de ces renseignements.

La nouvelle vision de la protection des renseignements personnels au 21^e siècle doit être audacieuse, rigoureuse et fondée sur les meilleures pratiques afin de réduire les enjeux inhérents à la protection des renseignements personnels.

Le projet de loi s'inspire notamment du Règlement général sur la protection des données de l'Union européenne (ci-après désigné « RGPD ») qui constitue le cadre juridique le plus moderne en termes de protection des renseignements personnels et celui qui accorde le plus de droits aux citoyens et aux citoyennes. Elle s'inspire également de nombreuses recommandations émises par la Commission d'accès à l'information (ci-après désignée « CAI »), notamment dans son rapport quinquennal 2016 qui a fait l'objet d'une

consultation générale et d'auditions publiques en août 2017. Il vise enfin à harmoniser la Loi sur le secteur privé et la Loi sur l'accès à la législation fédérale.

En ce qui concerne les partis politiques, ceux-ci ne sont pas assujettis à un régime de protection des renseignements personnels. La Loi électorale traite de l'utilisation et de la communication de la liste électorale, mais ne contient aucune règle sur les autres renseignements personnels détenus par les partis politiques. Le Directeur général des élections recommandait, dans son dernier rapport annuel, d'assujettir les partis politiques à un encadrement législatif général en matière de protection des renseignements personnels. Celui-ci n'a toutefois pas pu examiner et évaluer les pratiques des partis politiques concernant les renseignements personnels des électeurs et en faire rapport à l'Assemblée nationale conformément au projet de loi numéro 188, *Loi modifiant la Loi électorale et d'autres lois concernant la protection des renseignements personnels des électeurs*, ce projet de loi n'ayant pas été adopté avant la fin de la législature précédente.

3- Objectifs poursuivis

Ce projet de loi vise une révision de la Loi sur le secteur privé, du volet « protection des renseignements personnels » de la Loi sur l'accès et de la Loi électorale. Cette révision s'appuie sur les orientations suivantes :

1) Favoriser la transparence et conférer un meilleur contrôle par le citoyen

Cette orientation vise à étendre les droits conférés aux citoyens (droit à la portabilité, droit à la suppression, droit d'opposition) et à augmenter les exigences de transparence.

2) Renforcer la confidentialité

Cette orientation a pour objectif de renforcer les règles de confidentialité des renseignements personnels, notamment par l'exigence que les organisations se dotent de règles de gouvernance et qu'ils aient l'obligation de détruire ou d'anonymiser les renseignements. Elle vise également à renforcer l'encadrement des communications de renseignements personnels dans le contexte de contrat de service et à donner suite aux principes de *Privacy by Design*² et de *Privacy by Default*³.

3) Renforcer le consentement

Cette orientation vise à renforcer la pierre angulaire du régime de protection des renseignements personnels : le consentement. Elle implique l'exigence d'un consentement distinct pour chaque fin et d'un consentement du titulaire de l'autorité parentale pour la collecte des renseignements personnels des jeunes de moins de 14 ans, sauf en cas d'urgence. Elle implique aussi l'obtention d'un

² Ce principe implique que les enjeux et les risques liés à la protection de la vie privée soient pris en considération dès la conception d'un système ou d'un programme, afin d'être en mesure de les identifier et de prendre les mesures pour les atténuer.

³ Ce principe implique que chaque système assure, par défaut et sans l'intervention de la personne concernée, le plus haut niveau de confidentialité.

consentement explicite pour la communication et l'utilisation à d'autres fins, avec le consentement de la personne, des renseignements personnels dits sensibles.

4) Favoriser la conformité et actualiser les pouvoirs de la CAI

Cette orientation vise notamment à augmenter le montant des amendes applicables, à permettre à la CAI d'imposer des sanctions administratives pécuniaires et à offrir une protection pour les personnes qui divulgueraient à la CAI une conduite répréhensible.

5) Soutenir la transformation numérique de l'État

Cette orientation vise à faciliter la communication de renseignements personnels entre certains organismes publics lorsque cela est au bénéfice du citoyen ou dans l'intérêt public, afin de reconnaître la nécessité du gouvernement, dans certaines circonstances, de travailler en réseau.

6) Moderniser les règles applicables et soutenir l'innovation

Cette orientation vise à moderniser la loi notamment en permettant la communication de renseignements personnels dans le cadre de transaction commerciale et en précisant les règles applicables aux renseignements anonymisés et aux renseignements dépersonnalisés.

7) Simplifier les obligations administratives

Cette orientation, applicable au secteur public, vise à simplifier les exigences administratives applicables aux organismes publics.

8) Encadrer les partis politiques

Cette orientation consiste à prévoir un encadrement des renseignements personnels concernant les électeurs et détenus par les partis politiques, adapté à leur contexte et à leur réalité.

4- Proposition

La proposition vise à renforcer et à moderniser l'encadrement en matière de protection des renseignements personnels de trois catégories d'organisation : les organismes publics, les entreprises et les partis politiques. Elle nécessite de modifier les lois suivantes :

- Loi sur la protection des renseignements personnels dans le secteur privé;
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels;
- Loi électorale.

4.1. Favoriser la transparence et conférer un meilleur contrôle par le citoyen

4.1.1. Bonification des informations transmises aux citoyens

Un citoyen bien informé est un citoyen qui peut exercer un certain contrôle sur ses renseignements. Il est proposé de bonifier l'information qui doit être fournie aux personnes concernées lors de la collecte de leurs renseignements personnels, notamment en les informant des fins pour lesquelles les renseignements sont recueillis, des moyens par lesquels les renseignements sont recueillis, de leurs droits et de la possibilité de retirer leur consentement. La personne concernée sera également informée, lorsqu'applicable, du fait que ses renseignements seront communiqués à l'extérieur du Québec ou utilisés pour rendre une décision fondée exclusivement sur un traitement automatisé. Certaines informations supplémentaires devront aussi être fournies sur demande, notamment la durée de conservation des renseignements ainsi que le nom du responsable de la protection des renseignements personnels. Cette bonification des informations transmises aux personnes favoriserait la transparence des entreprises, des organismes publics et des partis politiques à l'égard des citoyens en ce qui concerne leurs renseignements personnels.

En outre, puisque les renseignements personnels sont fréquemment collectés par un moyen technologique, et que cette collecte peut permettre de recueillir des renseignements à l'insu d'une personne, il est suggéré qu'une entreprise, un organisme public ou un parti politique qui collecte des renseignements personnels par un moyen technologique doit adopter et publier une politique de confidentialité accessible par l'entremise de son site Internet et contenant certaines informations spécifiques. Elle doit également être diffusée par tout moyen propre à atteindre les personnes concernées. Afin d'assurer la compréhension de la politique, celle-ci doit être rédigée en termes simples et clairs.

4.1.2. Droit à la portabilité

La Loi sur l'accès ainsi que la Loi sur le secteur privé encadrent le droit de toute personne d'avoir accès aux renseignements personnels qui la concernent et, sous certaines conditions, d'en demander la rectification et la suppression.

Il est souhaité de renforcer le contrôle du citoyen sur ses renseignements. Un des moyens de renforcer ce contrôle, inspiré d'un nouveau droit conféré aux citoyennes et citoyens européens par le RGPD, est l'inclusion du droit à la portabilité. La portabilité vise un double objectif, soit celui d'augmenter le contrôle du citoyen sur ses renseignements personnels et de faciliter le transfert des renseignements. Il est proposé d'ajouter ce droit, qui constitue en quelque sorte une extension du droit à la communication, et qui permet aux personnes d'obtenir les renseignements personnels qu'ils ont fournis sur un support technologique structuré et couramment utilisé. À la demande de la personne, ces renseignements seront communiqués à toute autre personne ou tout organisme autorisé par la loi à recueillir un tel renseignement.

Ce droit ne vise pas les renseignements qui sont créés, dérivés, calculés ou inférés à partir des renseignements fournis par la personne concernée (ex. : profil d'un utilisateur), lesquels peuvent avoir une valeur commerciale pour les entreprises. Par ailleurs, les

nouveaux systèmes d'information ou de prestation électronique de service devront permettre la portabilité.

4.1.3. Droit au déréférencement

Une personne physique peut faire supprimer un renseignement détenu par une entreprise à son sujet lorsque sa collecte n'est pas autorisée par la loi ou lorsque les fins pour lesquelles il a été collecté sont accomplies.

Les capacités actuelles de recherche dans un contexte technologique, notamment par le biais des moteurs de recherche, ainsi que la permanence de l'information publiée en ligne, soulèvent de nouveaux enjeux en matière de protection de la vie privée. C'est dans ce contexte qu'est apparu, en Europe, le « droit à l'oubli », qui comprend le « droit au déréférencement », c'est-à-dire le droit de faire désindexer dans un moteur de recherche certains liens hypertextes qui apparaissent lorsqu'une recherche est effectuée à partir du nom et du prénom d'une personne. Ce droit constitue en quelque sorte une extension du droit de suppression et une réponse au rôle central des moteurs de recherche. Dans certains cas, le déréférencement est une mesure plus effective et plus simple que la suppression des renseignements.

Une modification est introduite dans la Loi sur le secteur privé pour permettre à une personne de faire désindexer un hyperlien rattaché à son nom, c'est-à-dire de faire retirer le lien hypertexte d'un moteur de recherche, ou de faire cesser la diffusion d'un renseignement personnel qui la concerne lorsque sa diffusion contrevient à la loi ou à une ordonnance judiciaire. La personne concernée pourrait faire de même, ou faire déplacer le lien hypertexte, si la diffusion du renseignement lui cause un préjudice grave relatif au droit au respect de sa réputation ou de sa vie privée. Ce préjudice doit être manifestement supérieur à l'intérêt du public de connaître ce renseignement ou à l'intérêt de toute personne de s'exprimer librement et la cessation de la diffusion, la désindexation ou le déplacement demandé n'excède pas ce qui est nécessaire pour éviter la perpétuation du préjudice.

Cet ajout augmenterait le contrôle des personnes sur leurs renseignements personnels et leur donnerait accès à un mécanisme plus accessible que les tribunaux de droit commun pour protéger les atteintes à leur vie privée, soit une demande à l'entreprise suivie, au besoin, d'un recours à la section juridictionnelle de la CAI. À titre d'exemple, ce droit pourrait permettre à une victime d'acte criminel de faire supprimer les hyperliens relatifs à l'acte criminel qui sont générés lors d'une recherche effectuée avec le nom de la victime.

4.1.4. Droit d'opposition

Le droit d'opposition permet à une personne de s'opposer à ce que ses renseignements soient utilisés par une entreprise pour un objectif précis. Il se distingue du droit à l'effacement par le fait que l'entreprise conserve les renseignements, lesquels peuvent d'ailleurs être utilisés à certaines fins, mais ne peut plus les utiliser pour les finalités pour lesquelles la personne s'est opposée.

Actuellement, la Loi sur le secteur privé permet la communication et l'utilisation de liste nominative par une entreprise à des fins de prospection commerciale ou philanthropique,

dans la mesure notamment où les personnes concernées ont une occasion valable de refuser que leurs renseignements soient utilisés à cette fin.

Or, depuis l'adoption de la Loi sur le secteur privé en 1993, des mesures ont été prises au niveau fédéral, par le biais de la Loi canadienne antipourriel⁴, pour exiger un consentement exprès avant toute activité de prospection commerciale par message électronique commercial tel qu'un courriel ou un texto. Cette loi exige également la présence d'un mécanisme d'exclusion.

Cet encadrement témoigne d'un changement dans les mœurs et pratiques depuis que la Loi sur le secteur privé a été adoptée en 1993. À cette époque, la loi partait de la prémisse que les personnes étaient en accord avec l'utilisation de leurs renseignements personnels en prévoyant un droit de retrait, tandis que les nouvelles règles fédérales exigent un consentement clair. De ce fait, en matière de message électronique commercial, la règle d'« opting out » québécoise prévue dans la Loi sur le secteur privé cède le pas devant l'exigence d'« opting in » du fédéral.

Dans un souci de maximiser le contrôle du citoyen sur l'utilisation de ses renseignements, et d'assurer une cohérence entre les règles fédérales et celles de la Loi sur le secteur privé, et ce, sans égard au moyen par lequel est effectuée l'activité de prospection commerciale, il est proposé de modifier la Loi sur le secteur privé afin :

- d'exiger un consentement de la personne pour l'utilisation de ses renseignements à des fins de prospection commerciale ou philanthropique en supprimant les dispositions qui permettaient une telle prospection sans le consentement de la personne concernée;
- d'exiger que la personne soit informée de son droit de s'opposer à cette utilisation lorsqu'elle est contactée à des fins de prospection; et
- de prévoir le droit d'opposition de la personne.

4.1.5. Encadrement applicable aux renseignements personnels utilisés lors de la prise de décisions automatisées

Les décisions fondées exclusivement sur un traitement automatisé de renseignements personnels sont de plus en plus fréquentes et sont susceptibles d'affecter les personnes concernées. Il s'avère dès lors nécessaire de moderniser les lois sur la protection des renseignements personnels pour favoriser la transparence du processus décisionnel, pour que les personnes puissent garder le contrôle sur leurs renseignements personnels et pour s'assurer que la bonne décision soit rendue.

Il est proposé, dans un premier temps, que les entreprises et les organismes publics aient l'obligation d'informer la personne concernée lorsque ses renseignements personnels sont utilisés pour rendre une décision fondée exclusivement sur un traitement automatisé.

⁴ Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications (L.C. 2010, ch. 23)

La personne concernée pourra également, sur demande, connaître les renseignements utilisés par l'organisation et ayant mené à la décision. De plus, l'organisation devra fournir les raisons, ainsi que les principaux facteurs et paramètres, qui ont permis de rendre la décision et informer la personne concernée de son droit de faire rectifier les renseignements personnels utilisés pour rendre la décision. Cette orientation permet une transparence, sans nuire au secret industriel.

Finalement, il est proposé que la personne concernée ait l'occasion de présenter ses observations à un membre du personnel de l'entreprise en mesure de réviser la décision. Dans le secteur public, le droit de révision d'une décision administrative concernant un administré est généralement prévu dans les lois sectorielles et la Loi sur la justice administrative (chapitre J-3) prévoit les règles générales de procédures applicables à ces décisions.

4.1.6. Transparence à l'égard des mécanismes de localisation et de profilage

Il est prévu que lorsqu'une organisation recourt à des mécanismes susceptibles d'identifier, de localiser ou d'effectuer un profilage d'une personne physique, elle doit informer celle-ci de l'existence de ce mécanisme et des moyens offerts, le cas échéant, pour désactiver les fonctions de localisation, d'identification ou de profilage.

4.1.7. Transparence relative aux incidents de confidentialité

Lors de la survenance d'incidents de confidentialité mettant en cause des renseignements personnels, il est proposé d'ajouter des obligations aux organismes publics, aux entreprises et aux partis politiques.

Ainsi, il est proposé qu'en cas d'incidents de confidentialité, les organisations aient l'obligation de prendre les mesures requises afin de réduire les risques de préjudices pour les personnes concernées et aussi d'agir afin d'éviter que ce type d'incidents ne se reproduisent.

Dans les cas où un préjudice sérieux pour les personnes concernées pourrait s'ensuivre, les organisations seraient tenues d'informer celles-ci et d'aviser la CAI de l'incident.

Finalement, chaque organisation devrait tenir un registre de l'ensemble des incidents de confidentialité, lequel pourrait être consulté par la CAI au besoin. Les contenus et les modalités des avis à la CAI et aux personnes, ainsi que la teneur du registre, seraient précisés par voie réglementaire.

Ces nouvelles obligations iraient dans le sens des recommandations formulées par la CAI dans son rapport quinquennal 2011 et réitérées dans le rapport quinquennal 2016.

4.2. Renforcer la confidentialité

4.2.1. Renforcement de la gouvernance

La gouvernance, au sens de l'exercice de l'autorité de gestion aux plus hauts niveaux, se doit d'être renforcée dans les différentes organisations en matière de protection des

renseignements personnels. Les personnes responsables de la protection des renseignements personnels doivent assumer un leadership accru quant aux lois applicables.

Ainsi, des rôles et des responsabilités mieux définis et connus de chacun, de même qu'une implication accrue des plus hautes autorités administratives, participeraient à mettre en place ou à accroître une culture de protection des renseignements personnels.

La responsabilité

La modification proposée introduirait dans la loi de façon explicite le principe selon lequel chaque organisation est responsable de la protection des renseignements personnels qu'elle détient. Aux fins de l'exercice de cette responsabilité, il est proposé que chaque organisation ait l'obligation d'adopter et de publier les règles encadrant sa gouvernance à l'égard de la collecte, de l'utilisation, de la communication, de la conservation et de la destruction des renseignements personnels. Ces obligations s'appliqueraient aux entreprises, aux organismes publics et aux partis politiques.

La nomination d'une personne responsable

Dans le secteur public, la Loi sur l'accès prévoit que la personne ayant la plus haute autorité au sein de l'organisme public exerce les fonctions que la loi confère à la personne responsable de la protection des renseignements personnels. Elle prévoit en outre que cette personne peut déléguer cette fonction.

Il est proposé de modifier la Loi sur le secteur privé afin de conférer à la personne ayant la plus haute autorité au sein de l'entreprise ou du parti politique la fonction de responsable, laquelle pourrait également être déléguée. La personne responsable aura notamment comme fonction de traiter les demandes d'accès et de rectification.

Dans le secteur public, le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels prévoit l'obligation pour les organismes assujettis de mettre sur pied un comité sur l'accès à l'information et la protection des renseignements personnels qui relève du sous-ministre ou du dirigeant de l'organisme.

Il est proposé d'enchâsser cette obligation dans la Loi sur l'accès afin de marquer l'importance que l'application de la loi soit portée par les plus hautes instances administratives, que le comité exerce un leadership à cet égard, et incidemment, qu'il contribue à une culture organisationnelle où la protection des renseignements personnels devient partie intégrante des processus. Le comité serait notamment consulté pour les évaluations des facteurs relatifs à la vie privée de tout projet de système d'information ou de prestation électronique de services impliquant des renseignements personnels.

L'ajout de l'obligation de mettre en place un comité à même la loi aurait aussi pour effet d'étendre cette obligation à l'ensemble des organismes publics assujettis à la Loi sur l'accès, incluant les réseaux de la santé, de l'éducation et du secteur municipal. Le gouvernement pourra, par voie réglementaire, exclure certains organismes publics de l'obligation de former un comité ou modifier les obligations en fonction de critères qu'il définit, notamment pour tenir compte des organismes de très petite taille.

D'autre part, afin de dissiper certaines craintes ou perceptions lorsque l'organisme est dirigé par un élu, la fonction de responsable, et donc la responsabilité de traiter les demandes d'accès serait transférée de la personne élue vers le plus haut dirigeant administratif, soit, par exemple, le sous-ministre dans le cas des ministères et le directeur général dans le cas des municipalités.

4.2.2. Destruction des renseignements après utilisation

La limite à la conservation des renseignements personnels, c'est-à-dire l'obligation pour les organisations de détruire ou d'anonymiser les renseignements personnels lorsque les fins pour lesquelles ils ont été collectés sont atteintes, est un principe de base en matière de protection des renseignements personnels. La destruction des renseignements devenus inutiles peut permettre de diminuer la portée des incidents de confidentialité.

Actuellement, la Loi sur le secteur privé prévoit que l'utilisation des renseignements contenus dans un dossier n'est permise, une fois l'objet du dossier accompli, qu'avec le consentement de la personne sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement du gouvernement.

Puisque le gouvernement n'a pas adopté de règlement en application de cette disposition, aucun calendrier de conservation ne s'applique au secteur privé. L'absence de réglementation précisant le délai de conservation des renseignements personnels dans le secteur privé a amené la Cour du Québec⁵ à conclure qu'une entreprise peut conserver des renseignements personnels caducs même si elle ne peut plus les utiliser en vertu de la loi. Autrement dit, en vertu de la loi actuelle, une entreprise n'a pas d'obligation légale de détruire les renseignements personnels et la CAI n'a pas compétence pour lui ordonner de le faire.

Il s'agit d'une situation problématique qui devrait être corrigée. Selon la CAI, cette absence des règles en matière de conservation des renseignements personnels est une des plus importantes lacunes de la Loi sur le secteur privé.

La modification proposée vient corriger cette lacune et encadre la conservation et la destruction des renseignements personnels détenus par les entreprises, en les obligeant à détruire ou à anonymiser un renseignement personnel lorsque les fins pour lesquelles il a été recueilli sont accomplies.

Les organismes publics sont déjà soumis à une telle obligation.

4.2.3. Contrats de service ou d'entreprise

Il est possible pour une organisation de communiquer à un tiers des renseignements personnels dans le cadre de la réalisation d'un contrat de service ou d'entreprise. Dans le secteur public, cette communication fait l'objet d'un encadrement qui exige la signature d'une entente qui doit inclure certaines mesures de protection. L'article 20 de la Loi sur

⁵ Dans la décision *Équifax Canada inc. c. Fugère* [1998] CAI 510 (C.Q.), la Cour conclut que le pouvoir d'établir des délais de conservation appartient au gouvernement exclusivement et qu'en l'absence de règlement, une entreprise peut conserver des renseignements personnels caducs même si elle ne peut plus les utiliser en vertu de la loi.

le secteur privé permet cette communication, mais n'exige aucune mesure particulière ni la signature d'une entente.

Il est proposé que les entreprises et les partis politiques soient assujettis aux mêmes exigences que les organismes publics lorsqu'elles communiquent des renseignements personnels dans le cadre d'un contrat de service ou d'entreprise.

4.2.4. Protection de la vie privée dès la conception (Privacy by design)

Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels prévoit l'obligation pour les ministères et organismes du gouvernement d'évaluer certains de leurs projets technologiques impliquant des renseignements personnels, qu'il s'agisse d'acquisition, de développement ou de refonte d'un système d'information ou encore de prestation électronique de services.

L'évaluation des facteurs relatifs à la vie privée est un processus qui permet de déterminer si des initiatives comportant l'usage de renseignements personnels posent des risques pour la protection de la vie privée, de mesurer, décrire et quantifier ces risques ainsi que de proposer des solutions dans le but de les éliminer ou de les ramener à un niveau acceptable. Cet exercice oblige l'organisation à se questionner dès le début d'un projet sur les risques que celui-ci soulève et sur les mesures à prendre pour s'assurer du respect des principes de protection des renseignements personnels.

Il est proposé qu'une évaluation des facteurs relatifs à la vie privée soit exigée pour tout projet de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. Les dispositions réglementaires actuelles prévoient que cette évaluation est facultative. Cette modification viserait les organismes publics, les entreprises ainsi que les partis politiques.

Dans le secteur public, il est également proposé d'ajouter l'obligation que le comité sur l'accès à l'information et la protection des renseignements personnels soit consulté sur ces évaluations préalables, de manière à ce que les décisions, choix et orientations d'un projet technologique impliquant des renseignements personnels demeurent sous la responsabilité de l'instance qui en est ultimement imputable. En ce qui a trait aux partis politiques et aux entreprises, c'est la personne responsable de la protection des renseignements personnels qui serait consultée aux fins de cette évaluation.

Ces nouvelles obligations iraient dans le sens de recommandations formulées par la CAI dans son rapport quinquennal 2016.

4.2.5. Protection de la vie privée par défaut (Privacy by default)

Le principe de « privacy by default » ou de « protection par défaut » implique que les données à caractère personnel soient automatiquement protégées sans qu'aucune action supplémentaire ne soit requise de la part d'un particulier.

Autrement dit, ces mesures garantissent que, par défaut, les renseignements personnels ne sont pas rendus accessibles à un nombre indéterminé de personnes physiques ou morales sans l'intervention de la personne physique concernée.

Ainsi, lorsqu'un produit ou un service (application, média social, objet connecté) offre des paramètres de confidentialité (communication des données principalement), ces paramètres doivent au départ assurer le plus au niveau de confidentialité. Par la suite, la modification de ces paramètres doit nécessiter une intervention de la personne concernée.

Pour inscrire ce principe dans la Loi sur le secteur privé, il est proposé d'ajouter une disposition qui exige que les paramètres des produits ou des services offerts assurent le plus haut niveau de confidentialité sans aucune intervention de la personne concernée.

4.2.6. Encadrement des agents de renseignements personnels

La Loi sur le secteur privé prévoit un encadrement particulier pour les agents de renseignements personnels, c'est-à-dire pour toute personne qui fait le commerce de constituer des dossiers sur autrui, ce qui inclut les agences de crédit, mais également les agences d'investigation ou de recouvrement. Ces personnes doivent notamment s'inscrire à la CAI et un registre est diffusé sur le site de la CAI.

Il est proposé de modifier la Loi sur le secteur privé afin que les agents de renseignements personnels aient l'obligation d'établir et d'appliquer des modalités d'opérations propres à garantir que les renseignements personnels sont communiqués conformément à la loi. L'objectif de cette modification est que l'agent de renseignements personnels vérifie, par exemple, le consentement de la personne concernée afin de valider qu'il est en droit de communiquer les renseignements personnels.

Il est aussi proposé de modifier la loi afin de bonifier les informations que les agents de renseignements personnels doivent transmettre à la CAI, afin que celle-ci soit mieux informée au moment de l'inscription et ainsi, de faciliter son rôle de surveillance.

Il est finalement proposé de modifier la loi afin de préciser un délai de conservation maximal durant lequel les agents peuvent conserver les renseignements personnels qu'ils détiennent. Un délai de sept ans a été retenu, lequel s'inspire des pratiques déjà établies dans le domaine par les agences de crédit⁶.

4.3. Renforcer le consentement

Les renseignements personnels appartiennent à la personne concernée. Il importe donc qu'elle soit en mesure de consentir valablement à leur utilisation ou à leur communication à un tiers.

4.3.1. Critères de validité du consentement

Il est proposé d'introduire dans la Loi sur l'accès les critères selon lesquels le consentement d'une personne peut être considéré comme étant valide. Ces critères sont déjà précisés dans la Loi sur le secteur privé et la CAI les applique également au secteur public dans ses décisions en surveillance. De fait, les bonnes pratiques dans les

⁶ AGENCE DE LA CONSOMMATION EN MATIÈRE FINANCIÈRE DU CANADA, *Comprendre votre dossier de crédit et votre pointage de crédit*, mars 2016.

organismes publics consistent déjà à appliquer ces critères dans l'appréciation de la validité d'un consentement.

4.3.2. Consentement distinct

Le consentement est souvent obtenu par le biais de l'acceptation de conditions d'utilisation qui sont longues, complexes et peu accessibles au commun des mortels. En outre, les informations fournies aux personnes sont généralement évasives et peu précises à l'égard des renseignements collectés, de leur utilisation et de leur communication subséquente. Il est proposé d'une part, d'ajouter une obligation voulant que le consentement doit être demandé en termes simples et clairs. En outre, le consentement à l'utilisation ou à la communication des renseignements personnels devra être demandé de façon distincte pour chaque fin et séparément de toute autre information communiquée aux personnes, notamment le consentement à la relation contractuelle.

4.3.3. Consentement pour les renseignements personnels sensibles

Certains renseignements dits sensibles nécessitent un degré important de protection considérant les attentes plus élevées en matière de vie privée. Bien que les attentes en matière de vie privée liées à un renseignement personnel dépendent du contexte, certains renseignements sont généralement reconnus comme sensibles, notamment les renseignements de santé et ceux d'ordre financier. Il est proposé de renforcer le contrôle des personnes en exigeant un consentement exprès pour l'utilisation de ces renseignements à d'autres fins sur la base d'un consentement. Il en est de même pour une communication de ces renseignements avec consentement. De ce fait, les communications et les utilisations prévues par la loi ne nécessiteraient pas de consentement exprès. Le consentement exprès, ou explicite, exige que la personne pose une action pour exprimer son consentement. Par exemple, remplir un formulaire, cocher une case, répondre « oui » à une question, etc. Cette modification s'appliquerait aux organismes publics, aux entreprises et aux partis politiques et donnerait directement suite à une recommandation émise par la CAI dans son rapport quinquennal 2016.

4.3.4. Consentement pour les jeunes de moins de 14 ans

Les jeunes sont avides de nouvelles technologies et de grands utilisateurs d'Internet, ils y partagent des vidéos, photos, opinions et autres renseignements personnels. Les personnes mineures devraient bénéficier d'une protection particulière à l'égard de la collecte, de l'utilisation et de la communication de leurs renseignements personnels. Par ailleurs, le droit québécois reconnaît au mineur, généralement de 14 ans et plus, certains droits, notamment celui de contracter, de donner son consentement ainsi que le droit à la confidentialité dans le domaine de la santé.

Il est proposé d'exiger que, pour les jeunes de moins de 14 ans, la collecte, l'utilisation et la communication de leurs renseignements personnels nécessitent le consentement du titulaire de l'autorité parentale, autant dans le secteur public que dans le secteur privé.

4.4. Favoriser la conformité et actualiser les pouvoirs de la CAI

4.4.1. Sanctions administratives pécuniaires

Aujourd'hui, les renseignements personnels ont une grande valeur pour les entreprises et constituent une source de revenus considérable. Avec la logique économique qui prévaut, certaines entreprises pourraient prendre le risque de contrevenir aux lois sur la protection des renseignements personnels plutôt que d'adopter des pratiques qui limiteraient la valeur et la valorisation des renseignements personnels qu'elles détiennent. Des lois prépondérantes doivent, pour en assurer le respect, être accompagnées de mesures assurant un effet dissuasif.

Dans le cas contraire, l'organisme de surveillance peut se retrouver démuni et incapable d'assurer le respect de la loi, comme le dénonçait le commissaire à la vie privée du Canada en avril 2019. En Europe, le nouveau Règlement général sur la protection des données (RGPD) prévoit des sanctions pouvant s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial.

Dans la dernière année, les entreprises suivantes ont été sanctionnées pour des manquements aux lois régissant la protection des renseignements personnels :

- Google : 50 millions d'euros par la CNIL⁷ française;
- Tik Tok : 5,7 millions de dollars par la Federal Trade Commission américaine;
- British Airways : 183 millions de livres sterling (1,5 % du chiffre d'affaires) par le commissaire à l'information du Royaume-Uni.

Il est proposé de conférer à la CAI le pouvoir d'émettre des sanctions administratives pécuniaires dans le secteur privé pouvant s'élever jusqu'à 10 M\$ ou 2 % du chiffre d'affaires mondial si ce montant est plus élevé. En effet, pour être efficaces et atteindre leur objectif de dissuasion, les sanctions doivent être proportionnelles aux avantages que retire l'entreprise de l'utilisation des renseignements personnels et aux capacités de celle-ci. Ces sanctions doivent être assez élevées pour amener les entreprises à modifier leurs pratiques ou à investir dans la sécurité de l'information afin de mieux protéger les renseignements personnels.

4.4.2. Sanctions pénales

La Loi sur l'accès prévoit des pénalités et des sanctions pouvant s'appliquer en cas de non-respect de l'une ou l'autre de ses dispositions. Le fardeau de preuve lié à ces infractions est assez important pour le poursuivant qui doit démontrer l'intention coupable pour que le comportement ou l'action soit susceptible de constituer une infraction, compte tenu de l'emploi du mot *sciemment*.

Il est proposé d'alléger le fardeau de la preuve en retirant le terme *sciemment* dans les dispositions concernées puis d'augmenter le montant des amendes prévues à un niveau qui assure un certain effet dissuasif.

⁷ Commission nationale de l'informatique et des libertés

De manière corollaire, les infractions d'ordre général ne seraient pas retenues afin de ne conserver que les infractions spécifiques dont la gravité le justifie.

Par ailleurs, de nouvelles dispositions seraient ajoutées pour prévoir qu'en cas de récidive, l'amende prévue serait doublée et que toute poursuite pénale devrait être intentée dans les trois ans suivant l'infraction, alors que le Code de procédure pénale prévoit un délai d'un an.

Le tableau ci-dessous présente le montant des sanctions qui seraient applicables advenant l'adoption du projet de loi proposé.

	Personne physique		Autres	
	Min	Max	Min	Max
Secteur privé (SAP)	-	50 000 \$	-	10 M\$ ou 2 %
Secteur privé (pénal)	5 000 \$	50 000 \$	15 000 \$	25 M\$ ou 4 %
Secteur public (pénal)	5 000 \$	50 000 \$	15 000 \$	150 000 \$

4.4.3. Protection contre les dénonciations

Dans le secteur public, la Loi facilitant la divulgation d'actes répréhensibles à l'égard des organismes publics (RLRQ chapitre D-11.1) a pour objet de faciliter la divulgation d'actes répréhensibles et d'établir un régime général de protection contre les représailles. En vertu de cette loi, toute personne peut divulguer un acte répréhensible au protecteur du citoyen, au responsable du suivi des divulgations au sein de l'organisme public concerné ou à d'autres instances dans certaines situations (ex. : aux ministres responsables des affaires municipales pour les actes commis au sein d'une municipalité ou d'un organisme municipal).

La protection des renseignements personnels détenus par les entreprises est un enjeu important dont le non-respect peut avoir des conséquences majeures pour les personnes concernées. Pour faciliter l'identification des infractions, il s'avère pertinent d'offrir une protection contre les dénonciations aux employés œuvrant dans le secteur privé ou au sein d'un parti politique.

Il est proposé de modifier la Loi sur le secteur privé pour offrir une protection contre les dénonciations à l'égard du non-respect des règles de protection des renseignements personnels.

4.4.4. Ordonnance de sauvegarde et demande péremptoire

Il importe que la CAI détienne tous les outils et pouvoirs nécessaires à l'exercice de son rôle de surveillance des lois sur la protection des renseignements personnels.

Il est proposé d'attribuer à la CAI le pouvoir de rendre des ordonnances de sauvegarde afin de lui permettre d'agir dans un contexte d'urgence lors de la survenance d'un incident de confidentialité.

Il est également proposé que la CAI ait le pouvoir d'émettre des demandes péremptoires afin d'exiger de toute personne la production de tous renseignements permettant de vérifier l'application de la loi et des règlements.

4.5. Soutenir la transformation numérique de l'État

La Loi sur l'accès considère chaque organisme public, incluant chaque ministère, comme des entités distinctes. De ce fait, les communications des renseignements personnels entre les organismes publics sont généralement encadrées par un régime juridique qui exige certaines modalités administratives. Cet encadrement, qui date de l'adoption de la Loi sur l'accès en 1982, est peu adapté au contexte technologique actuel et à la nécessité d'offrir des services publics efficaces, intuitifs et à moindre coût. Cet encadrement constitue une entrave à la volonté gouvernementale de faciliter la vie du citoyen pour qu'il ne fournisse ses renseignements qu'une seule fois.

Il apparaît nécessaire de simplifier les échanges de renseignements personnels, tout en mettant en place un encadrement rigoureux en matière de protection des renseignements personnels, pour que le gouvernement puisse mettre en place des projets d'intérêt public ou au bénéfice des personnes concernées. On peut penser à des projets qui simplifieront l'admissibilité à un programme ou qui contribueront à une meilleure gestion des ressources du gouvernement.

Pour ce faire, il est proposé de permettre au gouvernement de désigner un ou plusieurs organismes publics pour exercer la fonction de gestionnaire de renseignements personnels. Ces organismes pourront collecter, utiliser ou communiquer les renseignements personnels nécessaires aux fins permises par la loi :

- la prestation de services communs, la réalisation de missions communes;
- l'accomplissement d'un mandat ou d'une initiative à portée gouvernementale;
- la vérification de l'admissibilité d'une personne à un programme ou une mesure;
- la planification, la gestion, l'évaluation ou le contrôle de ressources, de programmes ou de services gouvernementaux.

Pour concrétiser cette gestion et pour assurer une mise en œuvre qui assure un haut niveau de protection des renseignements personnels, le gestionnaire de renseignements personnels ainsi désigné devra faire approuver par la CAI les règles de gouvernance dont il s'est doté pour encadrer sa gouvernance à l'égard de ces renseignements avant de pouvoir procéder à leur collecte, à leur utilisation ou à leur communication.

En outre, le gestionnaire de renseignements personnels désigné devra procéder à une évaluation des facteurs relatifs à la vie privée avant de procéder à la collecte, à l'utilisation ou à la communication de renseignements personnels et devra produire et diffuser annuellement un rapport portant sur la gestion de ces renseignements.

En définitive, ce cadre juridique permettrait au gouvernement, pour certaines fins, de mettre en place des projets qui permettraient aux organismes publics de travailler en collaboration, plutôt qu'en silo. Cet encadrement faciliterait le transfert des renseignements tout en maintenant un haut niveau de protection des renseignements

personnels par l'intermédiaire d'un cadre de gouvernance rigoureux et chapeauté par la CAI.

4.6. Moderniser les règles applicables et soutenir l'innovation

4.6.1. Renseignements anonymisés et dépersonnalisés

Le projet de loi définit un renseignement anonymisé comme un renseignement concernant une personne physique ne permettant plus, de façon irréversible, d'identifier, directement ou indirectement, cette personne. Un renseignement anonymisé ne serait plus un renseignement personnel et ne serait donc plus visé par les dispositions des lois sur la protection des renseignements personnels.

Le projet de loi définit aussi un renseignement dépersonnalisé comme un renseignement personnel ne permettant plus d'identifier directement la personne concernée. Il s'agit de renseignements dont les identifiants directs ont été retirés, tels que le nom, le prénom, l'adresse ou un numéro unique comme le numéro d'assurance sociale (NAS) ou le numéro de permis de conduire. Ces renseignements sont toujours des renseignements personnels et sont soumis aux dispositions des lois sur la protection des renseignements personnels.

Ces deux termes seraient ainsi définis afin de clarifier la définition d'un renseignement anonymisé et ainsi d'éviter que les organisations croient à tort qu'un renseignement dépersonnalisé n'est pas soumis à la loi.

Par ailleurs, il est proposé de permettre l'utilisation des renseignements personnels dépersonnalisés à des fins d'étude, de recherche ou de production de statistiques. Cette disposition facilitera l'utilisation des renseignements personnels au sein des organisations dans un objectif d'étude et de recherche et devrait favoriser l'innovation dans le respect de la protection de la vie privée des personnes concernées.

Aussi, il est proposé de reconnaître dans le secteur privé, comme c'est déjà le cas dans le secteur public, la possibilité d'utiliser les renseignements personnels à des fins compatibles aux fins pour lesquelles ils ont été collectés. Une fin est compatible si elle a un lien direct et pertinent. Par exemple, l'utilisation des renseignements personnels collectés dans le cadre d'un contrat de service à des fins d'évaluation de la satisfaction de la clientèle peut être considérée comme une fin compatible.

4.6.2. Communication dans le cadre de transaction commerciale

Actuellement, la Loi sur le secteur privé ne permet pas de communiquer ou d'utiliser sans consentement des renseignements personnels lors d'une transaction commerciale, notamment en cas d'acquisition ou de fusion d'entreprise. Pourtant, la loi fédérale ainsi que celles de l'Alberta et de la Colombie-Britannique prévoient cette possibilité. Un tel ajout a fait l'objet de demandes de plusieurs intervenants du secteur privé⁸.

⁸ Notamment le Bureau d'assurance du Canada, la Fédération des chambres de commerce du Québec, Desjardins ainsi que l'association canadienne des compagnies d'assurance de personne.

Il est donc proposé de modifier la Loi sur le secteur privé afin de permettre la communication de renseignements personnels sans le consentement des personnes lors de transactions commerciales tout en mettant des mesures pour assurer la protection des renseignements, notamment l'obligation d'informer les personnes concernées dans un délai raisonnable suivant la transaction.

4.6.3. Retrait de la notion de dossier dans le secteur privé

La Loi sur le secteur privé permet à une entreprise de constituer un dossier sur autrui si elle a un intérêt sérieux et légitime. Or, plusieurs entreprises collectent, utilisent, communiquent et conservent des renseignements personnels, sans pour autant constituer un dossier au sujet d'une personne dans le cadre d'une relation contractuelle. Par exemple, certaines entreprises peuvent collecter des renseignements susceptibles d'identifier une personne physique en captant les images par une caméra de surveillance. Ces renseignements personnels détenus par l'entreprise ne sont pas conservés nécessairement dans un « dossier » identifié au nom d'un individu.

Le constat est donc que la notion de dossier sur laquelle est basée la Loi sur le secteur privé doit être modernisée. Cette modification donnerait suite à une recommandation émise par la CAI dans son rapport quinquennal 2016.

4.7. Simplification des obligations administratives

4.7.1. Communication de renseignements personnels sans le consentement dans le secteur public

Les articles 67 et 68 de la Loi sur l'accès permettent la communication de renseignements personnels sans le consentement des personnes dans diverses situations, principalement lorsque la communication est nécessaire à l'application d'une loi (art. 67) ou lorsqu'elle est nécessaire à l'exercice des attributions de l'organisme (art. 68). Le choix de l'une ou l'autre de ces dispositions a un impact sur les organismes puisque l'article 68 exige une autorisation préalable de la CAI, alors que l'article 67 permet une communication sans autorisation. Ces dispositions font l'objet de différentes interprétations au sein des organismes publics.

Il est proposé de clarifier la portée de ces deux dispositions. D'une part, il est proposé que les communications de renseignements personnels qui sont expressément prévus par la loi puissent continuer de se faire sans entente, tout comme les communications ponctuelles qui sont nécessaires à l'application d'une loi et qui ne concernent qu'un nombre restreint de personnes.

De ce fait, les communications de renseignements qui concernent un grand nombre de personnes ou qui sont continues dans le temps devront être faites via une entente écrite transmise à la CAI. Celle-ci entrera en vigueur 30 jours après sa réception par la CAI. L'autorisation au cas par cas de la CAI serait donc remplacée par une possibilité de réagir à l'intérieur du délai de 30 jours.

4.7.2. Communication à des fins de recherche

Au Québec, l'accès par les chercheurs aux renseignements personnels qui leur sont nécessaires à des fins de recherche, d'étude ou de production statistiques est encadré par un processus qui exige l'autorisation de la CAI et des organisations qui détiennent les renseignements personnels. En outre, les chercheurs doivent souvent obtenir l'autorisation d'un comité d'éthique de la recherche.

Ce processus a été qualifié comme étant lourd, long et complexe par des représentants du secteur de la recherche. La révision de ce processus a fait l'objet de travaux par un groupe de travail interministériel auquel participait le Scientifique en chef du Québec. La CAI a fait écho aux résultats de ces travaux collaboratifs dans son rapport quinquennal 2016.

Conformément au consensus dégagé lors des travaux du comité et à la recommandation de la CAI, il est proposé de modifier le processus par lequel les chercheurs demandent à recevoir des renseignements personnels détenus par un ou des organismes publics. De tels changements impliqueraient les modifications suivantes :

- les personnes s'adresseraient directement aux organismes publics qui détiennent les renseignements personnels requis à des fins de recherche, au lieu de demander l'autorisation préalable à la CAI;
- les conditions d'autorisation ainsi que les modalités seraient précisées afin que les règles en soient connues, tant par les organismes que par les chercheurs;
- la communication de renseignements personnels, le cas échéant, devrait faire l'objet d'une entente écrite;
- la CAI devrait recevoir une copie de l'entente conclue.

Cette modification contribuerait à une efficacité accrue de la CAI, du fait d'un volume moindre de dossiers à traiter, tout en simplifiant la démarche des chercheurs concernés. La simplification de la démarche et le fait que les conditions et critères d'application soient mieux connus contribueraient à réduire les itérations nécessaires et, incidemment, les délais d'obtention des renseignements par les chercheurs.

Dans le cadre du budget 2018-2019, le gouvernement du Québec a confié à l'Institut de la statistique du Québec le mandat de mettre sur pied un guichet unique d'accès aux données aux fins de recherche. Ce guichet unique serait soumis à un régime juridique défini dans la loi constitutive de l'Institut de la statistique du Québec. Le projet de guichet unique et la modification apportée par le présent projet de loi constituent des réponses complémentaires à une même problématique. En effet, ce guichet permettra l'accès uniquement à certains renseignements personnels fréquemment demandés par les chercheurs. En ce qui concerne les autres renseignements détenus par les organismes publics, la procédure prévue par le présent projet de loi s'appliquera.

4.7.3. Administration de la CAI

Le présent projet de loi propose de permettre à la CAI de se concentrer sur ses missions premières, soit la surveillance de l'application de la loi et les demandes de révision des demandes d'accès et de rectification.

Pour ce faire, il est notamment proposé de retirer l'autorisation préalable de la CAI pour les communications à des fins de recherche et pour les communications en vertu de l'article 68.

Il est aussi proposé d'accorder à la CAI le pouvoir d'interdire dans certains cas à une personne d'introduire une demande ou de présenter un acte de procédure dans une instance déjà introduite sans l'autorisation préalable du président de la Commission et selon les conditions que celui-ci détermine, c'est-à-dire de limiter le droit de recours devant la CAI d'une personne ayant indûment multiplié les procédures.

4.8. Encadrement des partis politiques

Il est proposé d'assujettir les renseignements personnels détenus sur les électeurs par les entités autorisés⁹, incluant les partis politiques, à la Loi sur la protection des renseignements personnels dans le secteur privé. Les partis politiques seraient donc visés par les règles applicables aux entreprises mentionnées précédemment ainsi qu'au pouvoir de surveillance de la CAI. Cependant, pour tenir compte de leurs particularités, certaines dispositions de cette loi ne leur seraient pas applicables et seraient remplacées par des dispositions spécifiques prévues à la Loi électorale.

Premièrement, les entités autorisées ne seraient pas visées par l'obligation générale de déterminer les finalités de la collecte avant celle-ci, de ne collecter que les renseignements personnels nécessaires et de ne pas utiliser les renseignements à d'autres fins que celle déterminée lors de la collecte.

En lieu et place de ces règles générales, et compte tenu du caractère homogène des activités des différents partis, la Loi électorale serait modifiée pour prévoir qu'une entité autorisée ne peut recueillir que les renseignements nécessaires à des fins électorales ou de financement politique et ne peut utiliser les renseignements ainsi recueillis qu'à ces fins.

Deuxièmement, les entités autorisées ne seraient pas assujetties à l'obligation de supprimer les renseignements personnels lorsque les fins pour lesquelles ils sont utilisés ont été accomplies. La mise en place de mesure pour assurer le respect du délai de conservation, et donc la destruction périodique de renseignements, pourrait s'avérer un fardeau disproportionné par rapport aux capacités des entités autorisées, voire même, favorisant les grands partis organisés ou détrimement des partis émergents. Il est plutôt proposé de ne pas exiger la destruction des renseignements personnels par les entités autorisées, mais de permettre à chaque personne de demander la suppression des renseignements personnels qui la concerne, à l'exception de ceux provenant de la liste électorale.

⁹ Est une entité autorisée, au sens de l'article 43 de la Loi électorale, un parti politique, une instance de parti, un député indépendant ou un candidat indépendant qui détient une autorisation du Directeur général des élections.

4.9. Autres modifications

4.9.1. Communication de renseignements personnels lors d'une infraction à la loi

L'article 59 de la Loi sur l'accès permet à un organisme public de communiquer un renseignement personnel à un organisme qui est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec. Cependant, selon une interprétation de l'article 60, qui encadre cette communication, un organisme public peut communiquer un renseignement dans ces conditions uniquement sur demande. Selon cette interprétation, un organisme ne pourrait pas, lorsqu'il constate une infraction, la dénoncer de sa propre initiative à un service de police. La modification proposée clarifie le fait que cette communication peut se faire à la suite d'une demande ou à l'initiative de l'organisme public.

4.9.2. Communications à l'extérieur du Québec

La Loi sur l'accès prévoit que les organismes publics doivent s'assurer, avant de communiquer des renseignements personnels à l'extérieur du Québec (pour des services infonuagiques ou autres), que ceux-ci y bénéficieront d'une protection équivalente. Cette disposition soulève des difficultés d'application.

La disposition concernée est modifiée en vue d'encadrer une telle communication, d'abord par l'obligation d'effectuer une analyse préalable des facteurs relatifs à la vie privée qui tient compte notamment du régime juridique qui s'applique dans l'État où il est envisagé de communiquer les renseignements.

Ainsi, les règles d'équivalence du régime juridique de l'État où seraient communiqués les renseignements ne constitueraient plus le seul critère applicable en vertu de la disposition. Ces règles deviendraient l'un des facteurs soupesés dans l'analyse préalable à la décision de communiquer ou non un renseignement à l'extérieur du Québec.

Il est également proposé d'ajouter l'obligation de conclure un contrat écrit avec l'instance concernée avant de procéder à une communication de renseignements personnels à l'extérieur du Québec, un tel contrat devant prévoir, dans la mesure du possible, toutes les mesures requises pour protéger les renseignements personnels.

Ces dispositions s'appliqueraient aux entreprises, aux organismes publics et aux partis politiques, assurant ainsi une protection uniforme à l'égard de flux transfrontaliers de renseignements personnels. Par ailleurs, ces modifications iraient dans le sens de recommandations de la CAI dans son rapport quinquennal publié en 2016.

L'évaluation par chaque organisation du degré d'équivalence d'un régime juridique, comme c'est actuellement le cas, soulève des enjeux de cohérence. Afin de simplifier le travail des organismes publics, mais aussi de nombreuses entreprises et des partis politiques qui devront appliquer ce critère, il est proposé que le ministre publie à la *Gazette officielle du Québec* une liste d'États dont le régime juridique encadrant les renseignements personnels équivaut aux principes de protection des renseignements personnels applicables au Québec.

4.9.3. Communication pour motifs de compassion

Dans son rapport quinquennal de 2016, la CAI a recommandé que la Loi sur l'accès puisse permettre la communication de certains renseignements personnels à des fins de compassion, par exemple, la photo d'une personne décédée pour aider un proche dans son processus de deuil.

Pour donner suite à cette recommandation, il est proposé d'ajouter à la Loi sur l'accès et à la Loi sur le secteur privé la possibilité de communiquer un renseignement personnel au conjoint ou à un proche parent d'une personne décédée si la connaissance de ce renseignement est susceptible d'aider le requérant dans son processus de deuil.

4.9.4. Report du rapport quinquennal

La CAI a l'obligation de produire un rapport aux cinq ans sur l'application de la Loi sur le secteur privé et de la Loi sur l'accès, le prochain rapport est prévu pour 2021. Or, compte tenu des modifications importantes qui seraient apportées à ces deux lois, il est proposé de reporter en 2026 l'obligation de la CAI de produire le prochain rapport quinquennal. En effet, la valeur ajoutée d'un rapport quinquennal portant sur une loi qui viendrait tout juste d'entrer en vigueur paraît faible. Notons que lors des modifications apportées à la Loi sur l'accès et à la Loi sur le secteur privé en 2006, l'obligation de déposer un rapport quinquennal avait été reportée par le projet de loi en 2011.

5- Autres options

5.1. Aucune intervention

Le statu quo aurait pour effet d'accentuer le fossé entre le cadre juridique visant la protection des renseignements personnels et les risques découlant des nouvelles technologies, des pratiques des organismes publics, des entreprises et de celles des partis politiques. L'absence de modernisation de cet encadrement juridique dans un contexte de progression de l'intelligence artificielle et de la valorisation des données massives présente un risque de déséquilibre en défaveur du citoyen et d'effritement graduel du droit à la vie privée des personnes physiques ainsi qu'une perte de confiance de la population.

5.2. Intervenir à l'égard d'un seul ou de deux secteurs

Une intervention à l'égard d'une ou de deux catégories d'organisation (entreprise / organisme public / parti politique) peut être envisagée. Cependant, les citoyens ont des préoccupations à l'égard de la collecte, de l'utilisation et de la communication de leurs renseignements personnels sans égard à la catégorie d'organisation qui les détient. La mise en place d'un encadrement similaire pour l'ensemble des organisations constitue une réponse complète susceptible de rassurer la population.

6- Évaluation intégrée des incidences

6.1. Incidences sur les citoyens

Le projet de loi prévoit de nouveaux droits au bénéfice du citoyen, notamment le droit à l'effacement, le droit d'opposition, la portabilité ainsi que diverses mesures de transparence et d'information lui permettant entre autres de mieux comprendre quels renseignements sont collectés à son sujet et à quelles fins.

6.2. Incidences sur les entreprises

Le projet de loi a pour effet d'imposer certaines nouvelles obligations aux personnes qui exploitent une entreprise au Québec. Les coûts liés à ces nouvelles obligations sont estimés à 68 M\$ lors de l'implantation et de 52 M\$ de coûts récurrents par année. Ces coûts sont établis pour l'ensemble des entreprises.

Par ailleurs, certaines mesures offriront davantage de souplesse pour les entreprises, notamment la possibilité de communiquer des renseignements personnels dans le cadre de transaction commerciale (fusion, acquisition, etc.) et la possibilité d'utiliser les renseignements dépersonnalisés à des fins d'étude, de recherche ou de statistique.

6.3. Incidences sur les municipalités

Les municipalités sont assujetties à la Loi sur l'accès et donc aux nouvelles règles et obligations qui sont proposées dans le présent projet de loi. Ces modifications auront un impact sur les municipalités et les organismes paramunicipaux assujettis. Afin de tenir compte de leur capacité, il est prévu que le gouvernement puisse, par règlement, exclure de l'obligation de former un comité sur l'accès à l'information et la protection des renseignements personnels certains organismes publics. Les autres obligations prévues au projet de loi proposé s'appliqueraient aux municipalités sans possibilité d'adaptation.

7- Consultation entre les ministères et avec d'autres parties prenantes

La CAI, le ministère de la Justice, le Secrétariat du Conseil du trésor, le ministère des Finances ainsi que des experts de la société civile ont été consultés durant le processus de révision de la loi. Pour les éléments qui étaient déjà inclus dans le projet de loi numéro 179, plusieurs organismes publics avaient été consultés en 2017 et 2018. Les modifications qui donnent suite aux recommandations de la CAI ont fait l'objet d'une consultation générale et d'auditions publiques tenues par la Commission des institutions en 2017 dans le cadre de l'étude du rapport quinquennal 2016.

Dans le secteur privé, un comité consultatif a été formé avec quatre associations représentatives, soit la Fédération canadienne de l'entreprise indépendante, la Fédération des chambres de commerce du Québec, le Conseil du patronat du Québec, et le Conseil québécois du commerce de détail. En général, les entreprises accueillent bien les modifications proposées quoiqu'elles anticipent une certaine lourdeur administrative. Elles souhaitent également que les obligations imposées par les modifications s'arriment avec la législation fédérale puisque plusieurs entreprises sont à la fois assujetties à la loi québécoise et à la loi fédérale.

8- Mise en œuvre, suivi et évaluation

À partir de 2026 et par la suite à chaque période de cinq ans, la CAI produira un rapport quinquennal sur l'application de la Loi sur l'accès et de la Loi sur le secteur privé. Ce rapport fera l'objet d'un dépôt à l'Assemblée nationale et d'une consultation publique en commission parlementaire. Cette évaluation périodique de l'application de ces deux lois permettra d'assurer un suivi de la mise en œuvre par l'Assemblée nationale sur la base des observations et recommandations d'un organisme indépendant.

9- Implications financières

Les solutions proposées ne nécessiteraient pas que des crédits budgétaires supplémentaires soient octroyés pour leur réalisation.

En effet, le coût de la mise en œuvre et les coûts récurrents sur cinq ans sont estimés à quelque 6,6 M\$ pour l'ensemble des quelques 120 ministères et organismes du gouvernement, ce qui représente un coût moyen de 11 550 \$ par année par ministère ou organisme. La période de cinq ans est calculée depuis la sanction de la loi, ce qui inclut un délai précédant l'entrée en vigueur qui pourrait s'appliquer.

Concernant le secteur privé, les coûts estimés dans l'analyse d'impact réglementaire sont de 68 M\$ lors de l'implantation et de 52 M\$ de coûts récurrents par année.

10- Analyse comparative

Dans le cas d'une réforme de cette envergure, il est essentiel de considérer les avenues qui ont été privilégiées par certains pays. La présente proposition de réforme s'inspire principalement de l'Union européenne (RGPD), de la législation fédérale et de celles des autres provinces canadiennes.

Le RGPD inclut les mesures suivantes qui ont inspiré certaines modifications du projet de loi proposé :

- un droit à la portabilité;
- un droit d'effacement et un droit au déréférencement;
- un droit à la limitation du traitement des données;
- un droit d'opposition;
- l'obligation de réaliser des évaluations des facteurs relatifs à la vie privée;
- la protection de la vie privée par défaut;
- l'obligation d'obtenir le consentement du titulaire de l'autorité parentale pour les jeunes de moins de 16 ans;
- la notification obligatoire des incidents de confidentialité;
- l'encadrement des décisions automatisées;
- des sanctions administratives pouvant s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial si ce montant est plus élevé.

La loi californienne prévoit également le droit à la portabilité des données.

La Children's Online Privacy Protection Act – 1998 (COPPA) américaine prévoit l'obligation d'obtenir le consentement des parents pour la collecte des renseignements personnels des jeunes de moins de 14 ans.

La modification qui permet au gouvernement de désigner des organismes publics pour exercer les fonctions de gestionnaire de renseignements personnels s'inspire d'encadrements similaires prévus dans la loi ontarienne applicable au secteur de la santé¹⁰ et dans celle applicable aux organismes publics¹¹.

La modification qui permet la communication de renseignements personnels lors de transactions commerciales ainsi que celle qui exige la nomination d'un responsable de la protection des renseignements personnels s'appuient sur des dispositions similaires prévues dans la loi fédérale, la loi de la Colombie-Britannique et celle de l'Alberta.

Ministre responsable des Institutions
démocratiques, de la Réforme électorale et
de l'Accès à l'information,

Madame Sonia LeBel

¹⁰ Loi de 2004 sur la protection des renseignements personnels sur la santé, L.O. 2004, chap. 3

¹¹ Loi sur l'accès à l'information et la protection de la vie privée, L.R.O. 1990, chap. F.31