



Commission d'accès
à l'information
du Québec

Transparence et vie privée : protéger la démocratie à l'ère numérique

Rapport quinquennal — 2026

Transparence et vie privée : protéger la démocratie à l'ère numérique

Rapport quinquennal — 2026

Ce rapport est disponible sur le site Web de la Commission d'accès à l'information du Québec à l'adresse suivante: www.cai.gouv.qc.ca

Avertissement : Le présent rapport se veut essentiellement un document d'analyse et de réflexion sur l'encadrement actuel de l'accès à l'information et de la protection des renseignements personnels ainsi que des renseignements de santé et de services sociaux. À ce titre, les propos qu'il contient et les exemples de pratiques utilisés pour illustrer ces propos ne doivent pas, d'aucune façon, être considérés comme liant la Commission et ses membres dans l'exercice de leurs fonctions juridictionnelles et de surveillance. L'inclusion des exemples de pratiques ne doit pas non plus être interprétée comme une affirmation de leur légalité en contexte québécois.

Pour préparer ce rapport, la Commission a consulté de la documentation publiée avant le 17 avril 2026. Les développements ultérieurs à cette date ne sont pas pris en compte.

Dépôt légal – 2026

Bibliothèque et Archives nationales du Québec

ISBN 978-2-555-03796-0 (version imprimée)

ISBN 978-2-555-03795-3 (version électronique)

Tous droits réservés pour tous les pays.

© Gouvernement du Québec – 2026



Québec, mai 2026

Monsieur Jean-François Roberge

Ministre de la Langue française

Ministre responsable de la Francophonie canadienne

Ministre responsable de la Laïcité

Ministre responsable des Institutions démocratiques

Ministre responsable de l'Accès à l'information

et de la Protection des renseignements personnels

875, Grande Allée Est

3^e étage, secteur 500

Québec (Québec) G1R 4Y8

Monsieur le Ministre,

Conformément aux dispositions de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels dans le secteur privé*, j'ai le plaisir de vous transmettre le rapport quinquennal 2026 de la Commission d'accès à l'information du Québec, intitulé *Transparence et vie privée : protéger la démocratie à l'ère numérique*.

Veillez agréer, Monsieur le Ministre, l'expression de mes sentiments distingués.

La présidente,

LISE GIRARD



Mot de la présidente

Québec, mai 2026



Déjà dix ans se sont écoulés depuis le dernier rapport quinquennal de la Commission : des transformations majeures se sont enchaînées pendant cette période. Le présent rapport tombe à point nommé, alors qu'il permet de marquer un temps d'arrêt et d'évaluer, rétrospectivement et prospectivement, les lois québécoises sur l'accès à l'information et la protection des renseignements personnels.

Qu'avons-nous constaté au fil de la dernière décennie?

Par-dessus tout, les technologies numériques se sont immiscées dans tous les aspects de nos vies individuelles, sociales et professionnelles, entraînant des bouleversements dans nos habitudes.

L'information qui circule dans nos sociétés émane désormais d'une variété de sources reflétant une grande pluralité de points de vue sur le monde. Cependant, l'hyperpersonnalisation des flux d'information par l'effet des algorithmes de recommandation et la prolifération de contenus trompeurs contribuent à la fragmentation des repères communs.

Dans ce contexte, il peut devenir ardu de discerner la vérité. La transparence gouvernementale trouve ici toute sa pertinence : la diffusion d'informations fiables permet aux débats de s'ancrer sur des références partagées. Cette transparence donne, en outre, l'heure juste sur les activités de l'administration publique.

Les organismes publics génèrent aussi plus d'informations que jamais, sous l'impulsion du numérique. Les pratiques de gestion de l'information doivent être adaptées à cette nouvelle réalité.

Depuis sa création, la Commission souligne l'effet des technologies sur la vie privée. Celui-ci n'a fait que s'intensifier avec le brouillement des frontières entre les mondes physique et numérique. Les exemples foisonnent : les appareils connectés sont omniprésents, les rencontres amoureuses se font sur des applications, les parents et les amis se partagent leur géolocalisation, et les systèmes d'intelligence



artificielle font office, pour certains, de conseillers, voire de confidents. Quelles activités humaines ne comportent pas encore une dimension numérique?

Les entreprises qui offrent ces technologies collectent de plus en plus de renseignements personnels, dont certains particulièrement sensibles. Or, cette vaste collecte propulse des modèles d'affaires visant à capter l'attention et à dresser des profils détaillés sur les personnes. Ces organisations en acquièrent un grand pouvoir d'influence et de décision.

Les technologies permettent ainsi de faire la lumière sur les individus, et même sur des groupes entiers de personnes. À l'inverse, les pratiques des organisations sont des plus complexes et opaques. Cette asymétrie informationnelle constitue l'un des grands enjeux de notre temps.

Ces phénomènes ne connaissent pas de frontières. Les plateformes numériques sont accessibles partout dans le monde. Les données voyagent d'un bout à l'autre de la planète en un instant. Des considérations nouvelles, de souveraineté numérique par exemple, font ainsi leur entrée dans le débat public.

Une certitude anime donc la Commission : plus que jamais, à l'ère numérique, la transparence administrative et la vie privée doivent être protégées en tant que socles de la démocratie.

Face aux enjeux de société soulevés dans le présent rapport, le Québec doit oser aller plus loin.

Sur le plan normatif, nos lois doivent être à la hauteur des défis. En particulier, le régime d'accès aux documents de la Loi sur l'accès, autrefois avant-gardiste, ne garantit plus la transparence dont a besoin la société québécoise d'aujourd'hui.

En matière de protection des renseignements personnels, le législateur a agi. De récentes réformes ont amené plusieurs obligations pour les organisations, petites et grandes. Experts et praticiens se sont alliés pour rechercher les façons optimales de s'y conformer. Leur point de vue et leur expérience seront des plus précieux alors qu'une réflexion collective renouvelée s'impose face aux enjeux du numérique.

Sur le plan culturel, les organisations doivent faire vivre concrètement la transparence et la protection de la vie privée. Cela peut notamment passer par une plus grande diffusion proactive, des initiatives novatrices minimisant la collecte de renseignements personnels ou encore de nouveaux modèles de gouvernance collective de l'information. La collaboration entre les parties prenantes sera l'une des clés de la réussite.

Enfin, l'État québécois devra déployer des moyens suffisants au service de ces efforts. La pleine efficacité des régimes d'accès et de protection des renseignements personnels en dépend.

Par où commencer? Dans ce rapport quinquennal, la Commission formule de nombreuses recommandations qui peuvent servir de tremplin pour atteindre les objectifs énoncés précédemment.

En terminant, je tiens à souligner le dévouement exceptionnel de toutes les personnes œuvrant au sein de la Commission qui, de près ou de loin, ont participé à la production de ce rapport. Ce travail réflexif s'est ajouté à celui qu'elles accomplissent au quotidien pour incarner la mission de la Commission, au service de l'intérêt public. Chacune des pages qui suivent témoigne de leur compétence et de leur effort soutenu. Je les remercie pour leur contribution à l'amélioration de la transparence et de la protection de la vie privée au Québec.

Lise Girard



Table des matières

Mot de la présidente	II
Table des matières	IV
Liste des sigles et abréviations	VII
Introduction	1
1. L'accès aux documents des organismes publics	6
Introduction	7
1.1. La portée et la prépondérance de la Loi sur l'accès	11
1.1.1. Les critères d'assujettissement à la Loi	11
1.1.2. Les dérogations à la Loi et les régimes particuliers	18
1.2. Le traitement des demandes d'accès	32
1.2.1. Les restrictions au droit d'accès	32
1.2.2. La consultation non systématique des tiers	58
1.2.3. Les délais de traitement des demandes par les organismes publics	62
1.3. La culture des organismes en matière de transparence	78
1.3.1. Les ressources dévolues à l'accès à l'information	78
1.3.2. La gestion de l'information	85
1.3.3. L'absence d'une obligation de documenter	97
1.3.4. La diffusion proactive	102
1.4. Le portrait statistique du système d'accès à l'information	125
1.4.1. Contexte	125
1.4.2. Situation actuelle	126
1.4.3. Enjeux	128
1.4.4. Recommandation	131
1.4.5. Pour aller plus loin	133
2. La protection des renseignements personnels	138
Introduction	139
2.1. Les éléments justifiant des ajustements aux lois actuelles	143



2.1.1. Le paradigme du contrôle individuel	143
2.1.2. Le critère de nécessité	168
2.1.3. Les inférences algorithmiques	181
2.1.4. Le moissonnage de renseignements personnels	197
2.1.5. Le courtage en données	205
2.1.6. L'anonymisation des renseignements personnels	215
2.1.7. L'évaluation des facteurs relatifs à la vie privée	227
2.1.8. Les interfaces truquées	246
2.1.9. Les enjeux particuliers relatifs à la vie privée des jeunes	259
2.1.10. Les dispositions concernant la biométrie	268
2.2. Une nouvelle approche de la protection des renseignements personnels à l'ère numérique	272
2.2.1. Contexte	272
2.2.2. Appel à une réflexion collective	274
2.2.3. Pistes pour alimenter la réflexion	274
3. La loi sur les renseignements de santé et de services sociaux	283
Introduction	285
3.1. Situation actuelle	287
3.2. Enjeux	290
3.2.1. Des outils, des procédures et des infrastructures technologiques nécessaires à l'application de la LRSSS sont manquants	290
3.2.2. L'absence de journalisation de l'accès aux renseignements entrave la transparence envers les personnes concernées	293
3.2.1. La LRSSS soulève d'ores et déjà certains importants enjeux d'interprétation	296
3.3. Recommandations	301
3.3.1. Accélérer la mise en place d'outils et rendre la journalisation complète obligatoire	301
3.3.2. Envisager des modifications législatives pour clarifier l'interprétation de la Loi	302
4. La Commission d'accès à l'information	304
Introduction	305
4.1. La capacité d'agir de la Commission	307
4.1.1. Les ressources financières et humaines disponibles	307
4.1.1. L'indépendance administrative	323
4.2. L'appel des décisions de la section juridictionnelle	327
4.2.1. Contexte et situation actuelle	327



4.2.2. Enjeux	327
4.2.3. Recommandation	328
4.3. Le caractère objectif des manquements passibles de sanctions administratives pécuniaires	330
4.3.1. Contexte	330
4.3.2. Situation actuelle	331
4.3.3. Enjeux	332
4.3.4. Recommandation	333
4.4. L'accompagnement des entreprises	334
4.4.1. Contexte	334
4.4.2. Situation actuelle	335
4.4.3. Moyens mis en œuvre par la Commission	337
4.4.4. Conclusion	342
Table des recommandations du Rapport quinquennal 2026	344
Annexe 1 – Table des recommandations du Rapport quinquennal 2016	355
Annexe 2 – Compilations de données en accès dans sept juridictions	364



Liste des sigles et abréviations

AAPI	Association des professionnels en accès à l'information et en protection de la vie privée	LGRI	<i>Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, c. G-1.03)</i>
AIPD	Analyse d'impact sur la protection des données	LGSSS	<i>Loi sur la gouvernance du système de santé et de services sociaux (RLRQ, c. G-1.021)</i>
BAnQ	Bibliothèque et Archives nationales du Québec	Loi 25	<i>Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (LQ 2021, c. 25)</i>
CAI	Commission d'accès à l'information	Loi sur l'accès	<i>Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1)</i>
Charte	<i>Charte des droits et libertés de la personne (RLRQ, c. C-12)</i>	Loi sur le privé	<i>Loi sur la protection des renseignements personnels dans le secteur privé (RLRQ, c. P-39.1)</i>
CPVPC	Commissariat à la protection de la vie privée du Canada	LPCRS	<i>Loi concernant le partage de certains renseignements de santé (RLRQ, c. P-9.0001)</i>
CSESJ	Commission spéciale sur les impacts des écrans et des médias sociaux sur la santé et le développement des jeunes	LQE	<i>Loi sur la qualité de l'environnement (RLRQ, c. Q-2)</i>
EFVP	Évaluation des facteurs relatifs à la vie privée	LRSSS	<i>Loi sur les Renseignements de santé et de services sociaux (RLRQ, c. R-22.1)</i>
ETC	Équivalent temps complet		
FIP	<i>Fair information practice (principles)</i>		
FPT	Fédéral, provinces et territoires		
GPEN	Global Privacy Enforcement Network		
IA	Intelligence artificielle		
LCCJTI	<i>Loi concernant le cadre juridique des technologies de l'information (RLRQ, c. C-1.1)</i>		



LSSSS	<i>Loi sur les services de santé et les services sociaux</i> , version antérieure au 1 ^{er} juillet 2024 (RLRQ, c. S-4.2)	OCDE	Organisation de coopération et de développement économiques
MCN	Ministère de la Cybersécurité et du Numérique	PME	Petite(s) et moyenne(s) entreprise(s)
Obvia	Observatoire international sur les impacts sociétaux de l'IA et du numérique	RGPD	<i>Règlement général sur la protection des données</i> de l'Union européenne (UE 2016/679)
		SRIDAIL	Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité



Introduction

Depuis près de 45 ans déjà, la Commission d'accès à l'information (la Commission) voit à l'application et à la promotion des lois sur l'accès à l'information et sur la protection des renseignements personnels au Québec et, depuis peu, d'une loi spécifique aux renseignements de santé et de services sociaux. Elle veille ainsi au respect de droits qui sont fondamentaux en démocratie. La transparence des organismes publics est une condition essentielle d'une participation citoyenne significative aux activités de l'État et de l'imputabilité du gouvernement. La protection de la vie privée assure que les renseignements personnels sont traités de manière légitime et conforme, tout en permettant aux personnes d'exercer pleinement l'ensemble de leurs droits et libertés. Elle a en outre une valeur inestimable pour la collectivité, agissant comme rempart contre l'exploitation injustifiée de renseignements personnels dans une société libre et démocratique¹.

L'importance qu'accorde l'État québécois à l'accès à l'information et à la protection des renseignements personnels se manifeste de plusieurs façons. Historiquement, le Québec a été une figure de proue. Dès 1982, il a adopté la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*² (la Loi sur l'accès). En 1994, la *Loi sur la protection des renseignements personnels dans le secteur privé*³ (la Loi sur le privé) a étendu la protection des renseignements personnels au secteur privé, une première en Amérique du Nord. Le législateur a aussi voulu que ces lois aient un statut prépondérant⁴, leur conférant ainsi un caractère quasi constitutionnel. Enfin, il a souhaité que la Commission amorce périodiquement un processus de révision de ces lois. Cette révision permet de prendre en compte l'évolution des attentes des citoyens en matière de transparence et de vie privée ainsi que les progrès technologiques, lesquels ne cessent de bouleverser les cadres établis.

Ainsi, la Commission a eu l'occasion de produire, au fil de son histoire, six rapports quinquennaux à l'intention du gouvernement sur l'application des lois qu'elle surveille⁵. Chaque fois, elle a rappelé l'importance des deux volets de sa mission et a proposé des améliorations au régime d'accès à l'information et de protection des renseignements personnels.

Le dernier rapport quinquennal de la Commission remonte à 2016⁶. La Commission y recommandait une révision substantielle de la législation en matière d'accès aux documents des organismes publics ainsi que de nombreux changements au régime de protection des renseignements personnels.

¹ Ces motifs sont à l'origine même du régime d'accès à l'information et de protection des renseignements personnels au Québec. Voir COMMISSION D'ÉTUDE SUR L'ACCÈS DU CITOYEN À L'INFORMATION GOUVERNEMENTALE ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, *Information et liberté*, Québec, Direction générale des publications gouvernementales, 1981.

² *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1 [ci-après *Loi sur l'accès*].

³ *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1 [ci-après *Loi sur le privé*].

⁴ *Loi sur l'accès*, art. 168; *Loi sur le privé*, art. 94.

⁵ *Loi sur l'accès*, art. 179; *Loi sur le privé*, art. 88.

⁶ Les recommandations formulées dans ce rapport sont reproduites à l'annexe 1. COMMISSION D'ACCÈS À L'INFORMATION, *Rétablir l'équilibre*, 2016 [ci-après *Rapport quinquennal 2016*], en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_RQ_2016.pdf>. Un rapport quinquennal devait être produit en 2021, mais l'échéance a été repoussée en raison de l'adoption contemporaine de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021, c. 25.



Au cours des dix dernières années, c'est surtout en matière de protection des renseignements personnels que la législation québécoise a été bonifiée. La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (la Loi 25), une réforme importante, a aligné le régime québécois aux plus hauts standards mondiaux. Elle est entrée en vigueur en trois phases principales, dont la dernière a eu lieu en septembre 2024. Parallèlement, en juillet 2024, une troisième loi générale est entrée en vigueur, soit la *Loi sur les renseignements de santé et de services sociaux*⁷ (la LRSSS). Une variété d'autres modifications législatives évoquées au fil du présent rapport ont introduit d'autres règles particulières.

En ce qui a trait à l'accès aux documents, peu de choses ont changé, bien que la Commission ait demandé à maintes reprises une réforme en profondeur, et en dépit de l'adoption unanime par les parlementaires d'une motion en faveur de cet exercice⁸. En effet, la Loi 25 n'a apporté qu'un nombre limité de bonifications en cette matière, telles que l'autonomie des responsables de l'accès et leur devoir de prêter assistance aux demandeurs⁹.

Au-delà du contexte législatif, force est d'admettre que le paysage géopolitique, technologique et social s'est radicalement transformé en une décennie.

La pandémie de COVID-19 a secoué le monde. À partir de mars 2020, la place du numérique dans nos vies s'est considérablement accrue. Le télétravail et l'utilisation des technologies de l'information et des communications modernes se sont imposés dans notre quotidien, tant dans le cadre du travail que dans le maintien des liens sociaux. La pandémie a aussi fait émerger des interrogations sur l'importance accordée à la vie privée en contexte de crise, notamment lorsqu'il était question de traçage des contacts, notamment par le biais d'applications¹⁰ ou de registres tenus par divers établissements¹¹, de passeports vaccinaux¹² ou d'exploitation à grande échelle de données de mobilité¹³. Par ailleurs, il a pu être constaté à maintes reprises que la transparence des gouvernements constitue une condition essentielle à la confiance et à la mobilisation des citoyens au service d'une cause commune. Cette transparence s'est en outre révélée une composante majeure de la lutte contre la désinformation et la mésinformation¹⁴, lesquelles ont proliféré en

[ci-après Loi 25], en ligne :

<https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2021/2021C25F.PDF>.

⁷ *Loi sur les renseignements de santé et de services sociaux*, RLRQ, c. R-22.1 [ci-après LRSSS].

⁸ ASSEMBLÉE NATIONALE DU QUÉBEC, « Procès-verbal de l'Assemblée - Le jeudi 5 mai 2022 », dans *Journal des débats de l'Assemblée nationale*, 46-56, 2022, en ligne : <http://www.assnat.qc.ca/Media/Process.aspx?MediaId=ANQ.Vigie.Bll.DocumentGenerique_183039>.

⁹ Loi sur l'accès, art. 8 et 50.

¹⁰ COMMISSION D'ACCÈS À L'INFORMATION, *Avis de la Commission d'accès à l'information sur le volet provincial du Système national de notification d'exposition Alerte COVID*, Québec, 2020, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_Avis_Alerte_COVID_2020-11-10.pdf>.

¹¹ Divers arrêtés et décrets adoptés en 2020 et 2021 imposaient ainsi à des établissements comme des bars, des restaurants ou des résidences pour aînés de tenir un registre des clients ou des visiteurs, contenant leur nom et leurs coordonnées, visant à faciliter le travail des autorités de santé publique pour retracer les cas de COVID-19.

¹² COMMISSAIRES FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX À LA PROTECTION DE LA VIE PRIVÉE, « La vie privée et les passeports vaccinaux relatifs à la COVID-19 », *Commissariat à la protection de la vie privée du Canada* (19 mai 2021), en ligne : <https://www.priv.gc.ca/fr/nouvelles-du-commissariat/discours-et-declarations/2021/s-d_20210519/> (consulté le 28 avril 2026).

¹³ COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Enquête sur la collecte et l'utilisation de données dépersonnalisées sur la mobilité dans le cadre de la pandémie de COVID-19 » (29 mai 2023), en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-institutions-federales/2022-23/pa_20230529_aspc/> (consulté le 28 avril 2026).

¹⁴ COMMISSAIRES ET OMBUDS FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX RESPONSABLES DE L'ACCÈS À L'INFORMATION, « La confiance, la transparence et la démocratie à l'ère de la mésinformation », *Commissariat à l'information du Canada* (8 octobre 2025), en



temps de pandémie. Ces phénomènes se sont depuis complexifiés : on a vu apparaître récemment de faux médias relayant uniquement du contenu généré par l'intelligence artificielle (**IA**), s'appropriant et déformant du matériel journalistique authentique¹⁵.

Le monde traverse aussi une période d'instabilité. L'État de droit connaît une certaine érosion dans plusieurs pays, notamment à travers des reculs en matière de transparence et de protection de la vie privée. Certaines réformes rendent les procédures d'accès à l'information plus longues et plus exigeantes et augmentent la discrétion des organismes publics de refuser certains documents¹⁶. Aux États-Unis, des milliers de pages Web et de données scientifiques ont été retirées des sites gouvernementaux¹⁷. Lorsque les informations pertinentes sont moins accessibles à la société civile, il lui devient d'autant plus difficile de comprendre ou de contester les choix gouvernementaux. Par ailleurs, certains gouvernements se procurent des jeux de données auprès de courtiers privés, ou encore mettent en commun des bases de données gouvernementales, à diverses fins de surveillance et de contrôle¹⁸. Des technologies comme la reconnaissance faciale, la surveillance des médias sociaux ou la géolocalisation des appareils mobiles sont exploitées en ce sens¹⁹.

Ces bouleversements profonds sont contemporains d'évolutions technologiques majeures, qui se traduisent entre autres par la présence accrue des objets connectés. Téléphones, montres ou lunettes intelligentes, téléviseurs, voitures ou assistants vocaux : tous participent à la captation et à la création de données toujours plus nombreuses concernant les personnes. La popularité des environnements numériques, qu'il s'agisse de sites Web, d'applications, de logiciels de communication professionnelle ou de plateformes qui hébergent du contenu audiovisuel, ne se dément pas.

Les personnes évoluent ainsi dans un monde où s'imposent les technologies numériques et prévalent des modèles d'affaires reposant sur la surveillance et le traitement de renseignements personnels. Les nouvelles technologies en développement – pensons aux neurotechnologies, au calcul quantique et, surtout, à l'**IA** – laissent d'ailleurs présager la production de renseignements personnels toujours plus révélateurs et une intensification de l'exploitation des données.

Ainsi, les avancées en apprentissage profond²⁰, puis en **IA** générative, représentent un point de bascule pour la société. Les modèles d'**IA** d'aujourd'hui sont entraînés sur des sommes colossales de données comportant des renseignements personnels, que les organisations acquièrent notamment par le

ligne : <<https://www.oic-ci.gc.ca/fr/ressources/communiqués-presse/les-autorités-de-contrôle-du-canada-en-matière-d'accès-l'information#confiance>> (consulté le 6 novembre 2025).

¹⁵ CONSEIL DE PRESSE DU QUÉBEC, « Décision D2026-01-008 » (13 mars 2026), en ligne : <<https://conseildepresse.qc.ca/decisions/d2026-01-008/>> (consulté le 15 mars 2026).

¹⁶ Dean BEEBY, « Federal, provincial governments reducing public access to information », *Investigative Journalism Foundation* (13 avril 2026), en ligne : <<https://theijf.org/article/governments-limiting-foi>> (consulté le 14 avril 2026).

¹⁷ Ethan SINGER, « Thousands of U.S. Government Web Pages Have Been Taken Down Since Friday », *The New York Times* (2 février 2025), en ligne : <<https://www.nytimes.com/2025/02/02/upshot/trump-government-websites-missing-pages.html>> (consulté le 14 avril 2026). Voir aussi Mélanie MELOCHE-HOLUBOWSKI, « Sauver les données scientifiques de la purge numérique de l'administration Trump », *Radio-Canada* (15 février 2025), en ligne : <<https://ici.radio-canada.ca/nouvelle/2140521/donald-trump-donnees-scientifiques-web>> (consulté le 14 avril 2026).

¹⁸ Alexandra BERZON, Hamed ALEAZIZ, Nicholas NEHAMAS, Ryan MAC et Tara Siegel BERNARD, « Social Security Lists Thousands of Migrants as Dead to Prompt Them to 'Self-Deport' », *The New York Times* (10 avril 2025), en ligne : <<https://www.nytimes.com/2025/04/10/us/politics/migrants-deport-social-security-doge.html>> (consulté le 14 avril 2026).

¹⁹ Eva DOU, « ICE amps up its surveillance powers, targeting immigrants and antifa », *The Washington Post* (17 octobre 2025), en ligne : <<https://www.washingtonpost.com/technology/2025/10/17/ice-surveillance-immigrants-antifa/>> (consulté le 14 avril 2026).

²⁰ OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « apprentissage profond », en ligne : <<https://vitrlinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26532876/apprentissage-profond>> (consulté le 28 avril 2026).



moissonnage de milliers de sites Web, par exemple des médias sociaux²¹. Ils se distinguent par leur puissante capacité d'exploration des données massives, dont ils peuvent tirer des inférences sur les personnes et les groupes.

L'**IA** s'impose désormais dans le quotidien de chacun, que ce soit au travail, dans le cadre de sa vie personnelle ou dans ses relations avec les organisations privées et publiques. Les modèles basés sur des réseaux de neurones artificiels²², dont le fonctionnement est opaque, seront entre autres mobilisés pour soutenir la prise de décision, voire pour rendre des décisions entièrement automatisées sur les personnes à partir de leurs renseignements personnels. L'**IA** apporte par ailleurs de nouveaux développements technologiques dans son sillage. C'est le cas par exemple de la vidéosurveillance algorithmique, de l'estimation de l'âge par l'analyse de traits faciaux ou encore de l'hypertrucage.

Dans ce contexte, certaines organisations voient leur capital informationnel grandir, et avec lui, leur pouvoir. Les citoyens sont quant à eux plus que jamais observés et profilés, mais en toute opacité. Privés de l'information pertinente, ils ne peuvent pas, autant qu'ils pourraient le vouloir, réagir, questionner ou modifier leurs choix individuels ou collectifs.

Devant tant de bouleversements, la Commission réaffirme l'importance cruciale de l'accès à l'information et de la protection des renseignements personnels pour l'État de droit. À travers ce septième rapport quinquennal, elle recommande des changements à la hauteur des enjeux contemporains, et ce, afin de protéger les assises démocratiques de la société.

Dans le premier chapitre, elle réitère l'urgence d'une réforme en profondeur de la Loi sur l'accès. Elle formule des recommandations notamment pour en étendre la portée, en raffermir la prépondérance et améliorer le traitement des demandes d'accès aux documents, en plus de se pencher sur la culture des organismes en matière de transparence et sur les statistiques concernant le système d'accès à l'information.

Dans le deuxième chapitre, la Commission s'intéresse aux phénomènes contemporains qui affectent la protection des renseignements personnels²³. Face à l'économie de la donnée et aux nouvelles technologies, elle propose diverses améliorations aux lois dans la continuité de la Loi 25. Cependant, comme le numérique met en lumière les limites dans les fondations mêmes des lois sur la protection des renseignements personnels, au Québec comme ailleurs, elle appelle à une réflexion collective visant à penser le futur de cet encadrement.

Dans le troisième chapitre, la Commission aborde la LRSSS, dont l'entrée en vigueur est encore récente. Si cette loi constitue une véritable révolution pour le secteur de la santé et des services sociaux, force est d'admettre que tout n'est pas encore en place pour qu'elle atteigne les fins recherchées. La Commission formule des recommandations pour la rendre mieux applicable.

²¹ Notamment, les entreprises qui possèdent les plateformes de médias sociaux utilisent certaines publications des abonnés pour entraîner leurs propres modèles. Voir LINKEDIN, « Mise à jour de nos Conditions générales et de notre utilisation des données », *LinkedIn*, en ligne : <<https://www.linkedin.com/help/linkedin/answer/a8059228>> (consulté le 28 avril 2026); et META, « IA par Meta: plus de transparence sur nos données d'entraînement », *Meta*, en ligne : <<https://transparency.meta.com/features/ai-at-meta-training-data/>> (consulté le 28 avril 2026).

²² Un réseau de neurones artificiels est un « [e]nsemble organisé de neurones artificiels interconnectés, créé dans le but d'effectuer des opérations complexes ou de résoudre des problèmes grâce à un mécanisme d'apprentissage. » Voir OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « réseau de neurones artificiels », *Grand dictionnaire terminologique*, en ligne : <<https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8386038/reseau-de-neurones-artificiels>> (consulté le 29 avril 2026).

²³ Dans ce rapport, par souci de simplicité, le terme « renseignements personnels » englobe les renseignements de santé et de services sociaux au sens de la LRSSS. Cette seconde notion est utilisée lorsque le contexte requiert plus de précision.



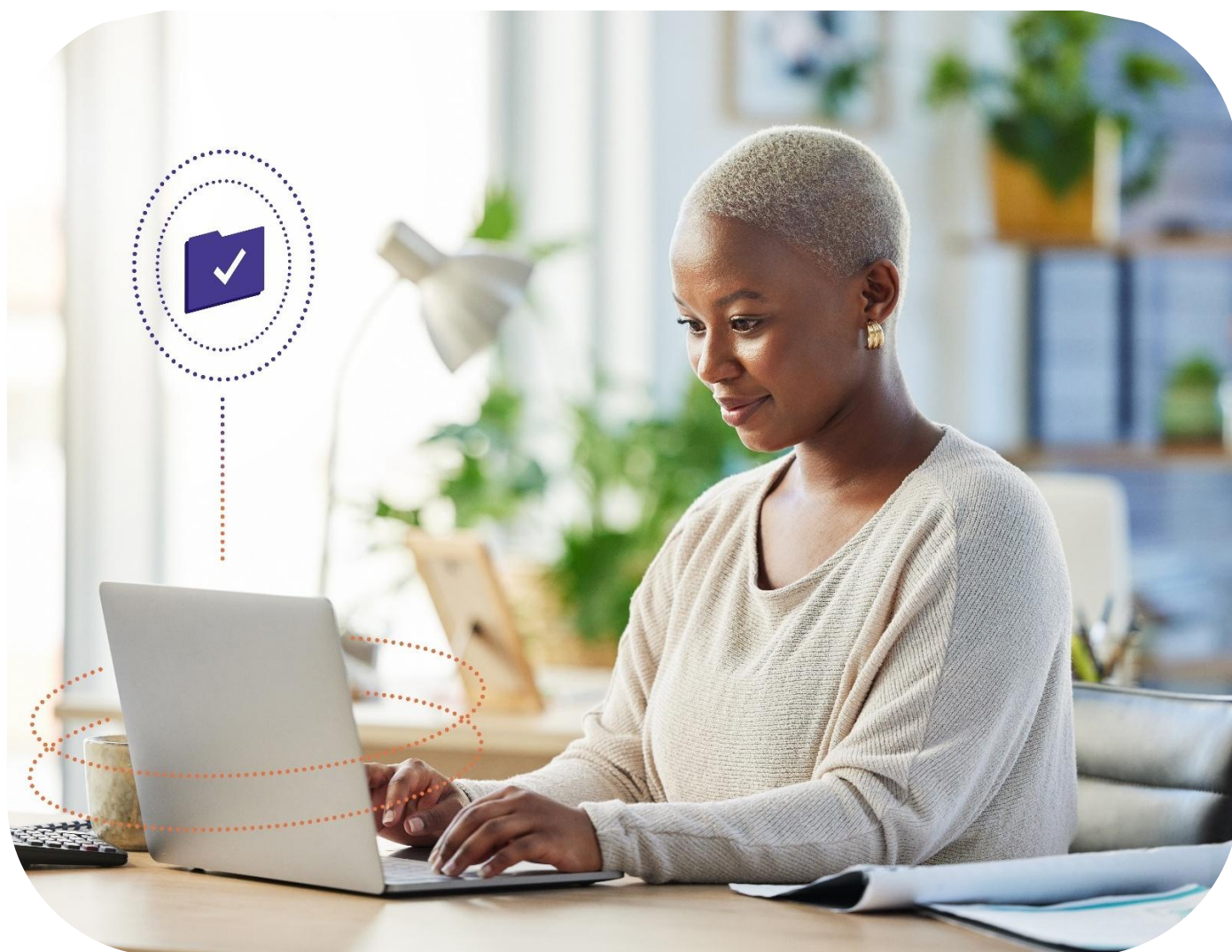
Enfin, le quatrième chapitre porte sur la Commission en tant qu'autorité indépendante chargée de l'accès à l'information et de la protection des renseignements personnels. Considérant son rôle névralgique, elle souligne entre autres l'importance qu'elle dispose des moyens nécessaires pour s'acquitter pleinement de sa mission.

Portée par le respect qu'elle voue à cette mission si importante pour la santé démocratique, et considérant la façon dont les choses évoluent à l'ère numérique, la Commission estime qu'il est temps d'améliorer significativement le régime d'accès aux documents et de faire preuve d'audace en vue de compléter le régime en protection des renseignements personnels. En mettant de l'avant 74 recommandations dans ce rapport quinquennal, la Commission invite le législateur et la société civile à une réflexion d'avenir.



CHAPITRE 1

1. L'accès aux documents des organismes publics





Introduction

La Loi sur l'accès constitue un véritable pilier de la démocratie. Depuis maintenant 44 ans, elle garantit l'exercice du droit quasi constitutionnel à l'information²⁴. Au cœur de la Loi sur l'accès se trouvent des objectifs de transparence, d'imputabilité et de participation citoyenne, autant d'éléments essentiels à la démocratie telle que nous la connaissons.

« Plusieurs manifestations de la démocratie sont largement tributaires de l'accès à l'information détenue par l'État. Exercice du droit de vote pour le choix de nos dirigeants, reddition de compte de l'administration publique, voire même liberté d'expression, liberté d'opinion ou liberté de presse ne seraient que des coquilles vides s'ils ne pouvaient s'appuyer sur une information de qualité. Transparence et démocratie vont donc de pair.

[...] Outre qu'elle favorise une meilleure reddition de compte, la transparence de l'administration publique engendre aussi l'adoption de meilleures politiques qui prennent en compte les besoins et opinions de la population.

Tel que l'a déjà précisé la Cour suprême du Canada, une loi en matière d'accès à l'information favorise la démocratie en garantissant aux citoyens l'accès à l'information nécessaire pour participer utilement au processus démocratique et en obligeant les politiciens à rendre compte de leurs activités²⁵. »

Mais cette loi porte avec elle le poids de son âge. Bien qu'elle s'appuie sur des principes toujours pertinents, elle met en œuvre un régime d'accès aux documents des organismes publics qui n'a pas fait l'objet de modifications substantielles depuis son adoption en 1982, à l'exception de l'ajout du principe de diffusion automatique en 2006²⁶.

Chaque année, le fossé entre les dispositions de la Loi sur l'accès et la réalité se creuse davantage. L'évolution technologique, entre **IA** et traitement massif des données, bouleverse les activités de l'administration publique. L'instantanéité des échanges et l'utilisation parfois interchangeable des appareils professionnels et personnels modifient le contexte dans lequel gouvernants et fonctionnaires débattent et prennent des décisions. La masse informationnelle détenue par les organismes publics ne cesse de croître au fil de l'adoption de nouveaux outils numériques qui facilitent la production et la conservation dématérialisée de l'information.

À travers la planète, des attaques de plus en plus fréquentes visent les fondements de la démocratie, et ce, dans plusieurs États où l'on aurait cru de telles atteintes impossibles. La désinformation et la mésinformation façonnent un terreau fertile pour le cynisme et fragilisent le tissu social en altérant notre perception commune de la vérité.

²⁴ Charte des droits et libertés de la personne, RLRQ, c. C-12, art. 44 [ci-après Charte].

²⁵ COMMISSION D'ACCÈS À L'INFORMATION, *Une réforme de l'accès à l'information : le choix de la transparence*, 2002 [ci-après Rapport quinquennal 2002], p. 10-11, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_RQ_2002.pdf>.

²⁶ Par le truchement de la *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*, LQ 2006, c. 22, en ligne : <https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2006/2006C22F.PDF>.

« La mésinformation peut façonner les opinions, les comportements, voire les politiques publiques. Elle peut déformer le débat public, influencer des élections, nuire à la santé et à la sécurité publiques, déstabiliser les économies et, en définitive, saper la compréhension mutuelle nécessaire à la prise de décisions collectives dans une société démocratique. Dans ce contexte, l'accès du public à des informations fiables revêt une importance primordiale²⁷. »



Dans ce contexte éminemment dynamique, 44 ans sans réforme paraissent une éternité. Les conséquences de la désuétude de la Loi sur l'accès – et de l'opacité qui s'installe parfois dans son sillage – se font sentir notamment par l'allongement des délais avant d'obtenir l'information et la divulgation insuffisante de documents d'intérêt public.

Le décalage croissant entre les objectifs de la Loi sur l'accès et la manière dont elle est appliquée, d'une part, et le contexte social, administratif, politique, économique et environnemental d'aujourd'hui, de l'autre, ne cesse de rendre plus pressante une refonte du régime d'accès aux documents. Ce message d'urgence, la Commission le lance depuis des années déjà. Elle plaide ainsi pour une révision en profondeur de la Loi afin de mieux répondre aux attentes légitimes de la population en matière de transparence et de participation aux débats publics. Il y a dix ans, dans son plus récent rapport quinquennal, elle formulait un ensemble de recommandations pour une modernisation de la Loi²⁸. Débattu en commission parlementaire, ce rapport a rallié un grand nombre d'intervenants autour d'un consensus sur la nécessité d'une réforme.

La présentation d'un projet de loi aux tout derniers jours de la 41^e législature, en 2018²⁹, mort au feuillet, constitue la dernière ambition de réforme majeure en date. La Loi 25³⁰, adoptée en 2021, se concentrait sur la protection des renseignements personnels. Elle n'a permis la concrétisation que de quelques-unes des recommandations de la Commission en matière d'accès³¹.

C'est avec tout le poids de son rôle de gardienne du droit d'accès aux documents que la Commission insiste aujourd'hui : une réforme de la Loi sur l'accès s'impose urgemment pour renouveler ce rempart démocratique.

²⁷ COMMISSAIRES ET OMBUDS FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX RESPONSABLES DE L'ACCÈS À L'INFORMATION, préc., note 14.

²⁸ Rapport quinquennal 2016.

²⁹ Kathleen WEIL, *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, 179 (présenté - 17 mai 2018), 41^e lég., 1^{re} sess., RLRQ [PL179], en ligne : <<https://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-179-41-1.html?appelant=MC>> (consulté le 28 octobre 2025).

³⁰ Loi 25.

³¹ Comme une plus grande marge de manœuvre dans l'examen des demandes d'autorisation des organismes publics de ne pas tenir compte de certaines demandes d'accès, ou encore une précision quant à l'autonomie du responsable de l'accès aux documents.



L'Assemblée nationale du Québec lançait le même message en 2022 en adoptant à l'unanimité une motion où les parlementaires ont résolu³² :

[QUE l'Assemblée nationale] reconnaisse que la transparence et l'accès à l'information sont le gage d'une information de qualité pour les citoyens;

QU'elle affirme que l'esprit de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels est de rendre disponible un maximum d'information et d'assurer la plus grande transparence;

QU'elle rappelle que la non-divulgaration de renseignements devrait constituer l'exception;

QU'elle insiste sur le fait qu'un employé ne devrait jamais avoir à choisir entre la loyauté à son employeur et son devoir de rendre l'information disponible en vertu de la loi;

QU'elle condamne avec vigueur toutes tentatives d'ingérence ou d'intimidation envers les responsables de l'analyse des demandes d'accès à l'information;

QU'elle demande au gouvernement d'accorder des ressources suffisantes à la Commission d'accès à l'information du Québec pour mener à bien sa mission;

Considérant ce qui précède, qu'elle affirme l'importance de procéder à une réforme de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels afin que la divulgation devienne la norme;

Enfin, qu'elle souligne l'apport des journalistes dans le maintien du droit à l'accès à l'information.

À l'heure actuelle, le classement international des lois sur l'accès à l'information réalisé par le Centre for Law and Democracy octroie à la Loi sur l'accès une note de 81 points sur une possibilité de 150³³. Elle se place ainsi au 11^e rang parmi les 14 lois canadiennes, y compris la loi fédérale. Dans une perspective plus large, cette note la rend comparable à celles des États-Unis, du Burkina Faso ou du Honduras : elle occuperait le 79^e rang sur 142 lois dans le classement international. Le Québec peut mieux faire et témoigner à nouveau de l'avant-gardisme qui l'a mené à adopter une loi sur l'accès aux documents bien avant de nombreuses autres juridictions, en 1982.

On a vu se succéder au Canada, ces dernières années, diverses réformes effectives ou projetées des lois sur l'accès aux documents : au Manitoba, en Nouvelle-Écosse, en Ontario, en Alberta, en Colombie-Britannique et au fédéral. Les gouvernements qui en sont à l'origine ont souvent affirmé que ces réformes visaient à tenir compte de la complexité croissante de la gestion des demandes d'accès par les organismes publics et du plus grand volume de documents à traiter. **Dans l'ensemble, malgré certaines avancées concernant notamment les pouvoirs des homologues de la Commission et une base de diffusion proactive, les changements appliqués ou envisagés semblent généralement entraîner une diminution de la portée ou de la simplicité d'exercice du droit d'accès et conférer une discrétion accrue aux organismes publics pour traiter les demandes et décider de l'accessibilité des documents**³⁴. Par exemple, plusieurs réformes prévoient l'introduction de critères concernant le degré de précision requis des demandes d'accès, l'allongement des délais de traitement et l'extension de la portée

³² ASSEMBLÉE NATIONALE DU QUÉBEC, préc., note 8 aux pages 1011-1012.

³³ CENTRE FOR LAW AND DEMOCRACY, *Quebec Assessment*, 2012, en ligne : <<https://www.law-democracy.org/wp-content/uploads/2026/03/Quebec-Assessment.xls>>. Le classement repose sur 61 indicateurs relatifs à l'énonciation du droit d'accès, à la portée de la loi, à la procédure d'exercice du droit d'accès, aux restrictions, aux sanctions et aux mesures de promotion.

³⁴ Dean BEEBY, préc., note 16.



de certaines restrictions à l'accès concernant notamment les documents relatifs aux activités du Conseil exécutif et des cabinets.

La réforme québécoise qu'appelle la Commission devrait plutôt être audacieuse et avoir comme points de mire l'augmentation de la transparence de l'administration publique ainsi que la facilitation de l'accès à l'information par les citoyens, tout en tenant compte de la réalité des organismes publics.

Les recommandations formulées par la Commission dans le présent chapitre contribuent à ces objectifs. L'application de plusieurs d'entre elles pourrait certes atténuer l'intensité des enjeux évoqués à l'appui d'autres, mais pour la Commission, une refonte partielle de la Loi sur l'accès ne suffira pas. Les pierres de son édifice sont interdépendantes et toutes garantes de sa solidité. Une réforme complète garantirait la synergie des effets positifs attendus. Bon nombre de propos et de recommandations de la Commission formulés en 2016 sont toujours aussi pertinents dix ans plus tard. C'est pourquoi elle revient sur plusieurs des thèmes abordés alors et incite le législateur à agir d'une manière dont elle a déjà tracé les contours à l'époque.

Dans ce chapitre, la Commission :

- revient sur la portée et la prépondérance de la Loi sur l'accès en préconisant l'extension des critères d'assujettissement de même qu'une révision des dérogations et des régimes particuliers qui constituent des exceptions;
- aborde différents aspects du traitement des demandes d'accès par les organismes publics, en recommandant une refonte complète des restrictions au droit d'accès, mais aussi la consultation systématique des tiers par les organismes et des actions permettant d'améliorer les délais qui s'écoulent avant la transmission d'une décision aux demandeurs;
- revient sur diverses fondations d'un système d'accès en santé, soit la suffisance des ressources dévolues à cette fonction par les organismes, la saine gestion de l'information, l'obligation de documenter les décisions et le renforcement de la diffusion proactive;
- plaide pour une meilleure reddition de comptes au sujet de l'application même de la Loi sur l'accès.



1.1. La portée et la prépondérance de la Loi sur l'accès

1.1.1. Les critères d'assujettissement à la Loi

Sommaire

La Commission constate que certaines activités de l'administration publique ne sont pas assujetties à la Loi sur l'accès lorsqu'elles sont confiées à des organismes issus de nouveaux modes de gestion financière et économique de l'appareil gouvernemental. Or, de l'avis de la Commission, cette situation porte atteinte à d'importants principes démocratiques comme la transparence de l'État dans l'utilisation de fonds publics et l'imputabilité gouvernementale.

Dans cette section, la Commission :

- effectue un survol des organismes assujettis à la Loi sur l'accès;
- souligne que certains organismes échappent à cet assujettissement malgré un financement public ou une mission incombant à un organisme public, y compris les municipalités.

Dans l'optique de promouvoir le respect des principes démocratiques en cause, la Commission recommande de moderniser les critères d'assujettissement à la Loi sur l'accès afin d'élargir son champ d'application.

1.1.1.1. Contexte

La Loi sur l'accès et le droit d'accès aux documents qu'elle prévoit, notamment, sont reconnus comme des piliers fondamentaux de la démocratie. En assurant la transparence de l'État et de toutes ses sphères d'activités, cette loi permet aux citoyens d'obtenir les informations nécessaires à leur pleine participation au processus démocratique. De plus, elle garantit l'imputabilité des gouvernements et des organismes publics, peu importe le palier, envers la population qu'ils desservent.

Or, considérant son cadre d'application actuel et les règles d'assujettissement qu'elle fixe, la Loi sur l'accès ne s'applique pas à certains organismes issus de nouveaux modes de gestion financière et économique de l'appareil gouvernemental comme les partenariats, la sous-traitance et la création de filiales. Dans cette ère où la confiance des citoyens dans les institutions publiques est fragilisée, la



Commission juge nécessaire d'améliorer le niveau de transparence applicable en s'assurant d'élargir les critères d'assujettissement à la Loi sur l'accès de manière à permettre un portrait plus complet de la façon dont est utilisé et géré l'ensemble des fonds et des services publics, et ce, peu importe les modes de gestion choisis par l'appareil gouvernemental.

1.1.1.2. Situation actuelle

La Loi sur l'accès s'applique actuellement :

- au gouvernement, au Conseil exécutif et au Conseil du trésor³⁵;
- au lieutenant-gouverneur, à l'Assemblée nationale, aux organismes dont les membres sont nommés par l'Assemblée nationale³⁶ ou aux personnes désignées par celle-ci pour exercer une fonction qui en relève, y compris les personnes qu'elle dirige³⁷;
- aux ministères et aux organismes gouvernementaux³⁸;
- aux autres organismes dont le gouvernement ou un ministre nomme la majorité des membres³⁹, dont la loi ordonne que le personnel soit nommé suivant la *Loi sur la fonction publique*⁴⁰ ou dont le fonds social fait partie du domaine de l'État⁴¹;
- au Conseil de la magistrature⁴²;
- au Curateur public⁴³;
- aux personnes nommées par le gouvernement ou un ministre, avec le personnel qu'elle dirige, dans le cadre des fonctions qui lui sont attribuées par la loi, le gouvernement ou le ministre⁴⁴;
- aux organismes municipaux⁴⁵;
- aux organismes scolaires⁴⁶;

³⁵ Loi sur l'accès, art. 3 al. 1.

³⁶ Par exemple, la Commission d'accès à l'information ou la Commission des droits de la personne et des droits de la jeunesse.

³⁷ Loi sur l'accès, art. 3 al. 2. Par exemple, le Commissaire au bien-être et aux droits des enfants, le Commissaire à l'éthique et à la déontologie ou le Protecteur du citoyen sont des personnes désignées par l'Assemblée nationale.

³⁸ *Id.*, art. 3 al. 1.

³⁹ Par exemple, la Société du Grand Théâtre de Québec, Bibliothèque et Archives nationales du Québec, le Conseil des arts et des lettres du Québec ou encore le Musée de la Civilisation.

⁴⁰ *Loi sur la fonction publique*, RLRQ, c. F-3.1.1. Par exemple, le personnel du Coroner en chef est nommé suivant cette loi, comme le prescrit la *Loi sur les coroners* (RLRQ, c. C-68.01), art. 24 al. 2.

⁴¹ Loi sur l'accès, art. 4 al. 1. Par exemple, le fonds social d'Hydro-Québec fait partie du domaine de l'État.

⁴² *Id.*, art. 4 al. 2. La Loi sur l'accès ne s'applique pas au Conseil de la magistrature lorsqu'il exerce ses fonctions judiciaires en matière de déontologie.

⁴³ *Id.*, art. 4 al. 3. Le Curateur public est visé pour les documents autres que ceux visés par l'article 2.2 de la Loi sur l'accès.

⁴⁴ *Id.*, art. 4 al. 4; par exemple, le directeur d'un cabinet d'un ministre ou un commissaire nommé par le gouvernement en vertu de la *Loi sur les commissions d'enquête*, RLRQ, c. F-3.1.1.

⁴⁵ Loi sur l'accès, art. 5. Ceux-ci comprennent notamment les municipalités, les communautés métropolitaines, les régies intermunicipales, les organismes que la loi déclare mandataires ou agents d'une municipalité, les organismes dont le conseil d'administration est formé majoritairement de membres du conseil d'une municipalité, les organismes dont le conseil d'administration est formé d'au moins un élu municipal siégeant à ce titre et dont une municipalité ou une communauté métropolitaine adopte ou approuve le budget ou contribue à plus de la moitié du financement, les sociétés d'économie mixte constituées conformément à la *Loi sur les sociétés d'économie mixte dans le secteur municipal* (RLRQ, c. S-25.01) et les organismes analogues constitués conformément à une loi d'intérêt privé. L'Union des municipalités du Québec et la Fédération québécoise des municipalités locales et régionales ne sont pas des organismes municipaux.

⁴⁶ *Id.*, art. 6. Les organismes scolaires comprennent notamment les centres de services scolaires, les commissions scolaires, les institutions dont le régime d'enseignement est l'objet d'une entente internationale au sens de la *Loi sur le ministère des Relations internationales* (RLRQ, c. M-25.1.1), les collèges d'enseignement général et professionnel, les établissements universitaires mentionnés aux paragraphes 1 à 11 de l'article 1 de la *Loi sur les établissements d'enseignement de niveau universitaire* (RLRQ, c. E-14.1) ainsi que les établissements agréés aux fins de subventions en vertu de la *Loi sur l'enseignement privé* (RLRQ, c. E-9.1).



- aux établissements de santé et de services sociaux⁴⁷;
- aux ordres professionnels⁴⁸, dans la mesure prévue par le *Code des professions*⁴⁹.

1.1.1.3. Enjeux

Si la liste des organismes actuellement assujettis à la Loi sur l'accès peut sembler impressionnante, elle ne reflète pourtant pas toute la complexité de l'organisation de l'administration publique. Cette dernière s'est complexifiée, notamment par la conclusion de différents partenariats et des changements dans la façon de dispenser les services publics.

La Commission note, entre autres, que :

- la mondialisation des marchés et la complexité du contexte économique favorisent la création de filiales d'entreprises publiques dont certaines échappent aux règles de transparence établies par la Loi sur l'accès, bien que ces filiales bénéficient d'importantes sommes provenant de fonds publics;
- l'intervention de plus en plus grande de l'État dans divers secteurs d'activité implique diverses formes d'association avec des organisations du secteur privé, comme des partenariats ou de la sous-traitance. Ces partenaires d'organismes publics, qui rendent parfois des services publics ou qui accomplissent des missions publiques, ne sont pas pour autant soumis à la Loi sur l'accès.

Par ailleurs, la rédaction actuelle des critères d'assujettissement génère certains angles morts. Par exemple, la Loi sur l'accès s'applique, comme mentionné précédemment, aux organismes dont le fonds social fait partie du domaine de l'État. La jurisprudence est toutefois riche en exemples d'organismes non visés par ce critère.

Premièrement, les organismes et leurs filiales dont les actions sont détenues seulement en partie par l'État ne sont pas visés. En 2002, la Cour d'appel a décidé qu'une filiale détenue à 100 % par un organisme assujetti à la Loi sur l'accès est également soumise à celle-ci⁵⁰, ce qui n'est pas le cas lorsque l'organisme détient moins de 100 % des parts⁵¹.

Deuxièmement, les filiales de deuxième rang d'un organisme public ne sont pas non plus visées par ce critère.

⁴⁷ *Id.*, art. 7. Les établissements de santé et de services sociaux comprennent notamment les établissements publics visés par la *Loi sur les services de santé et les services sociaux pour les Inuit et les Naskapi* (RLRQ, c. S-4.2) ou par la *Loi sur les services de santé et les services sociaux pour les autochtones cris* (RLRQ, c. S-5) ainsi que les établissements privés visés par ces lois qui fonctionnent en ayant recours à des sommes d'argent provenant du fonds consolidé du revenu, les établissements de santé et de services sociaux visés à l'annexe II de la *Loi sur la gouvernance du système de santé et de services sociaux* (RLRQ, c. G-1.021) et les établissements privés visés par cette loi qui fonctionnent en ayant recours à des sommes d'argent provenant du fonds consolidé du revenu.

⁴⁸ *Id.*, art. 1.1.

⁴⁹ *Code des professions*, RLRQ, c. C-26.

⁵⁰ *Pouliot c. Cour du Québec*, [2002] CANLII 41158 (QC. C.A.), en ligne : <<https://canlii.ca/t/1dw29>>.

⁵¹ *Bergeron c. Sidex*, 2024 QCCA 66, en ligne : <<https://canlii.ca/t/k4dmn>>.

Dans l'affaire *Hydro-Québec international inc. c. Boyer*⁵², la Cour du Québec conclut que la situation de HQI China est différente de celle d'Hydro-Québec International (HQI), analysée par la Cour d'appel dans l'affaire *Pouliot c. Cour du Québec*⁵³. Contrairement à HQI, filiale dont les actions sont détenues en totalité par Hydro-Québec, les actions de HQI China sont détenues par HQI et ne sont pas dévolues au domaine de l'État. Pour la Cour du Québec, cette distinction fait en sorte que le fonds social de HQI China n'appartient pas à l'État québécois et que cette sous-filiale n'est donc pas un organisme public assujéti à la Loi sur l'accès. En somme, HQI China n'est pas tenue au respect des exigences de transparence qui s'appliquent à son entreprise mère et à sa filiale de premier niveau.

Troisièmement, les organisations sans fonds social qui reçoivent des fonds publics ou exercent des activités habituellement confiées à des organismes publics sans répondre aux critères prévus aux articles 3 à 6 de la Loi sur l'accès échappent aussi à ce critère. On peut penser :

- aux associations touristiques régionales ou autres organisations vouées au développement touristique⁵⁴;
- aux organismes constitués pour des événements précis, notamment pour faire rayonner une ville ou la province⁵⁵;
- aux organismes voués au développement économique⁵⁶;
- aux organismes financés par l'État ou par des organismes publics⁵⁷.

Dans ces exemples, bien qu'un financement public ou des services publics soient impliqués, les activités échappent à l'application de la Loi sur l'accès et à la transparence qu'elle garantit.

Dans certains cas, la question de l'assujettissement ou non d'un organisme peut venir créer des débats juridiques complexes s'étalant sur plusieurs années⁵⁸.

⁵² *Hydro-Québec international inc. c. Boyer*, 2015 QCCQ 7681, en ligne : <<https://canlii.ca/t/glbbyg>>.

⁵³ *Pouliot c. Cour du Québec*, préc., note 50.

⁵⁴ *S.S. c. Tourisme Laval*, 2016 QCCA 1, en ligne : <<https://canlii.ca/t/gp35t>> (consulté le 9 mars 2026); dans cette affaire, il est démontré que Tourisme Laval reçoit 77 % de son financement en provenance de fonds publics.

⁵⁵ *A.B. c. Société du 400^e anniversaire de Québec*, 2009 QCCA 175, en ligne : <<https://canlii.ca/t/258mc>>.

⁵⁶ Voir notamment *Bergeron c. Sidex*, préc., note 51, où l'organisation vise la promotion et le soutien du développement de l'exploration minière sur le territoire du Québec; voir aussi *Lachance c. Société de développement industriel de St-Pamphile*, 2023 QCCA 265, en ligne : <<https://canlii.ca/t/k0twg>>, où l'organisation vise à favoriser l'expansion industrielle, commerciale et économique de la région de St-Pamphile.

⁵⁷ Voir notamment *Y. Z. c. Centre d'aide aux victimes d'actes criminels (CAVAC) de l'Outaouais*, 2021 QCCA 422, en ligne : <<https://canlii.ca/t/jmr47>>, où l'organisme est régi par la *Loi sur l'aide aux victimes d'actes criminels* (RLRQ, c. A-13.2) et est entièrement financé par le Fonds d'aide aux victimes d'actes criminels du ministre de la Justice; voir aussi *Santerre c. Groupe d'approvisionnement en commun de l'ouest du Québec*, 2019 QCCA 459, en ligne : <<https://canlii.ca/t/j5qr7>>; les groupes d'approvisionnements en commun dans le domaine de la santé et des services sociaux n'existent plus, mais ils avaient pour mission d'effectuer des achats exclusivement pour les établissements de santé et de services sociaux. Il s'agit donc d'un exemple intéressant où la Loi sur l'accès aurait dû s'appliquer à l'organisme.

⁵⁸ À titre d'exemple, dans l'affaire *Ouellet c. Comité paritaire et conjoint de la Sûreté du Québec*, la question centrale était de déterminer si le Comité paritaire et conjoint de la Sûreté du Québec était assujéti ou non à la Loi sur l'accès. Le dénouement de cette affaire a nécessité trois décisions distinctes. Voir : *Ouellet c. Comité paritaire et conjoint de la Sûreté du Québec*, 2020 QCCA 369, en ligne : <<https://canlii.ca/t/jctgw>>; *Procureur général du Québec c. Ouellet*, 2022 QCCQ 7068, en ligne : <<https://canlii.ca/t/jxsd2>>; *Ouellet c. Comité paritaire et conjoint de la Sûreté du Québec*, 2023 QCCA 400, en ligne : <<https://canlii.ca/t/k43xp>>.



Déjà dans ses rapports quinquennaux de 1997⁵⁹ et de 2002⁶⁰, la Commission attirait l'attention sur cette situation et recommandait que les organismes dont le financement est majoritairement assumé par des fonds publics soient assujettis à la Loi sur l'accès. Dans son rapport quinquennal de 2011, la Commission esquissait déjà les contours des enjeux d'assujettissement causés par les nouveaux modes de gestion financière et économique de l'appareil gouvernemental⁶¹. Force est de constater que la situation évoquée il y a quinze ans apparaît aujourd'hui avec une acuité encore plus marquée.

1.1.1.4. Recommandation

En 2026, la complexité de l'organisation de l'administration publique, de la dispensation des services publics et du financement de ces services exige que l'assujettissement à la Loi sur l'accès soit revu et modernisé pour refléter la réalité d'aujourd'hui. La Commission reconnaît que l'élargissement de l'assujettissement peut présenter certains défis, mais elle est convaincue que l'adaptation de la Loi aux nouveaux modes de gestion de l'appareil public est incontournable pour qu'elle puisse réellement atteindre ses objectifs.

La modernisation devrait faire en sorte que toutes les organisations qui évoluent au sein ou en périphérie de l'État, des organismes publics ou des municipalités soient soumises à la Loi sur l'accès. L'objectif serait de permettre aux citoyens d'accéder aux informations pertinentes relatives à toute activité financée en totalité ou en partie par l'État, ou qui visent la prestation de services ou la réalisation de missions relevant normalement des responsabilités de l'administration publique, mais qui sont dévolues pour une raison ou une autre à une organisation actuellement non assujettie à la Loi.

Pour ce faire, la Commission est d'avis que de nouveaux critères d'assujettissement précis et rationnels doivent être ajoutés à la Loi sur l'accès. Différents critères peuvent être envisagés, seuls ou combinés, comme le degré de contrôle de l'organisation par l'État ou un autre organisme public, le financement de l'organisation ou le mode de désignation des dirigeants. Concrètement, un critère basé sur le financement d'organisations par des fonds publics pourrait être ajouté⁶². Il pourrait également s'agir, comme le proposait la Commission dans son rapport quinquennal de 2011, d'assujettir à la Loi sur l'accès les organismes dont le fonds social est détenu à plus de 50 % par l'État⁶³.

Dans tous les cas, la Commission propose de s'inspirer des critères d'assujettissement prévus par d'autres juridictions afin d'alimenter les réflexions quant à cette modernisation. À cet égard, certains exemples intéressants sont abordés dans la section 1.1.1.5.

⁵⁹ COMMISSION D'ACCÈS À L'INFORMATION, *Vie privée et transparence administrative au tournant du siècle*, Québec, 1997, p. 77 à 79, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_RQ_1997.pdf>.

⁶⁰ Rapport quinquennal 2002, p. 53 à 55.

⁶¹ COMMISSION D'ACCÈS À L'INFORMATION, *Technologies et vie privée à l'heure des choix de société*, 2011 [ci-après Rapport quinquennal 2011], p. 68, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_RQ_2011.pdf>.

⁶² Dans un rapport de 2015, la commissaire fédérale à l'accès à l'information suggère comme critère : « les institutions financées en totalité ou en partie par le gouvernement du Canada, y compris celles pouvant réunir des fonds par l'intermédiaire d'emprunts publics [...] ». COMMISSAIRE À L'INFORMATION DU CANADA, *Viser juste pour la transparence: Recommandations pour moderniser la Loi sur l'accès à l'information*, 2015, p. 9, en ligne : <https://www.oic-ci.gc.ca/sites/default/files/userfiles/files/fra/reports-publications/Special-reports/Modernization2015/OIC_14-418_Modernization_french_v5.pdf>.

⁶³ Rapport quinquennal 2011, p. 67 à 69.

Recommandation 1

Modifier les critères d'assujettissement à la Loi sur l'accès afin qu'elle soit applicable à toutes les organisations qui gravitent dans la sphère d'activités de l'État, d'un organisme public ou d'une municipalité, par exemple en s'assurant qu'elle vise les organisations dont :

- le fonds social est détenu en totalité ou en partie par l'État ou par un organisme public;
- le financement est en grande partie assumé par l'État ou par un organisme public, en adoptant un seuil de financement ou en visant des activités spécifiques qui sont ainsi financées;
- les activités correspondent à un service ou à une mission dont la responsabilité incombe à l'État, à un organisme public ou à une municipalité.

1.1.1.5. Pour aller plus loin

De nombreuses juridictions ont adopté des dispositions d'assujettissement qui reflètent mieux les réalités contemporaines de l'organisation de l'appareil public. La Commission soumet quelques exemples d'assujettissement élargi :

- La loi de Terre-Neuve-et-Labrador utilise des critères d'assujettissement relatifs à la détention de la majorité des actions par la Couronne ainsi qu'à l'appartenance d'une entité à un gouvernement local (comme une municipalité) ou à un groupe de gouvernements locaux ou sa création par eux, pourvu que l'objectif premier de cette entité soit d'administrer des biens ou de s'acquitter d'une responsabilité appartenant à ces gouvernements locaux⁶⁴.
- La loi espagnole s'applique notamment :
 - aux entités privées qui perçoivent, au cours d'une année, des aides ou des subventions publiques supérieures à 100 000 euros;
 - à celles dont 40 % des revenus annuels proviennent de telles aides ou subventions publiques, à condition que ces fonds publics dépassent 5 000 euros⁶⁵.
- La loi polonaise s'applique notamment aux autorités publiques et aux « autres entités qui accomplissent des missions publiques⁶⁶ ». Ainsi, elle vise entre autres :
 - des entités qui représentent des personnes morales de droit public de différents paliers de l'organisation étatique;
 - des entités qui exercent des fonctions publiques ou disposent de biens publics.

⁶⁴ *Access to Information and Protection of Privacy Act [Terre-Neuve-et-Labrador]*, SNL 2015, c. A-1.2, art. 2(x), en ligne : <https://assembly.nl.ca/legislation/sr/statutes/a01-2.htm>.

⁶⁵ *Ley 19/2013, de 9 diciembre de transparencia, acceso a la información pública y buen gobierno [Espagne]*, BOE-A-2013-12887, art. 3, en ligne : <https://boe.es/buscar/act.php?id=BOE-A-2013-12887>.

⁶⁶ *Law on Access to Public Information of 6 September 2001 [Pologne]*, Journal of Laws 112, 1198, art. 4, en ligne : <https://www.rti-rating.org/wp-content/uploads/Poland.pdf>.



- La loi portugaise⁶⁷ s'applique notamment :
 - aux associations ou fondations de droit privé dans lesquelles des entités et des organismes publics désignés par la loi exercent des pouvoirs de contrôle de gestion ou désignent, directement ou indirectement, la majorité des membres de l'organe d'administration, de direction ou de surveillance;
 - aux documents détenus ou élaborés par des entités dotées de la personnalité juridique, créées pour répondre de manière précise à des besoins d'intérêt général dépourvus de caractère industriel ou commercial, lorsque l'une des circonstances suivantes est applicable :
 - Leur activité est majoritairement financée par un organisme public désigné par la loi.
 - Leur gestion est soumise à un contrôle exercé par un organisme public désigné par la loi.
 - Les membres de leurs organes d'administration, de direction ou de surveillance sont, pour plus de la moitié, désignés par un organisme public désigné par la loi.
- La *Loi-type interaméricaine relative à l'accès à l'information*⁶⁸, modèle élaboré par l'Organisation des États américains, prévoit l'assujettissement des organisations suivantes :
 - Les autorités publiques appartenant à n'importe quelle branche du gouvernement (exécutive, législative ou judiciaire), et ce, à tous les niveaux de la structure gouvernementale (fédéral, régional, provincial ou municipal).
 - Les organismes indépendants ou autonomes, les organisations et entités dont la propriété ou le contrôle appartiennent au gouvernement agissant en vertu de la Constitution ou de n'importe quelle autre loi.
 - Tout individu ou toute personne morale qui reçoit ou gère des ressources publiques ou qui exerce des actes d'autorité au niveau national ou fédéral, s'ils obtiennent des fonds publics.

⁶⁷ *Lei n.º 26/2016 de 22 de agosto [Portugal]*, Diário da República n.º 160/2016, art. 4, en ligne : <https://diariodarepublica.pt/dr/detalhe/lei/26-2016-75177807>.

⁶⁸ ORGANISATION DES ÉTATS AMÉRICAINS, *Loi-type interaméricaine 2.0 sur l'accès à l'information*, 2020, art. 2(3), en ligne : https://www.oas.org/en/sla/dil/docs/AG-doc_5718-20_FR.pdf.



1.1.2. Les dérogations à la Loi et les régimes particuliers

Sommaire

Malgré le caractère prépondérant de la Loi sur l'accès, son application est fréquemment écartée par l'adoption de lois y prévoyant des dérogations ou introduisant des régimes particuliers. Alors que cette pratique d'exception devrait être utilisée avec parcimonie, le législateur y a fréquemment recours. Chaque nouvelle dérogation ou régime particulier fragilise la prépondérance de la Loi sur l'accès et complexifie le cadre légal applicable.

C'est pourquoi la Commission recommande d'effectuer une révision globale de l'ensemble des dérogations à la Loi sur l'accès ou des régimes particuliers y suppléant. Cet exercice permettrait de ne conserver que ce qui se justifie toujours dans l'intérêt public. Il s'agirait là de réaffirmer clairement toute l'importance devant être accordée à la Loi sur l'accès et aux valeurs fondamentales promues par celle-ci.

1.1.2.1. Contexte

La Loi sur l'accès jouit d'un caractère prépondérant, un statut démontrant toute l'importance des objectifs qu'elle vise⁶⁹. Cette prépondérance peut être écartée par le législateur, mais une mention expresse doit alors être faite à la Loi pour l'annoncer. Ce mécanisme permet, entre autres, d'attirer l'attention des parlementaires et de toute personne intéressée sur la volonté explicite du législateur de déroger au régime prépondérant. Généralement, une dérogation ou un régime particulier devrait donc s'accompagner d'une réflexion étoffée justifiant la nécessité de créer une exception, et le tout devrait être débattu lors des travaux parlementaires. Le caractère exceptionnel de la prépondérance accordée à la Loi sur l'accès devrait, en principe, militer pour que le législateur fasse preuve d'une grande circonspection avant de l'écarter. L'histoire démontre toutefois que l'usage de dérogations et de régimes particuliers est fréquent. Déjà pointée par la Commission dans son rapport quinquennal de 2016⁷⁰, cette tendance ne s'est pas démentie depuis.

Bien que sensible à la pertinence de certaines exceptions, la Commission rappelle que chacune vient fragiliser le caractère prépondérant de la Loi sur l'accès et complexifier la compréhension et la fluidité de l'application du cadre légal.

Devant la multiplication des cas d'utilisation de dérogations ou de régimes particuliers par le législateur, la Commission réitère qu'une réflexion sérieuse doit se tenir à ce sujet et qu'un réexamen global s'impose.

⁶⁹ Bien que le présent texte porte, par souci de simplicité, essentiellement sur la Loi sur l'accès, la Commission tient à souligner que la même situation s'applique, avec les adaptations nécessaires, à la Loi sur le privé, bien que les dérogations à cette loi soient beaucoup moins fréquentes.

⁷⁰ Rapport quinquennal 2016, ch. 1.



1.1.2.2. Situation actuelle

La prépondérance d'une loi signifie qu'elle a un caractère prédominant sur les autres lois. Elle est alors élevée à un rang supérieur au sein du corpus législatif. La *Charte des droits et libertés de la personne* (la Charte) a été la première loi québécoise de cette nature, le législateur lui ayant conféré un statut quasi constitutionnel⁷¹.

La Charte est un fleuron législatif du Québec : elle consacre les droits et libertés fondamentaux des citoyens. Contrairement à la *Charte canadienne des droits et libertés*⁷², qui ne s'applique que dans les relations entre l'État et les citoyens canadiens, les droits protégés par la Charte québécoise s'étendent à l'ensemble des sphères relationnelles des Québécois, soit :

- les relations entre l'État et les citoyens;
- les relations entre citoyens;
- les relations entre citoyens et tout type d'organisation.

La reconnaissance de l'importance de la Charte permet également de réaliser le caractère fondamental de la Loi sur l'accès. En adoptant cette dernière en 1982, le législateur a suivi la recommandation de la Commission Paré⁷³, qui en avait élaboré l'ébauche, de lui conférer un statut prépondérant⁷⁴ :

168. Les dispositions de la présente loi prévalent sur celles d'une loi générale ou spéciale postérieure qui leur seraient contraires, à moins que cette dernière loi n'énonce expressément s'appliquer malgré la présente loi.

Le choix du législateur à cet égard marque le caractère essentiel des objectifs de la Loi sur l'accès qui viennent asseoir certains des droits prévus à la Charte, soit :

- le droit fondamental pour les citoyens d'accéder à l'information, à titre de pilier de la démocratie dans un État de droit⁷⁵
- le respect du droit à la vie privée de tous les citoyens face à l'État et aux organismes publics⁷⁶.

Les dispositions conférant un caractère prépondérant à la Charte ou à la Loi sur l'accès prévoient aussi la possibilité d'y déroger expressément. Ce fait sous-entend que des motifs légitimes peuvent exister, dans des sociétés libres et démocratiques, pour écarter l'application de ces lois prépondérantes.

Dans son rapport quinquennal de 2016, la Commission répartissait les différents types de dérogations à la Loi sur l'accès prévues dans le corpus législatif du Québec en quatre catégories⁷⁷, classification qui demeure intéressante aux fins des présentes réflexions :

1. **Les limitations au droit d'accès aux documents des organismes publics.** Il peut s'agir de lois sectorielles qui restreignent le droit d'accès, en déclarant confidentiels des documents administratifs qui pourraient autrement être accessibles en vertu de la Loi sur l'accès. Par exemple, la *Loi sur la*

⁷¹ Charte, art. 52.

⁷² *Charte canadienne des droits et libertés*, Loi constitutionnelle de 1982, constituant l'annexe B de la *Loi de 1982 sur le Canada* (R-U), 1982, c. 11.

⁷³ COMMISSION D'ÉTUDE SUR L'ACCÈS DU CITOYEN À L'INFORMATION GOUVERNEMENTALE ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, préc., note 1, p. 18.

⁷⁴ Loi sur l'accès, art. 168; à titre informatif, la Loi sur le privé reprend exactement le même libellé : Loi sur le privé, art. 94.

⁷⁵ Charte, art. 44.

⁷⁶ *Id.*, art. 5.

⁷⁷ Rapport quinquennal 2016, p. 6 et 7.



*gouvernance du système de santé et de services sociaux*⁷⁸ prévoit trois dérogations à la Loi sur l'accès.

2. **Les limitations de la protection des renseignements personnels.** Ce type de limitation permet, par exemple, la communication ou l'utilisation de renseignements personnels sans qu'il soit nécessaire d'obtenir le consentement préalable de la personne concernée⁷⁹.
3. **Des lois sectorielles mettant en place un régime distinct.** Ces lois sont parfois plus généreuses, mais majoritairement plus restrictives que la Loi sur l'accès. La plupart de ces régimes particuliers chevauchent à la fois l'accès à l'information et la protection des renseignements personnels⁸⁰.
4. **Des lois contenant une dérogation qui prévoit que certaines de leurs dispositions, ou l'ensemble d'entre elles, s'appliquent malgré la Loi sur l'accès**⁸¹. L'effet de ce type de dérogation est d'écarter l'ensemble du régime de la Loi sur l'accès.

1.1.2.3. Enjeux

La Commission est bien consciente du fait que le droit à l'accès n'est pas absolu et qu'il peut exister des motifs tout à fait légitimes et valides justifiant l'adoption de dérogations ou de régimes particuliers constituant des exceptions à la Loi sur l'accès. En revanche, cette situation doit conserver un caractère exceptionnel pour éviter d'éroder la primauté des principes fondamentaux établis par le régime de la Loi sur l'accès.

Or dès son adoption, la prépondérance de la Loi sur l'accès a été constamment érodée par l'ajout fréquent et régulier de dérogations. En 2016, lors de la publication du rapport quinquennal de la Commission, 89 dérogations significatives au droit d'accès aux documents⁸² étaient recensées dans le corpus législatif québécois. En date de mars 2026, on en compte désormais 29 de plus, pour un total de 118 : une augmentation marquée de 33 % en 10 ans qui illustre la récurrence de ce choix du législateur. Un portrait plus complet est présenté à la section 1.1.2.5.

Déjà en 2015, la Fédération professionnelle des journalistes du Québec constatait la dégradation de la prépondérance de la Loi sur l'accès⁸³ :

Quelles mesures sont proposées pour assurer la prééminence de la Loi d'accès? De plus en plus, d'autres lois viennent en gruger les dispositions, comme une modification récente à la Loi sur les contrats des organismes publics, qui a rendu secrets les noms des membres des comités de sélection des projets du ministère des Transports du Québec, malgré des décisions contraires de la CAI. Quelles mesures sont prévues par le

⁷⁸ *Loi sur la gouvernance du système de santé et de services sociaux*, RLRQ, c. G-1.021, art. 178, 211 et 224 [ci-après LGSSS]. Ces dérogations visent notamment à déclarer confidentiels les dossiers et procès-verbaux du comité de gestion des risques et du conseil des médecins, dentistes, pharmaciens et sages-femmes des établissements de Santé Québec. Voir aussi la *Loi sur l'assurance médicaments*, RLRQ, c. A-29.01, art. 60.0.3; voir encore la *Loi sur la sécurité incendie*, RLRQ, c. S-3.4, art. 133.

⁷⁹ Voir par exemple la *Loi sur les coroners*, RLRQ, c. C-68.01, art. 180; la *Loi concernant la lutte contre la corruption*, RLRQ, c. L-6.1, art. 16.1; la *Loi sur les biens non réclamés*, RLRQ, c. B-5.1, art. 21.

⁸⁰ Voir par exemple la *Loi sur l'administration fiscale*, RLRQ, c. A-6.002, art. 69 à 71.6.

⁸¹ Voir par exemple le *Code d'éthique et de déontologie des membres de l'Assemblée nationale*, RLRQ, c. C-23.1, art. 113.

⁸² Comme l'explique la Commission dans la section 1.1.2.5, ces dérogations concernent les articles 9, 10, 83 et 171 de la Loi sur l'accès. Elles visent aussi parfois toute la Loi sur l'accès dans un contexte d'accès aux documents.

⁸³ FÉDÉRATION PROFESSIONNELLE DES JOURNALISTES DU QUÉBEC, *Pour une refonte globale de la Loi sur l'accès, en faveur d'une réelle transparence de l'État – Mémoire de la Fédération professionnelle des journalistes du Québec sur les Orientations gouvernementales pour un gouvernement plus transparent, dans le respect du droit à la vie privée et la protection des renseignements personnels*, 2015, p. 5, en ligne :

<https://www.bibliotheque.assnat.qc.ca/DepotNumerique_v2/AffichageFichier.aspx?idf=165300>.



gouvernement pour garantir que d'autres lois ne viennent pas limiter peu à peu le champ de couverture de la Loi d'accès à l'information?

Ces multiples dérogations et régimes particuliers ont pour effet général d'éroder significativement le caractère prépondérant de la Loi sur l'accès. Cette érosion est malheureusement constante : chaque année, la tendance se concrétise davantage. La situation complexifie, pour le citoyen, l'exercice de ses droits en matière d'accès à l'information, de même que, pour les organismes publics, l'analyse avant de rendre une décision en accès.

La Commission note également que la multiplication de ces exceptions comporte un risque de générer des problématiques de superposition de dispositions applicables entraînant des débats juridiques complexes concernant par exemple des questions de compétence ou de prépondérance d'application de dispositions divergentes⁸⁴.

Dans la suite de cette section, la Commission illustre, à travers trois exemples, certains des enjeux soulevés par la situation actuelle, liés :

- au caractère répétitif de certaines dérogations;
- à des dérogations privant les personnes concernées de droits importants;
- à la complexification des règles applicables par la multiplication de dispositions dérogatoires, engendrant une pluralité de régimes.

1.1.2.3.1. Certaines dérogations se répètent à travers plusieurs lois

Inévitablement, certaines des dizaines de dérogations à la Loi sur l'accès visent les mêmes objectifs et se répètent donc d'une loi à l'autre, au lieu qu'une seule restriction générale existe au sein de la Loi sur l'accès. Ainsi, la multiplication des dérogations se poursuit à mesure qu'une même situation se présente à travers de nouvelles lois, engendrant un risque croissant d'incohérence. Cette répétition complique l'application des restrictions ainsi que leur contrôle par la Commission, en plus d'alourdir le corpus législatif.

La répétition des dérogations en matière de conciliation ou de médiation illustre bien cet enjeu. Moyennant certaines adaptations propres à chaque contexte législatif, de nombreuses lois contiennent une disposition semblable à celle-ci⁸⁵ :

Malgré l'article 9 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1), nul n'a droit d'accès à un document contenu dans le dossier de conciliation ou de médiation.

Ces dispositions visent à empêcher toute personne d'accéder à des documents détenus par des organismes publics et utilisés dans le cadre d'un processus de conciliation, de médiation ou d'un processus de même nature. Ces dispositions permettent d'assurer la confidentialité de ces processus.

⁸⁴ Voir, à titre d'exemple en ce qui concerne l'accès aux documents du Bureau du coronier : *Dufresne c. Bureau du coronier*, 2025 QCCA 266, en ligne : <<https://canlii.ca/t/kfjn1>>.

⁸⁵ *Loi sur les assureurs*, RLRQ, c. A-32.1, art. 56 al. 3.

La Commission ne remet pas en question la nécessité de cet objectif. Toutefois, selon la recension effectuée par la Commission, pas moins de 25 lois⁸⁶ contiennent une telle disposition, ce qui démontre le caractère peu économe de l'approche actuelle.

1.1.2.3.2. Des dérogations peuvent priver les personnes concernées de droits importants

Certaines dérogations paraissent difficilement justifiables en raison de leur forte incidence sur les droits des personnes. C'est notamment le cas de celles qui visent la communication potentielle d'un dossier de plainte ayant été fourni par une organisation du secteur financier.

La *Loi visant principalement à améliorer l'encadrement du secteur financier, la protection des dépôts d'argent et le régime de fonctionnement des institutions financières*⁸⁷, une réforme importante du secteur financier, a introduit dans plusieurs lois de ce secteur une disposition comparable à celle-ci⁸⁸ :

Malgré les articles 9 et 83 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1), l'Autorité ne peut communiquer un dossier de plainte sans l'autorisation de l'assureur qui le lui a transmis.

Une dérogation à l'article 83 de la Loi sur l'accès a pour conséquence d'empêcher une personne d'obtenir les renseignements personnels la concernant directement. Concrètement, elle prive une personne de plusieurs droits :

- Le droit de demander l'accès à ses propres renseignements, peu importe l'organisme public qui les détient.
- Corollairement, la possibilité de vérifier l'exactitude de ces renseignements.
- Le droit de demander la rectification d'un renseignement inexact, incomplet ou équivoque.

Or, dans les pièces législatives où a été introduite cette dérogation, l'organisme public concerné est susceptible d'utiliser les renseignements personnels pour prendre une décision à propos de la personne concernée. Il est donc essentiel que cette personne puisse s'assurer que ses renseignements sont exacts et, au besoin, qu'elle puisse en demander la rectification.

Dans ces circonstances, la Commission se questionne de manière générale sur la plus-value et la pertinence de ce type de dérogation dans des lois particulières. C'est d'autant plus vrai que s'il y a bel et bien lieu de restreindre l'accès aux renseignements d'une personne, l'organisme public concerné pourrait invoquer les restrictions au droit d'accès prévues par la Loi sur l'accès⁸⁹.

⁸⁶ *Id.*; des dispositions visant un objet identique ou similaire se trouvent également dans plus d'une vingtaine d'autres lois; voir par exemple *Code de procédure civile*, RLRQ, c. C-25.01, art. 607; *Loi sur les agents d'évaluation du crédit*, RLRQ, c. A-8.2, art. 43 al. 3; *Loi sur la protection contre les représailles liées à la divulgation d'actes répréhensibles*, RLRQ, c. P-33.01, art. 10 al. 3; *Loi sur la justice administrative*, RLRQ, c. J-3, art. 123 al. 2; *Loi sur les coopératives de services financiers*, RLRQ, c. C-67.3, art. 131.5 al. 3; *Loi sur les accidents du travail et les maladies professionnelles*, RLRQ, c. A-3.001, art. 429.48 al. 2.

⁸⁷ *Loi visant principalement à améliorer l'encadrement du secteur financier, la protection des dépôts d'argent et le régime de fonctionnement des institutions financières*, LQ 2018, c. 23.

⁸⁸ *Loi sur les assureurs*, préc., note 85, art. 57; plusieurs lois impliquant l'Autorité des marchés financiers contiennent une disposition identique : *Loi sur les agents d'évaluation du crédit*, préc., note 86, art. 44; *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.02, art. 41; *Loi sur les instruments dérivés*, RLRQ, c. I-14.01, art. 77.3; *Loi sur les valeurs mobilières*, RLRQ, c. V-1.1, art. 168.1.7; *Loi sur les institutions de dépôts et la protection des dépôts*, RLRQ, c. I-13.2.2, art. 28.18; *Loi sur la distribution de produits et services financiers*, RLRQ, c. D-9.2, art. 103.6; *Loi sur les coopératives de services financiers*, préc., note 86, art. 131.6.

⁸⁹ *Loi sur l'accès*, art. 87 et 18 à 41.3.



1.1.2.3.3. La pluralité des régimes d'accès à l'information environnementale complexifie les règles

Même lorsqu'ils sont plus généreux que la Loi sur l'accès, les régimes particuliers peuvent poser un problème lorsqu'ils se superposent à celui de la Loi sur l'accès. L'état actuel de l'accès à l'information environnementale illustre particulièrement bien cet enjeu.

Les questions environnementales sont au cœur de la vie de tous les citoyens. En effet, les enjeux environnementaux ont une incidence significative et directe sur nos milieux de vie, notre santé et notre sécurité, et les effets peuvent perdurer, parfois sur plusieurs générations. C'est donc sans surprise que l'actualité démontre l'intérêt constant de la population pour ces enjeux.

L'accès à l'information est conséquemment un pilier du droit à un environnement sain. En cette matière, une transparence maximale devrait être appliquée en toutes circonstances. Il s'agit de l'un des meilleurs exemples où l'intérêt public devrait généralement l'emporter.

Bien que des modifications législatives aient été édictées en 2017 pour favoriser la transparence en matière environnementale⁹⁰, certaines de ces modifications ne sont toujours pas entrées en vigueur. Il en résulte un ensemble de dispositions complexes qui entrave la capacité des citoyens à accéder aisément à l'information.

1.1.2.3.3.1. Trois régimes généraux s'appliquent simultanément

Actuellement, trois régimes à portée générale s'appliquent simultanément. Le premier est celui de la Loi sur l'accès, lequel s'applique à tous les renseignements qui ne sont pas visés par la *Loi sur la qualité de l'environnement* (LQE)⁹¹.

Le second régime, qui a préséance sur la Loi sur l'accès, repose sur des registres prévus à la LQE⁹². Les documents et les renseignements contenus dans ces registres ont un caractère public⁹³. Il s'agit donc d'un régime qui est, en principe, plus généreux que celui prévu à la Loi sur l'accès.

À cet égard, près de neuf ans après la sanction de la Loi modifiant la LQE, l'amendement prévoyant la création d'un registre public d'information environnementale⁹⁴ n'est toujours pas en vigueur. Un tel registre doit pourtant rassembler des documents significatifs relatifs à des demandes d'autorisation concernant des projets qui ont une incidence en matière d'environnement, par exemple :

- Les documents concernant la description de l'activité d'un tel projet.
- Les documents concernant les renseignements sur les rejets de contaminants dans l'environnement.
- Les études d'évaluation des impacts environnementaux.

La conséquence est relativement simple : les citoyens doivent souvent présenter une demande d'accès pour obtenir des renseignements ou des documents qui seraient pourtant accessibles sans formalité si ce

⁹⁰ *Loi modifiant la Loi sur la qualité de l'environnement afin de moderniser le régime d'autorisation environnementale et modifiant d'autres dispositions législatives notamment pour réformer la gouvernance du Fonds vert*, LQ 2017, c. 4 [ci-après *Loi modifiant la LQE*], en ligne : https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2017/2017C4F.PDF.

⁹¹ C'est-à-dire ceux énoncés à l'article 118.4 de cette loi : *Loi sur la qualité de l'environnement*, RLRQ, c. Q-2 [ci-après *LQE*].

⁹² *Loi modifiant la LQE*, art. 188; *LQE*, art. 118.5 et 118.5.0.1.

⁹³ *LQE*, art. 118.5.3.

⁹⁴ Il s'agit de la version de l'article 118.5 prévue par la *Loi modifiant la LQE*.



registre public était en place. Dans ce contexte, les dispositions transitoires de la Loi modifiant la LQE⁹⁵ continuent de s'appliquer depuis le 23 mars 2017. Elles permettent notamment à un tiers de s'opposer à la divulgation de certains renseignements.

Dans l'affaire *Watson c. Ministère de l'Environnement, de la Lutte contre les changements climatiques, de la Faune et des Parcs*⁹⁶, la Commission mentionnait à propos de cette situation :

« [67] À cet effet, la Commission retient que le régime de la Loi sur l'accès est mis de côté par un régime particulier afin d'assurer une plus grande transparence en matière de renseignements touchant l'environnement.

[68] Le régime transitoire prévu à l'article 298 de la [Loi modifiant la LQE] fait reposer la responsabilité au demandeur d'autorisation de s'assurer de soumettre ses observations quant aux secrets industriels ou commerciaux confidentiels pouvant se trouver dans les documents qu'il a lui-même soumis, ou qui ont été soumis par l'un de ses mandataires, dans le cadre de sa demande. »

Il est également intéressant de souligner que le ministère de l'Environnement, de la Lutte contre les changements climatiques, de la Faune et des Parcs est l'organisme public québécois qui reçoit le plus de demandes d'accès aux documents⁹⁷. Il ne fait aucun doute que l'entrée en vigueur des modifications à la LQE aurait une incidence sur le nombre de demandes d'accès qui lui sont formulées.

Le troisième régime est encore prévu à la LQE. Il prend la forme non pas d'un registre, mais d'un droit d'obtenir copie de certains renseignements ou documents du ministère. Ils peuvent concerner, par exemple :

- la concentration des contaminants rejetés par une source de contamination;
- des études de caractérisation des sols;
- des évaluations des risques toxicologiques et écotoxicologiques;
- des études relatives à l'impact d'un prélèvement d'eau sur l'environnement.

Concernant ces renseignements ou documents, seules trois restrictions de la Loi sur l'accès sont applicables⁹⁸.

En somme, non seulement y a-t-il trois régimes d'accès à l'information à portée générale en matière environnementale, mais l'un de ces régimes nécessite l'application de dispositions transitoires plus difficilement repérables au sein du corpus législatif⁹⁹. Cette situation présente donc

⁹⁵ Loi modifiant la LQE, art. 297 et 298.

⁹⁶ *Watson c. Ministère de l'Environnement, de la Lutte contre les changements climatiques, de la Faune et des Parcs*, 2024 QCCA 182, en ligne : <<https://canlii.ca/t/k6936>>.

⁹⁷ En 2024-2025, ce ministère a reçu 14 861 demandes : MINISTÈRE DE L'ENVIRONNEMENT, DE LA LUTTE CONTRE LES CHANGEMENTS CLIMATIQUES, DE LA FAUNE ET DES PARCS, *Rapport annuel de gestion 2024-2025*, 2025, p. 58, en ligne : <<https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/environnement/publications-adm/rapport-annuel-de-gestion/rapport-annuel-gestion-2024-2025-melccfp.pdf>>; ce nombre dépasse la dizaine de milliers depuis des années; voir notamment la compilation sur trois ans dans COMMISSION D'ACCÈS À L'INFORMATION, *Avoir accès en temps utile : portrait des délais de traitement des demandes d'accès au Québec*, 2022, p. 45, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_RAP_Delais_Acces.pdf>.

⁹⁸ LQE, art. 118.4 al. 2; ces restrictions sont celles des articles 28, 28.1 et 29 de la Loi sur l'accès.

⁹⁹ En effet, ces dispositions transitoires ne se retrouvent pas dans la version consolidée de la LQE disponible sur le site LégisQuébec. Pour les retracer, il faut plutôt consulter le texte sanctionné de la Loi modifiant la LQE dans le recueil annuel des lois sanctionnées de 2017 en format PDF, diffusé par les Publications du Québec.



un niveau de complexité supplémentaire pour des citoyens ou des organisations souhaitant faire valoir leur droit d'accès.

1.1.2.3.2. *D'autres lois sectorielles prévoient des régimes distincts*

La complexité évoquée ci-haut est encore augmentée par le fait que certaines lois sectorielles prévoient des régimes distincts d'accès à l'information environnementale. Un citoyen peut ainsi difficilement s'y retrouver.

Quelques constats s'imposent relativement à ces régimes particuliers en matière environnementale. Certains d'entre eux établissent un principe de transparence et de participation¹⁰⁰. D'autres se veulent plus permissifs que la Loi sur l'accès en conférant un caractère public à certains renseignements de nature environnementale¹⁰¹. Ces régimes sont néanmoins souvent d'application restreinte ou encore difficilement applicables.

Par exemple, la *Loi affirmant le caractère collectif des ressources en eau et favorisant une meilleure gouvernance de l'eau et des milieux associés* prévoit que¹⁰² :

Toute personne a le droit, dans les conditions et les limites définies par la loi, d'accéder aux informations relatives aux ressources en eau par les autorités publiques et de participer à l'élaboration des décisions prises par ces autorités qui ont une incidence sur ces ressources.

Comme il n'y a aucun mécanisme d'accès dans cette loi, il faut s'en remettre à la LQE, laquelle permet un accès circonscrit à certains renseignements ou documents relatifs à l'eau. Les citoyens ne participent donc pas en toute connaissance de cause à l'élaboration des décisions prises par les autorités puisque leur accès aux renseignements ou aux documents est limité, notamment parce que le registre public prévu par la Loi modifiant la LQE n'est toujours pas en vigueur.

La *Loi sur les mines* et la *Loi sur les pesticides* sont deux lois qui confèrent un caractère public à certains renseignements ou documents. Cependant, le nombre restreint de catégories de renseignements qui sont accessibles en vertu de ces lois en font des régimes incomplets. En effet, les régimes de la LQE ou de la Loi sur l'accès s'appliquent à tous les autres renseignements ou documents visés par l'objet de ces lois, mais qui ne figurent pas parmi ceux ayant un caractère public. La transparence maximale, pour un sujet aussi important que l'environnement, n'est donc pas atteinte.

En somme, cette multiplication de régimes particuliers aux objectifs variés complexifie davantage l'accès à l'information.

1.1.2.4. **Recommandations**

La Commission estime que le Québec doit se prémunir contre l'effritement de la prépondérance d'une loi aussi fondamentale que la Loi sur l'accès. **La Commission est d'avis qu'une révision des dérogations pour les limiter au maximum enverrait un message fort de l'État quant à l'importance capitale des protections prévues par la Loi sur l'accès dans une société libre et démocratique.**

¹⁰⁰ *Loi affirmant le caractère collectif des ressources en eau et favorisant une meilleure gouvernance de l'eau et des milieux associés*, RLRQ, c. C-6.2, art. 7.

¹⁰¹ Par exemple, la *Loi sur les pesticides*, RLRQ, c. P-9.3, art. 128; *Loi sur les mines*, RLRQ, c. M-13.1, art. 215.

¹⁰² *Loi affirmant le caractère collectif des ressources en eau et favorisant une meilleure gouvernance de l'eau et des milieux associés*, préc., note 100, art. 7.



Toute exception aux droits sous-tendant la Loi sur l'accès, tout comme ceux garantis par la Charte, devrait reposer sur des considérations relevant de l'intérêt public¹⁰³. Une dérogation à une loi prépondérante ne devrait se concrétiser que lorsque le respect des droits qu'elle procure ou protège constitue un obstacle incontournable et inévitable à l'atteinte d'objectifs suffisamment importants au bénéfice de l'intérêt public. Le cas échéant, une telle dérogation devrait porter sur une ou des dispositions précises, et non sur l'intégralité de cette loi.

Par conséquent, il est grand temps de réviser l'ensemble des dispositions dérogatoires et des régimes particuliers. Comme les dispositions de la Loi sur l'accès portant sur l'accès aux documents des organismes publics doivent faire l'objet d'une importante modernisation, un tel exercice permettrait de procéder à une analyse approfondie et étendue des dérogations à la Loi sur l'accès. Cette même analyse devrait également porter sur les régimes particuliers qui se sont ajoutés depuis son entrée en vigueur.

En effet, certaines dérogations ou certains régimes particuliers mériteraient d'être remis en question ou réformés, entre autres pour :

- éviter toute redondance avec la Loi sur l'accès. En effet, l'objet de certaines dispositions dérogatoires pourrait déjà être couvert par une restriction déjà dûment prévue à la Loi sur l'accès¹⁰⁴;
- faire cesser la multiplication des dérogations similaires dans plusieurs lois sectorielles. Il s'agirait plutôt de prévoir une nouvelle restriction générale directement à la Loi sur l'accès;
- éviter la multiplication de régimes concurrents applicables à un même domaine, comme en matière environnementale. À ce propos, considérant l'importance des enjeux environnementaux et la transparence attendue par les citoyens à cet égard, une révision de l'ensemble des dérogations et des régimes particuliers dans les lois touchant l'environnement apparaît, pour la Commission, indispensable.

Ces modifications viendraient simplifier le corpus législatif et en faciliter la compréhension par le citoyen.

Recommandation 2

Effectuer, dans le cadre d'une réforme de la Loi sur l'accès, une révision globale de l'ensemble des dérogations à la Loi sur l'accès ou des régimes particuliers y suppléant adoptés par le législateur, notamment dans l'objectif :

- d'éliminer les dérogations et les régimes particuliers s'ils ne sont pas justifiés et nécessaires dans une optique d'intérêt public;
- de retirer du corpus législatif les dérogations similaires reprises dans plusieurs lois sectorielles en les remplaçant par une restriction générale directement prévue à la Loi sur l'accès;
- d'instaurer des normes, comme des critères, processus et outils, pour limiter et encadrer l'introduction de nouvelles dérogations ou de nouveaux régimes particuliers dans le futur.

¹⁰³ Rapport quinquennal 2016, p. 8.

¹⁰⁴ Voir la section II du chapitre II de la Loi sur l'accès, art. 18 et suivants.



Recommandation 3

Revoir dès que possible l'ensemble des régimes particuliers applicables en matière d'accès à l'information environnementale pour simplifier l'accès et maximiser la transparence, notamment en faisant rapidement entrer en vigueur les dispositions concernant la mise en place du registre public d'information environnementale introduit à la *Loi sur la qualité de l'environnement*.

1.1.2.5. Pour aller plus loin : portrait de l'évolution des dérogations entre 2016 et 2026

La Commission a documenté l'évolution du nombre de dérogations au droit d'accès ou à l'ensemble de la Loi sur l'accès entre 2016 et 2026.

Aux fins de sa compilation, la Commission s'est concentrée sur deux types de dérogations :

- D'une part, puisqu'elles constituent des contraintes significatives au droit d'accès, les dérogations aux articles suivants de la Loi sur l'accès¹⁰⁵ :
 - Article 9 : droit d'accès aux documents des organismes publics;
 - Article 10 : droit d'obtenir une copie des documents;
 - Article 83 : droit d'accès d'une personne à ses renseignements personnels;
 - Article 171 : protection contre la restriction du droit d'accès.
- D'autre part, les dérogations totales à la Loi sur l'accès dans un contexte d'accès aux documents¹⁰⁶.

Le tableau qui suit présente l'ensemble des lois existant dans le corpus législatif québécois, en date de mars 2026¹⁰⁷, qui contiennent des dérogations des types ci-dessus.

Dérogations aux articles 9, 10, 83 et 171 de la Loi sur l'accès, ou à l'ensemble de cette loi en contexte d'accès aux documents, présentes dans le corpus législatif québécois en date de mars 2026

Loi	Article	Article(s) de la Loi sur l'accès concerné(s)	Dérogation ajoutée depuis 2016
A-29.01 – Loi sur l'assurance médicaments	60.0.3	9	Non
A-3.001 – Loi sur les accidents du travail et les maladies professionnelles	43	Dérogation totale	Non
A-32.1 – Loi sur les assureurs	56 al. 3	9	Non
A-32.1 – Loi sur les assureurs	57	9 et 83	Non
A-33.2.1 – Loi sur l'Autorité des marchés publics	36.1 al. 2	9 et 83	Oui
A-33.2.1 – Loi sur l'Autorité des marchés publics	73	9	Oui

¹⁰⁵ Dans le cadre de la présente analyse, la Commission se limite aux dérogations visant ces articles de la Loi sur l'accès constatées en 2016 et en 2026; l'exercice réalisé a donc une portée différente de celui qui appuyait l'annexe 2 du Rapport quinquennal 2016.

¹⁰⁶ La Commission n'a ainsi pas considéré les dérogations totales qui sont surtout applicables dans un contexte de communication de renseignements personnels, et non d'accès aux documents.

¹⁰⁷ Les dérogations abrogées depuis 2016 ne figurent pas dans le tableau.



Loi	Article	Article(s) de la Loi sur l'accès concerné(s)	Dérogation ajoutée depuis 2016
A-6.002 – Loi sur l'administration fiscale	69.0.0.15 al. 1	9 et 83	Non
A-8.2 – Loi sur les agents d'évaluation du crédit	43 al. 3	9	Oui
A-8.2 – Loi sur les agents d'évaluation du crédit	44	9 et 83	Oui
B-1.1 – Loi sur le bâtiment	129.2.3	9 et 83	Oui
B-1.2 – Loi sur Bibliothèque et Archives nationales du Québec	20	Dérogation totale	Non
C-11 – Charte de la langue française	203 al. 3	9	Oui
C-11 – Charte de la langue française	47.1 al. 3	9	Non
C-11.4 – Charte de la Ville de Montréal, métropole du Québec	Annexe C, article 23	83	Non
C-12 – Charte des droits et libertés de la personne	93 al. 1	9 et 83	Non
C-19 – Loi sur les cités et villes	114.2 al. 2	171	Non
C-19 – Loi sur les cités et villes	573 (3.1)	9	Non
C-19 – Loi sur les cités et villes	573.1.0.13 al. 2	9	Oui
C-19 – Loi sur les cités et villes	573.19	9	Non
C-23.1 – Code d'éthique et de déontologie des membres de l'Assemblée nationale	113	Dérogation totale	Non
C-25.01 – Code de procédure civile	607	9	Non
C-27.1 – Code municipal du Québec	1104.7 al. 2	9	Non
C-27.1 – Code municipal du Québec	209 al. 2	171	Non
C-27.1 – Code municipal du Québec	935 (3.1)	9	Non
C-27.1 – Code municipal du Québec	936.0.13 al. 2	9	Oui
C-35 – Loi sur la Commission municipale	23.8 al. 2	9	Non
C-37.01 – Loi sur la Communauté métropolitaine de Montréal	108 al. 8	9	Non
C-37.01 – Loi sur la Communauté métropolitaine de Montréal	112.0.1 al. 2	9	Oui
C-37.02 – Loi sur la Communauté métropolitaine de Québec	101 al. 8	9	Non
C-37.02 – Loi sur la Communauté métropolitaine de Québec	105.0.1 al. 2	9	Oui
C-37.4 – Loi autorisant la communication de renseignements personnels aux familles d'enfants autochtones disparus ou décédés à la suite d'une admission en établissement	11	83	Oui
C-47.1 – Loi sur les compétences municipales	78.12 al. 3	9	Non
C-65.01 – Loi sur les contrats des organismes municipaux	48 al. 3	9	Oui
C-65.01 – Loi sur les contrats des organismes municipaux	55 al. 3	9	Oui
C-65.01 – Loi sur les contrats des organismes municipaux	67 al. 2	9	Oui
C-65.01 – Loi sur les contrats des organismes municipaux	82 al. 2	9	Oui
C-65.1 – Loi sur les contrats des organismes publics	58.1 al. 1	9	Oui
C-67.3 – Loi sur les coopératives de services financiers	131.5 al. 3	9	Non
C-67.3 – Loi sur les coopératives de services financiers	131.6	9 et 83	Non
C-68.01 – Loi sur les coroners	180	Dérogation totale	Non



Loi	Article	Article(s) de la Loi sur l'accès concerné(s)	Dérogation ajoutée depuis 2016
C-73.2 – Loi sur le courtage immobilier	134 al. 3	9	Non
D-11.1 - Loi facilitant la divulgation d'actes répréhensibles à l'égard des organismes publics	29.1 al. 2	9 et 83	Oui
D-15.1 – Loi concernant les droits sur les mutations immobilières	22 al. 3	9	Non
D-9.2 – Loi sur la distribution de produits et services financiers	103.5 al. 3	9	Non
D-9.2 – Loi sur la distribution de produits et services financiers	103.6	9 et 83	Non
E-12.001 – Loi sur l'équité salariale	102.2 al. 6	9	Non
E-2.2 – Loi sur les élections et les référendums dans les municipalités	659 al. 1	9	Non
E-2.2 – Loi sur les élections et les référendums dans les municipalités	888 al. 2	9	Non
E-2.3 – Loi sur les élections scolaires visant certains membres des conseils d'administration des centres de services scolaires anglophones	282 al. 4	9	Non
E-3.3 – Loi électorale	126 al. 2	9	Non
E-3.3 – Loi électorale	246 al. 3	10	Non
E-3.3 – Loi électorale	436 al. 3	9	Non
E-3.3 – Loi électorale	457.7 al. 2	10	Non
E-3.3 – Loi électorale	570 al. 2	9	Non
E-6.1 – Loi sur l'encadrement du secteur financier	16 al. 2	9	Non
F-2.1 – Loi sur la fiscalité municipale	73.1 al. 1	9	Oui
F-2.1 – Loi sur la fiscalité municipale	79 al. 1	9	Non
F-3.1.1 – Loi sur la fonction publique	116.4 al. 2	9	Non
G-1.021 – Loi sur la gouvernance du système de santé et de services sociaux	178	Dérogation totale	Non
G-1.021 – Loi sur la gouvernance du système de santé et de services sociaux	211	Dérogation totale	Non
G-1.021 – Loi sur la gouvernance du système de santé et de services sociaux	224	Dérogation totale	Non
G-1.021 – Loi sur la gouvernance du système de santé et de services sociaux	405	9	Oui
G-1.021 – Loi sur la gouvernance du système de santé et de services sociaux	644	9	Oui
H-5 – Loi sur Hydro-Québec	49 al. 4	83	Non
I-13.011 – Loi sur l'Institut de la statistique du Québec	30 al. 2	9	Non
I-13.2.2 – Loi sur les institutions de dépôts et la protection des dépôts	28.17 al. 3	9	Oui
I-13.2.2 – Loi sur les institutions de dépôts et la protection des dépôts	28.18	9 et 83	Oui
I-14.01 – Loi sur les instruments dérivés	77.2 al. 3	9	Non
I-14.01 – Loi sur les instruments dérivés	77.3	9 et 83	Non
I-14.01 – Loi sur les instruments dérivés	93.1	9	Non
J-3 – Loi sur la justice administrative	123 al. 2	9	Non
J-3 – Loi sur la justice administrative	89 al. 1	9	Non



Loi	Article	Article(s) de la Loi sur l'accès concerné(s)	Dérogation ajoutée depuis 2016
LQ 2025, c. 38 – Loi sur la découvrabilité des contenus culturels francophones dans l'environnement numérique ¹⁰⁸	33	9	Oui
LQ 2025, c. 38 – Loi sur la découvrabilité des contenus culturels francophones dans l'environnement numérique	39	9	Oui
M-32.2 – Loi sur le ministère du Travail	15 al. 2	9	Non
N-1.1 – Loi sur les normes du travail	123.3 al. 4	9	Non
P-29 – Loi sur les produits alimentaires	9.2	9	Oui
P-32 – Loi sur le Protecteur du citoyen	34 al. 2	9 et 83	Non
P-32.01 - Loi sur le protecteur national de l'élève	52 al. 2	9	Oui
P-33.01 - Loi sur la protection contre les représailles liées à la divulgation d'actes répréhensibles	10 al. 3	9	Oui
P-39.3 – Loi visant à assurer la protection des stagiaires en milieu de travail	22 al. 4	9	Oui
P-44.1 – Loi sur la publicité légale des entreprises	131 al. 2	9	Non
P-9.0001 – Loi concernant le partage de certains renseignements de santé	112	83	Non
P-9.0001 – Loi concernant le partage de certains renseignements de santé	77	83	Non
P-9.002 – Loi sur le patrimoine culturel	73 al. 1	9	Non
P-9.02 – Loi sur la performance environnementale des bâtiments	17 al. 3	9	Oui
R-20 – Loi sur les relations du travail, la formation professionnelle et la gestion de la main-d'œuvre dans l'industrie de la construction	123.8 al. 2	9 et 83	Oui
R-6.01 – Loi sur la Régie de l'énergie	100.3 al. 2	9	Non
R-8.3 – Loi concernant le régime de négociation des conventions collectives et de règlement des différends dans le secteur municipal	43 al. 3	9	Oui
R-9 – Loi sur le régime de rentes du Québec	192 al. 3	83	Non
R-9 – Loi sur le régime de rentes du Québec	211 al. 2	83	Non
S-2.1 – Loi sur la santé et la sécurité du travail	62.21	9	Non
S-29.02 – Loi sur les sociétés de fiducie et les sociétés d'épargne	40 al. 3	9	Non
S-29.02 – Loi sur les sociétés de fiducie et les sociétés d'épargne	41	9 et 83	Non
S-3.1 - Loi sur la sécurité dans les loisirs et les sports	30.29 al. 2	9	Oui
S-3.4 – Loi sur la sécurité incendie	133	9	Non
S-3.5 – Loi sur la sécurité privée	81 al. 2	9	Non
S-30.01 – Loi sur les sociétés de transport en commun	95 al. 8	9	Non
S-30.01 – Loi sur les sociétés de transport en commun	99.1 al. 2	9	Oui
S-32.1 – Loi sur le statut professionnel des artistes des arts visuels, du cinéma, du disque, de la littérature, des métiers d'art et de la scène	68.4 al. 2	9	Non

¹⁰⁸ Cette loi a été sanctionnée en décembre 2025, mais n'est pas encore en vigueur. Elle le sera à la ou aux date(s) déterminée(s) par le gouvernement.



Loi	Article	Article(s) de la Loi sur l'accès concerné(s)	Dérogation ajoutée depuis 2016
S-4.2 – Loi sur les services de santé et les services sociaux pour les Inuit et les Naskapis	116.1	9	Non
S-4.2 – Loi sur les services de santé et les services sociaux pour les Inuit et les Naskapis	183.4	Dérogation totale	Non
S-4.2 – Loi sur les services de santé et les services sociaux pour les Inuit et les Naskapis	190	Dérogation totale	Non
S-4.2 – Loi sur les services de santé et les services sociaux pour les Inuit et les Naskapis	218	Dérogation totale	Non
S-4.2 – Loi sur les services de santé et les services sociaux pour les Inuit et les Naskapis	280	9	Non
S-4.2 – Loi sur les services de santé et les services sociaux pour les Inuit et les Naskapis	76.9	Dérogation totale	Oui
S-40.1 – Loi sur le système correctionnel du Québec	175.1	9 et 83	Non
S-5 – Loi sur les services de santé et les services sociaux pour les autochtones cris	114	Dérogation totale	Non
S-5 – Loi sur les services de santé et les services sociaux pour les autochtones cris	7	83	Non
S-5 – Loi sur les services de santé et les services sociaux pour les autochtones cris	8.1	83	Non
T-12 – Loi sur les transports	35.3	9	Non
T-15.01 – Loi sur le tribunal administratif du logement	31.04 al. 2	9	Oui
T-15.1 – Loi instituant le tribunal administratif du travail	13.1 al. 1	9	Oui
T-15.1 – Loi instituant le tribunal administratif du travail	25 al. 2	9	Non
V-1.1 – Loi sur les valeurs mobilières	168.1.6 al. 3	9	Non
V-1.1 – Loi sur les valeurs mobilières	168.1.7	9 et 83	Non
V-1.1 – Loi sur les valeurs mobilières	296 al. 3	9	Non
V-1.1 – Loi sur les valeurs mobilières	297	9	Non

En 2016, il existait 89 dérogations aux articles 9, 10, 83 et 171 de la Loi sur l'accès, ou à l'ensemble de cette loi en contexte d'accès aux documents. Ce nombre est désormais passé à 118 :

- 36 dérogations ont été adoptées depuis 2016¹⁰⁹;
- 7 dérogations ont été abrogées¹¹⁰.

¹⁰⁹ Les dérogations qui existaient en 2016 et qui ont été reprises dans le cadre de la refonte d'une loi n'ont pas été considérées comme étant de nouvelles dérogations (c'est le cas par exemple pour la *Loi sur les assurances*, RLRQ, c. A-32, devenue la *Loi sur les assureurs*, RLRQ, c. A-32.1, et de la *Loi sur les sociétés de fiducie et les sociétés d'épargne* (anciennement RLRQ c. S-29.01, devenue RLRQ c. S-29.02).

¹¹⁰ Il s'agit de dispositions dont les lois ont fait l'objet de refontes ou de révision. Ces opérations n'ont pas mené à la reconduction de l'ensemble des dérogations initialement relevées en 2016. Les dispositions concernées sont les suivantes : *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.01, art. 395; *Loi sur les assurances*, RLRQ, c. A-32, art. 16; *Loi sur les accidents du travail et les maladies professionnelles*, RLRQ, c. A-3.001, art. 429.48; *Loi sur les véhicules hors route*, RLRQ, c. V-1.2, art. 45.11; *Loi sur l'assurance maladie*, RLRQ, c. A-29, art. 64; *Loi visant principalement la récupération de sommes payées injustement à la suite de fraudes ou de manœuvres dolosives dans le cadre de contrats publics*, RLRQ, c. R-2.2.0.0.3, art. 8; *Loi sur l'Institut de la statistique du Québec*, RLRQ, c. I-13.1.1, art. 34.



1.2. Le traitement des demandes d'accès

1.2.1. Les restrictions au droit d'accès

Sommaire

La Loi sur l'accès restreint dans certains cas l'accessibilité des documents des organismes publics ou des renseignements personnels qu'ils détiennent pour protéger certains autres intérêts légitimes, comme la sécurité publique ou les relations économiques. Bien que la protection de ces intérêts conserve toute sa nécessité, la Commission souligne que le régime de restrictions actuel, pratiquement inchangé en 44 ans, comporte des lacunes substantielles qui nuisent à l'exercice de droits fondamentaux et à la confiance des citoyens envers l'administration publique. Il engendre de nombreux refus d'accès et du caviardage parfois excessif.

Comme elle l'expose dans cette section, la Commission relève notamment que :

- certaines restrictions s'appliquent trop largement ou sur une période trop longue, ou bien se recoupent;
- certaines restrictions s'appliquent sans que l'organisme doive démontrer que l'accès causerait un préjudice;
- les restrictions obligatoires sont trop nombreuses;
- l'intérêt public n'est pas suffisamment pris en compte;
- l'interprétation selon laquelle les restrictions obligatoires au droit d'accès aux documents deviennent facultatives en matière d'accès aux renseignements personnels a récemment été remise en cause par un jugement.

Selon la Commission, la situation nécessite une révision et une modernisation globale de l'ensemble des restrictions pour :

- limiter les restrictions au droit d'accès uniquement à ce qui est nécessaire afin de protéger des intérêts légitimes;
- viser une diffusion maximale de l'information relative aux organismes publics.

1.2.1.1. Contexte

Après 44 ans, la Commission estime qu'une révision complète des restrictions au droit d'accès est indispensable. Il est plutôt évocateur de constater que, dans le classement international des lois sur



l'accès à l'information évoqué dans l'introduction du présent chapitre, la Loi sur l'accès obtient une note d'à peine 11 points sur une possibilité de 30 concernant les restrictions au droit d'accès¹¹¹.

Le droit d'accès, malgré sa grande importance, n'est pas absolu. Un certain nombre de restrictions en limitent l'exercice aux fins de protéger des intérêts légitimes. Le gouvernement et les organismes publics ont besoin d'une sphère de confidentialité en certaines circonstances.

Cela dit, les restrictions actuelles de la Loi sur l'accès datent d'une autre époque. Elles ne conviennent plus aux attentes élevées de la population en matière d'accès à l'information et de transparence de l'État, ni aux standards internationaux modernes, qui établissent généralement qu'une loi sur l'accès doit être fondée sur un principe de divulgation maximale¹¹². Cela signifie que les motifs permettant de refuser l'accès ou de caviarder certaines parties de documents doivent être limités et circonscrits de façon précise et minutieuse.

1.2.1.2. Situation actuelle

En matière d'accès à l'information, la Loi sur l'accès énonce deux principes généraux :

- Toute personne qui en fait la demande a droit d'accès aux documents d'un organisme public¹¹³.
- Toute personne a le droit d'être informée de l'existence d'un renseignement personnel la concernant et d'en recevoir communication¹¹⁴.

Ces droits ne s'appliquent pas de manière universelle, car comme le rappelait déjà la Commission Paré au moment de recommander l'adoption de la Loi, celle-ci doit pondérer plusieurs intérêts concurrents¹¹⁵ :

Il arrive que l'intérêt public soit mieux servi par l'accès aux documents administratifs; il arrive qu'il soit mieux servi par la confidentialité. [...] Les exceptions inévitables doivent être peu nombreuses, rigoureusement définies et ne pas laisser place à l'arbitraire. Leur but est d'assurer un juste équilibre entre des objectifs contradictoires en apparence et de garantir trois droits concurrents: le droit à l'information, le droit à la vie privée, le droit au bon gouvernement.

¹¹¹ CENTRE FOR LAW AND DEMOCRACY, préc., note 33. Parmi les critères évalués, on retrouve : l'alignement des restrictions à celles habituellement acceptées dans les standards internationaux; l'existence d'un test de préjudice pour chaque restriction; l'existence d'une disposition prévoyant la primauté de l'intérêt public dans la divulgation des documents; la limitation de la durée des restrictions à un maximum de 20 ans; la possibilité de communiquer les documents partiellement en masquant seulement l'information inaccessible.

¹¹² Voir notamment : COMMISSAIRES À L'INFORMATION CANADIENS ET OMBUDS FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX, « Transparence par défaut – Les autorités de contrôle en matière d'accès à l'information réclament une nouvelle norme pour les services gouvernementaux », *Commissariat à l'information du Canada* (10 décembre 2024), en ligne : <<https://www.oic-ci.gc.ca/fr/ressources/communiqués-presse/les-commissaires-l'information-et-les-ombuds-du-canada-adoptent-une#transparence>> (consulté le 11 mars 2025); COMMISSAIRES ET OMBUDS À L'INFORMATION FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX, « Faciliter l'accès des Canadiens et Canadiennes aux documents gouvernementaux en vue de rétablir la confiance à l'égard de nos institutions », *Commissaire à l'information du Canada* (4 octobre 2023), en ligne : <<https://www.oic-ci.gc.ca/fr/ressources/communiqués-presse/les-autorités-de-contrôle-en-matière-d'accès-l'information-fédérale>> (consulté le 17 novembre 2023); AUSTRALIAN INFORMATION COMMISSIONERS AND OMBUDSMEN, *Statement of Principles to support proactive disclosure of government-held information*, 2021, en ligne : <https://www.oaic.gov.au/__data/assets/pdf_file/0013/10840/Statement-of-Open-by-Design-Principles.pdf>.

¹¹³ Loi sur l'accès, art. 9.

¹¹⁴ *Id.*, art. 83.

¹¹⁵ COMMISSION D'ÉTUDE SUR L'ACCÈS DU CITOYEN À L'INFORMATION GOUVERNEMENTALE ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, préc., note 1, p. 7-8.



Le législateur a donc prévu à la Loi sur l'accès des restrictions qui permettent ou obligent un organisme public à refuser l'accès à certains renseignements¹¹⁶. Elles sont introduites dans plusieurs dispositions concernant la protection de divers intérêts légitimes.

Pour ne donner que quelques exemples en matière d'accès aux documents, certaines restrictions ont ainsi pour objectif de préserver les intérêts suivants :

- La vie privée des autres personnes.
- La bonne conduite des relations intergouvernementales.
- L'intérêt économique du gouvernement ou celui de tiers.
- La sécurité publique et l'administration de la justice.
- Le processus décisionnel en matière administrative ou politique.

Les restrictions peuvent être classées en deux catégories, selon leur nature facultative ou obligatoire :

- **Les restrictions facultatives** permettent à un organisme public de refuser l'accès à certains renseignements ou documents. L'organisme jouit donc d'une discrétion : il peut décider, à la suite d'une évaluation, de donner accès ou non à l'information concernée.
- **Les restrictions obligatoires**¹¹⁷ concernent des intérêts légitimes particulièrement importants, comme la sécurité publique. Elles s'appliquent systématiquement : elles obligent l'organisme public à protéger les renseignements ou documents qu'elles visent, sans possibilité d'agir autrement.

La section 1.2.1.5.3 présente la liste des restrictions facultatives et obligatoires.

Il importe de souligner que lorsque la Commission constate, dans le cadre d'une demande de révision, que des documents sont concernés par une restriction obligatoire, elle doit agir de manière à s'assurer qu'elle soit bien appliquée.

Enfin, en matière d'accès aux renseignements personnels, la Loi sur l'accès prévoit qu'un organisme public peut également tenir compte des restrictions applicables en matière d'accès aux documents¹¹⁸. Ce lien entre ces deux volets de la Loi sur l'accès sera examiné plus avant dans la section 1.2.1.3.5.

1.2.1.3. Enjeux

La Commission expose ci-après plusieurs enjeux en lien avec les restrictions actuelles, dont l'imprécision de certaines d'entre elles, la longue durée de protection des documents, la variabilité dans l'obligation de démontrer un préjudice pour invoquer des restrictions et la quantité de restrictions obligatoires. De plus, elle note que la Loi sur l'accès ne tient pas adéquatement compte de la primauté de l'intérêt public. Enfin, un jugement récent¹¹⁹ a conclu que les restrictions obligatoires en matière d'accès aux documents restent obligatoires lorsqu'il s'agit du traitement d'une demande d'accès aux renseignements personnels par la personne concernée, alors que l'interprétation antérieure voulait qu'elles deviennent facultatives dans ce cas, en raison du libellé de l'article les rendant applicables à une telle demande. Cette évolution affecte l'équilibre d'intérêts qui avait été établi par la jurisprudence antérieure.

¹¹⁶ En matière de documents d'un organisme public, ce sont les articles 18 à 41 de la Loi sur l'accès qui prévoient les restrictions applicables. Les articles 41.1 et 41.2 prévoient des cas spécifiques dans lesquels les restrictions sont inapplicables. En matière de renseignements personnels concernant une personne, ce sont les articles 86 à 88.1 qui prévoient les restrictions applicables.

¹¹⁷ Il s'agit des articles 24, 28, 28.1, 29 et 29.1 al. 2 et al. 3 de la Loi sur l'accès.

¹¹⁸ *Id.*, art. 87.

¹¹⁹ *Ville de St-Jean-sur-Richelieu (Service de police) c. Cour du Québec*, 2024 QCCS 3155, en ligne : <<https://canlii.ca/t/jhhld>>.

Il y a aussi lieu de souligner que l'interprétation et l'application des restrictions dépendent, initialement, de chacun des organismes publics traitant des demandes d'accès. Cette décentralisation contribue à causer des applications et des interprétations variables à travers les divers organismes publics.

Ainsi, la Commission est d'avis que le cadre légal actuel, combiné avec certaines situations problématiques pouvant survenir dans certains organismes publics, comme une certaine opacité, un sous-investissement en accès ou encore la formation inadéquate du responsable de l'accès et de ses collaborateurs, peut contribuer à exacerber la méfiance du public envers les institutions¹²⁰.

Ces facteurs peuvent entraîner des refus d'accès répétitifs ou insuffisamment motivés. Ils peuvent aussi résulter en la communication de documents abondamment caviardés, au point de parfois les vider de leur substance. Ces situations génèrent une frustration légitime chez les personnes qui exercent leur droit d'accès.

La transparence étant la norme, l'application des restrictions devrait conserver un caractère exceptionnel, et leur utilisation par les organismes publics devrait être parcimonieuse, adéquatement réfléchie et la plus uniforme possible.

1.2.1.3.1. Certaines restrictions s'appliquent trop largement ou sur une trop longue période, ou se chevauchent

La portée d'une restriction est déterminée par :

- l'organisation qui peut l'invoquer;
- les critères d'application qui le lui permettent;
- les situations qui excluent son application.

Actuellement, certaines restrictions vagues et imprécises sont sujettes à des applications larges, ce qui ne favorise pas la transparence et la divulgation maximale en matière d'accès à l'information. Cette situation s'explique notamment par :

- l'utilisation de termes généraux, et donc très englobants ou susceptibles d'être interprétés subjectivement, comme « avis », « recommandation » ou « analyse »¹²¹;
- le fait que certaines restrictions peuvent être invoquées sans nécessiter la démonstration d'un préjudice lorsqu'elles impliquent une personne autre que le responsable de l'accès, comme dans le cas des restrictions établissant la confidentialité de certains documents, sauf si leur auteur ou un membre du Conseil exécutif ou de l'Assemblée nationale en « décide autrement » ou « juge opportun » de les divulguer¹²². La Commission y revient dans la section 1.2.1.5.1.3.

Par ailleurs, un chevauchement partiel de portée existe lorsque plusieurs dispositions semblent protéger des intérêts légitimes similaires et des renseignements de nature semblable. Comme le précise la Commission aux sections 1.2.1.5.1.1 et 1.2.1.5.1.2, certaines restrictions concernant les affaires intergouvernementales¹²³ ou les processus décisionnels¹²⁴ en sont des exemples. L'impression de redondance générée par cette situation peut contribuer à exacerber la perception que le cadre juridique

¹²⁰ Voir la section 1.3.1.

¹²¹ Loi sur l'accès, art. 37 à 39.

¹²² *Id.*, art. 33 et 34.

¹²³ *Id.*, art. 18 et 19.

¹²⁴ *Id.*, art. 37 et 38.

applicable est flou et complexe, tant pour les responsables d'accès devant lui donner application que les citoyens qui reçoivent une décision d'un organisme public invoquant ces restrictions.

Un autre enjeu se situe dans la durée d'application de certaines restrictions. Certaines prévoient une durée d'application en nombre d'années. Ainsi, il n'est plus possible de les invoquer au-delà d'un certain délai¹²⁵ qui est, dans certains cas, trop long pour la teneur des intérêts légitimes protégés. Certaines durées semblent excéder ce qui est nécessaire pour protéger les délibérations stratégiques dans les organismes publics. Par exemple :

- la Loi sur l'accès prévoit l'inaccessibilité des documents délibératifs du conseil d'administration d'un organisme public pendant 15 ans¹²⁶;
- plusieurs documents du Conseil exécutif ou du Conseil du trésor ne peuvent être divulgués avant l'expiration d'un délai minimal de 25 ans suivant leur création¹²⁷.

D'autres restrictions s'appliquent sans limites temporelles¹²⁸, alors que le passage du temps atténue les préjudices potentiels aux intérêts légitimes qu'elles visent à protéger. Les organismes publics pourront donc toujours les invoquer, même des dizaines d'années après les circonstances visées. Par exemple, un organisme public peut refuser de divulguer un renseignement obtenu d'un gouvernement autre que celui du Québec, d'un organisme d'un tel gouvernement ou d'une organisation internationale¹²⁹, indépendamment du délai écoulé depuis la fourniture des renseignements.

1.2.1.3.2. Certaines restrictions ne requièrent pas de démontrer un préjudice

Plusieurs restrictions trouvent application du fait qu'un document visé par une demande d'accès correspond à une catégorie donnée. Dans son rapport quinquennal de 2016, la Commission en donnait plusieurs exemples : « avis, analyse, recommandation, décision du Conseil exécutif ou du Conseil du trésor, document du bureau du cabinet d'un ministre, document obtenu d'un autre gouvernement, renseignement industriel, technique, syndical, financier, commercial confidentiel, etc.¹³⁰ ».

Autrement dit, bien que les restrictions visent à protéger des intérêts légitimes, plusieurs d'entre elles peuvent être invoquées sans démontrer un préjudice à ces intérêts – elles sont recensées dans la section 1.2.1.5.3. Par exemple, un organisme public peut refuser de communiquer un document obtenu d'un autre gouvernement simplement parce qu'il s'agit d'un tel document, et non parce qu'une telle communication soulèverait réellement un enjeu pour la préservation des relations intergouvernementales, comme exposé plus avant à la section 1.2.1.5.1.1.

Par contraste, d'autres restrictions sont bel et bien codifiées de manière à exiger une démonstration de risque vraisemblable de préjudice. À titre d'illustration, un organisme public peut invoquer une restriction facultative pour refuser l'accès à un tel renseignement dont la divulgation aurait pour effet de révéler un emprunt ou une transaction, effectifs ou projetés, ou encore un projet de tarification, de taxation ou de redevance¹³¹. Pour ce faire, il doit cependant établir qu'une telle divulgation, vraisemblablement, « procurerait un avantage indu à une personne ou lui causerait un préjudice sérieux » ou « porterait

¹²⁵ Par exemple : *Id.*, art. 27, 30, 33, 35, 36, 37 et 39.

¹²⁶ *Id.*, art. 35.

¹²⁷ *Id.*, art. 30 et 33.

¹²⁸ Par exemple : *Id.*, art. 18, 34 et 38.

¹²⁹ Voir la section 1.2.1.5.1.1.

¹³⁰ Rapport quinquennal 2016, p. 22.

¹³¹ Loi sur l'accès, art. 21.

sérieusement atteinte aux intérêts économiques de l'organisme public ou de la collectivité à l'égard de laquelle il est compétent ».

Il est important de noter que, suivant les dispositions actuelles, dès lors que la Loi sur l'accès prévoit une discrétion de l'organisme public dans l'application d'une restriction, le pouvoir d'intervention de la Commission dans le cadre d'une demande de révision est limité. Ainsi, lorsqu'une disposition n'aborde pas la nécessité de faire la démonstration d'un préjudice, la Commission ne peut pas statuer à ce sujet. En effet, même dans des cas probants de restriction invoquée sans véritable risque de préjudice pour un intérêt légitime, la Commission est actuellement cantonnée à constater la validité de l'application de la restriction, dès lors que ses autres critères d'application sont satisfaits.

1.2.1.3.3. Les restrictions obligatoires sont trop nombreuses

Les restrictions facultatives ont l'avantage de la flexibilité : elles n'ont pas à être invoquées en toutes circonstances. Au contraire, les restrictions obligatoires s'appliquent de manière indiscriminée lorsque leurs critères d'application sont satisfaits, que ce soit au moment du traitement de la demande d'accès par l'organisme public ou à tout moment au cours d'une demande de révision. Il s'agit donc d'outils à large spectre, qui devraient être limités à des cas exceptionnels. Or, la Commission estime que le corpus législatif compte actuellement un trop grand nombre de restrictions obligatoires étant donné leur effet.

Par exemple, les restrictions concernant les renseignements ayant des incidences sur l'administration de la justice et la sécurité publique sont d'application obligatoire¹³². Elles doivent être invoquées, et ce, même en l'absence d'un réel risque de péril à la sécurité publique ou au travail des policiers, puisque la loi n'en fait pas une exigence pour permettre leur application. Pourtant, plusieurs provinces canadiennes¹³³ ainsi que certains pays¹³⁴ ne refusent pas d'emblée l'accès aux documents contenant de tels renseignements, énonçant plutôt des restrictions facultatives associées à une démonstration de préjudice.

Il semble contradictoire et difficile de justifier l'inclusion dans la Loi sur l'accès, dont l'objectif principal est d'assurer la transparence gouvernementale, d'une obligation légale imposant le refus systématique d'accès à certains documents des organismes publics. De telles restrictions obligatoires contribuent à entretenir l'idée selon laquelle certains renseignements doivent demeurer confidentiels en tout temps, sans égard pour le contexte. La Commission est plutôt d'avis que la transparence devrait toujours primer si aucun motif d'intérêt public ne s'y oppose.

1.2.1.3.4. L'intérêt public n'est pas suffisamment pris en compte

En l'absence d'une disposition générale concernant l'intérêt public, la Commission constate que certaines restrictions, tant obligatoires que facultatives, sont fréquemment invoquées simplement parce que leurs critères d'application sont remplis.

¹³² *Id.*, art. 28 à 29.1.

¹³³ Voir notamment la Colombie-Britannique : *Freedom of Information and Protection of Privacy Act [Colombie-Britannique]*, RSBC 1996, c. 165, art. 15 [ci-après FIPPA de la Colombie-Britannique], en ligne : <https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00_multi>; l'Ontario : *Loi sur l'accès à l'information municipale et la protection de la vie privée [Ontario]*, L.R.O 1990, c. M-56, art. 14, en ligne : <<https://www.ontario.ca/lois/loi/90m56>>; le Nouveau-Brunswick : *Loi sur le droit à l'information et la protection de la vie privée [Nouveau-Brunswick]*, L.N.-B. 2009, c. R-10.6, art. 29, en ligne : <<http://laws.gnb.ca/fr/ShowTdm/cs/R-10.6/>>.

¹³⁴ Par exemple, la Nouvelle-Zélande : *Official Information Act 1982 [Nouvelle-Zélande]*, 1982 n. 156, art. 6 et 10, en ligne : <<https://www.legislation.govt.nz/act/public/1982/0156/latest/whole.html#DLM64785>>.

La Loi sur l'accès prévoit déjà que la plupart des restrictions ne s'appliquent pas dans certaines circonstances relevant de l'intérêt public. Ainsi, lorsque le renseignement concerné :

- révèle ou confirme « l'existence d'un risque immédiat pour la vie, la santé ou la sécurité d'une personne ou d'une atteinte sérieuse ou irréparable à son droit à la qualité de l'environnement »¹³⁵, sauf exception, les restrictions deviennent inapplicables, sauf celles des articles 28, 28.1, 29, 30, 33, 34 et 41 de la Loi¹³⁶;
- se rapporte à « la quantité, la qualité ou la concentration des contaminants émis, dégagés, rejetés ou déposés par une source de contamination » ou à « la présence d'un contaminant dans l'environnement »¹³⁷, la quasi-totalité des restrictions deviennent inapplicables, sauf celles de l'article 28 et, dans certains cas, de l'article 41¹³⁸.

D'une part, ces circonstances relevant de l'intérêt public sont assez restreintes. D'autre part, cette disposition n'écarter pas l'application de l'ensemble des restrictions au droit d'accès. La Commission considère ainsi qu'il est surprenant que des risques immédiats pour la vie, la santé ou la sécurité d'une personne ne puissent pas actuellement l'emporter en tout temps, y compris sur toutes les restrictions obligatoires¹³⁹. Le même constat doit être fait lorsqu'il est question d'une atteinte sérieuse ou même irréparable au droit d'une personne à la qualité de l'environnement.

Actuellement, d'une manière comparable à ce qui a été présenté à la fin de la section 1.2.1.3.2, la Commission ne possède que peu de leviers dans le cadre de ses fonctions juridictionnelles pour agir face à ces situations puisque les conditions d'application des restrictions ne prévoient pas l'examen de l'intérêt public. Un organisme public démontrant qu'une restriction existe et qu'il respecte ses conditions d'application bloque *de facto* toute possibilité d'intervention de la Commission, même si la situation laisse planer un doute sur le bien-fondé de la décision d'invoquer cette restriction.

1.2.1.3.5. L'interprétation de l'application des restrictions en matière d'accès aux renseignements personnels a été élargie

Un jugement récent de la Cour supérieure a remis en question des décennies de jurisprudence en élargissant l'application, en matière d'accès aux renseignements personnels, des restrictions visant normalement le droit d'accès aux documents.

Ainsi, en ce qui a trait au traitement des demandes d'accès aux renseignements personnels, la Loi sur l'accès réfère textuellement aux restrictions prévues en matière d'accès aux documents des organismes publics¹⁴⁰ :

*87. Sauf dans le cas prévu à l'article 86.1, un organisme public **peut refuser de confirmer l'existence ou de donner communication à une personne d'un renseignement personnel la concernant, dans la mesure où la communication de cette information révélerait un renseignement dont la communication doit ou peut être refusée en vertu de la section II du chapitre II ou en vertu des articles 108.3 et 108.4 du Code des professions (chapitre C-26).***

¹³⁵ Loi sur l'accès, art. 41.1.

¹³⁶ Les tableaux de la section 1.2.1.5.3 donnent plus de détails sur la nature des intérêts légitimes protégés par ces restrictions.

¹³⁷ Loi sur l'accès, art. 41.1 al. 2.

¹³⁸ Les tableaux de la section 1.2.1.5.3 donnent plus de détails sur la nature des intérêts légitimes protégés par ces restrictions.

¹³⁹ En effet, l'article 41.1 de la Loi sur l'accès n'écarter pas l'application des restrictions obligatoires prévues aux articles 28, 28.1, 29 et 33, qui concernent principalement la prévention, la détection ou la répression du crime ou des infractions aux lois, la sécurité de l'État et celle des biens ou des personnes, de même que les activités du Conseil exécutif et du Conseil du trésor.

¹⁴⁰ Loi sur l'accès, art. 87; nous soulignons.



Cette disposition soulève la question de l'interprétation du caractère obligatoire ou facultatif, *lorsqu'une personne demande accès à ses propres renseignements personnels*, des restrictions normalement obligatoires prévues par la Loi sur l'accès en matière d'accès aux documents¹⁴¹. Deux courants jurisprudentiels se sont opposés sur cette question, le plus récent l'emportant désormais.

1.2.1.3.5.1. L'interprétation antérieure rendait facultatives certaines restrictions obligatoires en accès aux documents

Un premier courant a prévalu à la Cour du Québec et à la Commission jusqu'à une décision de la Cour supérieure rendue en 2024, évoquée plus en détail à la section 1.2.1.3.5.2. Ainsi, avant ce jugement, l'interprétation de l'article 87 de la Loi sur l'accès avait pour effet de rendre *facultative* l'application des restrictions obligatoires en matière d'accès aux documents lorsqu'il était question de l'accès d'une personne à ses renseignements personnels. Elle reposait sur le fait qu'un organisme public « peut refuser de confirmer l'existence ou de donner communication à une personne d'un renseignement la concernant ».

Concrètement, cette interprétation signifiait que, lorsqu'une personne demandait accès à ses propres renseignements personnels, le responsable de l'accès disposait d'un pouvoir discrétionnaire pour appliquer ou non les restrictions obligatoires relatives aux renseignements ayant des incidences sur l'administration de la justice et la sécurité publique¹⁴². Autrement dit, il pouvait y renoncer, ce qu'il ne peut faire dans le contexte d'une demande d'accès aux documents.

Cette interprétation reposait sur le fait que la Loi sur l'accès prévoit deux régimes distincts pour l'accès aux documents des organismes publics et l'accès aux renseignements personnels. Chacun a sa propre procédure et ses propres objectifs qui répondent à des considérations ainsi qu'à des impératifs différents¹⁴³. En ce sens, le régime d'accès à des renseignements personnels est un corollaire du droit à la vie privée prévu à la Charte¹⁴⁴.

L'interprétation antérieure favorisait l'accès des personnes à leurs propres renseignements personnels dans des délais raisonnables, puisqu'elle obligeait les organismes publics à invoquer sans tarder les restrictions facultatives s'ils le jugeaient opportun. En effet, si le responsable ne rend pas sa décision dans le délai prévu par la Loi, il est réputé avoir refusé l'accès aux renseignements personnels¹⁴⁵. Or les restrictions, si elles sont facultatives, ne peuvent être soulevées qu'à l'intérieur de ce délai initial : une telle situation signifie donc que le responsable renonce, par son silence, à les invoquer, à moins d'être relevé du défaut d'avoir produit sa décision dans les délais requis¹⁴⁶. Ainsi, l'interprétation antérieure empêchait l'invocation tardive de restrictions normalement obligatoires.

1.2.1.3.5.2. La nouvelle interprétation maintient plutôt les restrictions obligatoires pour l'accès aux renseignements personnels

La nouvelle interprétation de l'article 87 de la Loi sur l'accès, suivant le jugement de la Cour supérieure dans l'affaire *Ville de St-Jean-sur-Richelieu (Service de police) c. Cour du Québec*¹⁴⁷, conclut plutôt que les

¹⁴¹ *Id.*, art. 28, 28.1, 29 et 29.1.

¹⁴² *Id.*, art. 28, 28.1, 29, 29.1 al. 2 et 3.

¹⁴³ *Ville de Saint-Jean-sur-Richelieu (Service de police) c. X.*, 2023 QCCQ 6477, par. 35, en ligne : <<https://canlii.ca/t/k0qbc>>.

¹⁴⁴ Charte, art. 5; Voir *Popovic c. Ville de Montréal*, 2025 QCCA 190, en ligne : <<https://canlii.ca/t/kdhw6>>; voir aussi *Québec (Sous-ministre du Revenu) c. Québec (Commission d'accès à l'information)*, [1990] CANLII 3074 (QC. C.A.).

¹⁴⁵ Loi sur l'accès, art. 102.

¹⁴⁶ *Service anti-crime des assureurs c. Ménard*, [1990] CANLII 30035, par. 54 à 60 (CQ).

¹⁴⁷ *Ville de St-Jean-sur-Richelieu (Service de police) c. Cour du Québec*, préc., note 119, par. 47.



restrictions obligatoires en matière d'accès aux documents conservent ce caractère obligatoire lorsqu'il s'agit d'accès par la personne à ses renseignements personnels.

Dans son jugement, la Cour conclut que les restrictions obligatoires, notamment celles qui étaient analysées dans cette affaire, relatives aux renseignements détenus dans l'exercice d'une fonction légale de prévention, de détection ou de répression du crime ou des infractions aux lois¹⁴⁸, ne perdent pas leur caractère impératif par le biais de l'application de l'article 87 de la Loi sur l'accès. Voici les motifs présentés par la Cour supérieure :

- L'emploi du mot « doit » à l'article 87 ne porte à aucune interprétation et signifie qu'une restriction obligatoire en accès aux documents le demeure lors de l'application de cet article¹⁴⁹.
- L'interprétation antérieure mène, selon la Cour, à des résultats absurdes. Elle présente comme exemple le cas d'un membre du crime organisé qui pourrait effectuer une demande d'accès à un corps de police pour obtenir une copie du dossier d'enquête le concernant; si le délai maximal de 20 jours n'était pas respecté, le membre du crime organisé pourrait accéder à tout son dossier, puisque la restriction n'aurait pas été invoquée en temps utile¹⁵⁰.
- L'interprétation antérieure mène également, toujours selon la Cour, à un résultat non souhaitable, c'est-à-dire d'inciter les organismes publics à invoquer le plus de dispositions législatives possible pour justifier le refus, et ce, afin d'éviter de se faire opposer plus tard la règle jurisprudentielle de la forclusion¹⁵¹.

Par l'application, dans le régime d'accès aux renseignements personnels, des principes relevant du régime d'accès aux documents, ce jugement a pour effet d'obliger les organismes publics à appliquer les restrictions obligatoires lorsqu'ils traitent une demande d'accès aux renseignements personnels par la personne concernée, ce qui peut restreindre ce droit d'accès.

1.2.1.4. Recommandations

Afin de rétablir un équilibre et de préserver la confiance du public envers la transparence du régime d'accès à l'information, la Commission réitère¹⁵² qu'une révision générale des restrictions existantes doit être menée de manière exhaustive.

De l'avis de la Commission, cette révision doit essentiellement être guidée par deux objectifs :

- Limiter les restrictions au droit d'accès uniquement à ce qui est nécessaire pour protéger des intérêts légitimes.
- Viser une diffusion maximale de l'information relative aux organismes publics¹⁵³.

Plus précisément, elle doit chercher à :

¹⁴⁸ Loi sur l'accès, art. 28.

¹⁴⁹ *Ville de St-Jean-sur-Richelieu (Service de police) c. Cour du Québec*, préc., note 119, par. 47.

¹⁵⁰ *Id.*, par. 49-50.

¹⁵¹ *Id.*, par. 54.

¹⁵² Il est important de signaler que la Commission réclame depuis plusieurs années une réforme du régime des restrictions au droit d'accès. Voir notamment : COMMISSION D'ACCÈS À L'INFORMATION, *Mémoire de la Commission d'accès à l'information présenté à la Commission des institutions concernant les orientations gouvernementales pour un gouvernement plus transparent, dans le respect du droit à la vie privée et la protection des renseignements personnels*, 2015, p. 18 à 30 et 33 à 46, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_ME_Orient_Gouvern_Transparent.pdf>; Rapport quinquennal 2016, p. 15 à 29, dont la plupart des recommandations ou propositions sont reprises dans le présent rapport quinquennal.

¹⁵³ À cet égard, voir : COMMISSAIRES À L'INFORMATION CANADIENS ET OMBUDS FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX, préc., note 112.



- préciser la portée et à limiter la durée d'application des restrictions;
- généraliser l'exigence de démontrer que la divulgation d'un document risque de causer un préjudice;
- limiter les restrictions obligatoires;
- affirmer la primauté de l'intérêt public en matière d'accès à l'information;
- préciser l'application des restrictions lorsqu'il s'agit d'accès par une personne à ses renseignements personnels.

Une réforme extensive du régime de restrictions ne présenterait pas comme seul avantage de favoriser la transparence des organismes publics, mais mènerait aussi à une simplification générale qui aurait pour effet :

- de favoriser la compréhension des citoyens des différents motifs de restrictions invoqués par les organismes publics;
- de faciliter l'application des motifs de restrictions par les responsables de l'accès;
- d'assurer une interprétation plus uniforme et homogène des restrictions entre les organismes publics;
- d'augmenter l'efficacité et l'efficience globale du régime d'accès à l'information;
- de protéger adéquatement les intérêts légitimes des organismes publics.

1.2.1.4.1. Préciser la portée des restrictions

De l'avis de la Commission, une meilleure circonscription et précision de la portée des restrictions au droit d'accès contribuerait à l'élargissement de ce droit, de même qu'à une meilleure compréhension et à une application plus uniforme de la Loi par les responsables de l'accès. Les organismes publics continueraient à pouvoir protéger la confidentialité des informations portant sur des intérêts légitimes, mais d'une manière mieux balisée.

Dans l'optique de préciser les restrictions applicables, la Commission recommande d'améliorer la rédaction des dispositions qui les prévoient, notamment :

- en évitant le recours à des termes très généraux invitant à une application large, englobante et subjective des restrictions. Par exemple, il faut éviter l'usage de termes comme « avis », « recommandations », « analyses » ou « renseignements obtenus d'un gouvernement autre que celui du Québec » et sélectionner des termes plus précis;
- en s'assurant que les dispositions qui relèvent de la discrétion d'une personne autre que le responsable de l'accès¹⁵⁴ prévoient également l'obligation de justifier ce refus;
- en précisant les conditions d'application des restrictions et les situations dans lesquelles elles ne peuvent être invoquées¹⁵⁵.

Par rapport aux dispositions protégeant des renseignements de même nature¹⁵⁶, la Commission estime qu'il serait préférable de les regrouper pour en réduire le nombre. Ce regroupement par thématique devrait permettre de mettre en évidence les intérêts légitimes à protéger par les restrictions. La section 1.2.1.5 donne des exemples concrets de pistes de solution à explorer, retenues à ce sujet par d'autres juridictions.

¹⁵⁴ Loi sur l'accès, art. 33-34.

¹⁵⁵ Voir le Rapport quinquennal 2016, p. 22.

¹⁵⁶ Par exemple, voir la Loi sur l'accès, art. 23 et 24 ou 37 et 38.



En ce sens, la portée des restrictions au droit d'accès devrait permettre de bien distinguer l'intérêt privé¹⁵⁷ de l'intérêt public¹⁵⁸ à protéger par une restriction¹⁵⁹. Cette approche permettrait, selon la Commission, d'améliorer la confiance des citoyens quant au fait qu'un refus d'accès par un organisme public est bien fondé sur la Loi et justifié par un réel intérêt légitime, et ne découle pas d'une simple possibilité de ne pas divulguer l'information.

La Commission soutient qu'il faudrait également revoir la durée d'application des restrictions de manière, notamment, à fixer une limite temporelle maximale pour certaines¹⁶⁰, ou réduire la durée pour d'autres. Dans un contexte où l'actualité est en mouvance constante, les citoyens s'attendent à une plus grande transparence de la part des organismes publics, mais également à un accès à l'information rapide et efficace. De l'avis de la Commission, la réalité d'aujourd'hui ne justifie plus l'application de restriction au droit d'accès pour une durée illimitée ou aussi longue que celle parfois prévue dans les dispositions actuelles. À cet égard, la réflexion devrait donc valoriser une divulgation maximale des informations en ne protégeant les intérêts légitimes que pour la durée nécessaire.

Recommandation 4

Revoir l'ensemble des restrictions au droit d'accès pour en préciser la portée et en circonscrire l'utilisation, entre autres en :

- utilisant des termes moins subjectifs et englobants;
- s'assurant que les refus qui relèvent de la discrétion d'une personne autre que le responsable de l'accès de l'organisme public doivent eux aussi être motivés;
- prévoyant pour chaque restriction des conditions d'application et, le cas échéant, des situations où elles ne peuvent être invoquées;
- réunissant les restrictions visant à protéger les mêmes intérêts légitimes;
- revoyant la durée d'application des restrictions de manière à la réduire, lorsqu'elle est déjà prévue, ou à la limiter pour éviter l'application permanente de certaines restrictions.

1.2.1.4.2. Étendre à toutes les restrictions l'obligation de démontrer que la divulgation d'un document risque d'entraîner un préjudice

Le régime de restrictions ne devrait pas permettre de refuser l'accès à un document simplement parce qu'il est possible de le faire. La restriction au droit d'accès, qu'elle soit de nature obligatoire ou facultative, devrait être une mesure d'exception.

Pour favoriser l'accès aux documents, la Commission estime donc toujours essentiel que les responsables de l'accès soient tenus de procéder à une évaluation des risques relatifs à une éventuelle divulgation afin d'ajuster leur décision en fonction des particularités du contexte.

¹⁵⁷ Comme la protection de la vie privée d'un tiers ou les intérêts économiques d'une entreprise.

¹⁵⁸ Comme la sécurité publique, le processus de délibération, les privilèges parlementaires ou les relations internationales.

¹⁵⁹ Rapport quinquennal 2016, p. 22.

¹⁶⁰ Par exemple : Loi sur l'accès, art. 18, 23, 34 et 38.



Dans son rapport quinquennal de 2016, la Commission préconisait l'introduction d'un test comportant certains critères afin d'évaluer si la divulgation d'un renseignement ou d'un document donné était susceptible de causer un préjudice réel, et ce, en s'appuyant sur les normes internationales reconnues en matière d'accès aux documents¹⁶¹ :

Selon ces normes, une exception au droit d'accès doit :

- *viser à protéger un intérêt légitime et circonscrit;*
- *ne s'appliquer qu'à l'information dont la divulgation est susceptible de causer un préjudice à ces intérêts;*
- *pouvoir être écartée lorsque la divulgation du renseignement est davantage dans l'intérêt public que le degré de préjudice susceptible d'en découler.*

Cette évaluation des risques devrait ensuite être expliquée et motivée dans la décision du responsable de l'accès aux documents¹⁶². Cet exercice permettrait de s'assurer que les décisions du responsable de l'accès aux documents ne visent qu'à protéger des intérêts légitimes.

Si la Loi sur l'accès prévoyait cette obligation pour l'application de l'ensemble des restrictions, la Commission pourrait se pencher sur l'adéquation de l'évaluation du préjudice dans le cadre de toute demande de révision impliquant l'application d'une telle restriction. Ainsi, sa capacité d'intervention serait renforcée, alors qu'elle est actuellement parfois limitée à constater que les organismes publics étaient en droit d'invoquer une restriction puisque les critères prévus étaient satisfaits, et ce, même en l'absence de démonstration de préjudice.

Recommandation 5

Modifier la Loi sur l'accès de manière à étendre l'obligation de démontrer l'existence d'un préjudice à des intérêts légitimes afin qu'elle concerne l'ensemble des restrictions, qu'elles soient de nature facultative ou obligatoire.

1.2.1.4.3. Réviser et limiter les motifs de refus obligatoires

La Commission estime que les restrictions facultatives constituent déjà des exceptions importantes au droit d'accès des citoyens. En ce sens, une restriction obligatoire devrait être une ultime exception, ne devant subsister que pour protéger les intérêts légitimes qui exigent une confidentialité quasi totale en toutes circonstances.

En ce sens, la Commission recommande un assouplissement des restrictions obligatoires prévues à la Loi sur l'accès afin de permettre aux responsables de l'accès des organismes publics d'effectuer une évaluation contextualisée des demandes, favorisant ainsi une plus grande transparence. Les responsables de l'accès devraient donc être autorisés à communiquer des documents relatifs à la sécurité publique ou à l'administration de la justice lorsque leur divulgation ne compromet pas la protection de ces intérêts

¹⁶¹ Rapport quinquennal 2016, p. 22; la Commission cite notamment : COMMISSAIRE À L'INFORMATION DU CANADA, préc., note 62.

¹⁶² À cet égard, voir : COMMISSION D'ACCÈS À L'INFORMATION, préc., note 152, p. 20.



légitimes¹⁶³. Une solution possible serait de rendre ces restrictions facultatives et sujettes au test de préjudice évoqué à la section 1.2.1.4.2.

Recommandation 6

Limiter le nombre de restrictions obligatoires au droit d'accès et les réserver aux seules situations visant à protéger un intérêt qui requiert une confidentialité quasi totale, en toutes circonstances.

1.2.1.4.4. Affirmer la primauté de l'intérêt public en matière d'accès à l'information

Pour que l'exercice de modernisation des règles relatives aux restrictions au droit d'accès soit complet, la Commission estime qu'il faut reconnaître que l'intérêt public doit, dans certaines circonstances, primer et justifier la levée de toute restriction, même obligatoire.

Soulignons que l'inclusion d'une disposition affirmant la primauté de l'intérêt public est reconnue comme étant incontournable dans un régime d'accès à l'information moderne¹⁶⁴.

D'ailleurs, plusieurs lois tant canadiennes¹⁶⁵ qu'étrangères¹⁶⁶ prévoient une disposition générale permettant de mettre en balance l'intérêt public et les intérêts légitimes protégés par les restrictions au droit d'accès. Ces dispositions permettent entre autres de divulguer des renseignements faisant connaître des violations contre les droits de la personne, des situations de corruption ou d'abus de pouvoir ou l'usage indu de fonds publics.

Il importe de préciser que la reconnaissance de l'intérêt public comme ultime critère en matière d'accès à l'information n'entraîne pas automatiquement la divulgation de renseignements qu'un organisme public considère comme confidentiels. En effet, il faut garder à l'esprit que les restrictions au droit d'accès

¹⁶³ Par exemple, lorsqu'un document susceptible d'être visé par une telle restriction a déjà fait l'objet d'une circulation publique, notamment par son dépôt dans un dossier devant le tribunal, il ne devrait pas être possible d'en refuser l'accès. Dans une affaire récente, la Cour du Québec a établi que l'état actuel du droit ne permettait pas, même dans un tel cas, d'écarter les restrictions obligatoires. Voir *École nationale de police du Québec c. Popovic*, 2025 QCCQ 4948, par. 21 à 44, en ligne : <<https://canlii.ca/t/kfr0l>>.

¹⁶⁴ ORGANISATION DES ÉTATS AMÉRICAINS, préc., note 68, p. 26 et 36; CENTRE FOR LAW AND DEMOCRACY et ACCESS INFO EUROPE, « Indicator 31 - Public Interest », *RTI Rating*, en ligne : <<https://www.rti-rating.org/country-data/by-indicator/31/>> (consulté le 12 novembre 2025).

¹⁶⁵ FIPPA de la Colombie-Britannique, art. 25; *Access to Information and Protection of Privacy Act [Terre-Neuve-et-Labrador]*, préc., note 64, art. 9; *Loi sur l'accès à l'information municipale et la protection de la vie privée [Ontario]*, préc., note 133, art. 23 (l'article 23 de la loi consacre le principe de la primauté des raisons d'intérêt public, mais celui-ci ne s'applique pas aux documents à l'égard desquels certains motifs de restriction sont invoqués, notamment le secret professionnel de l'avocat et le privilège rattaché aux écrits concernant l'exécution de la loi); *Access to Information Act [Alberta]*, SA 2024, c. A-1.4, p. 37, en ligne : <https://kings-printer.alberta.ca/1266.cfm?page=a01p4.cfm&leg_type=Acts&isbncIn=9780779851331&display=html>; *Loi sur l'accès à l'information et la protection de la vie privée [Manitoba]*, C.C.S.M., c. F175, p. 18(4), en ligne : <<https://web2.gov.mb.ca/laws/statutes/ccsm/f175.php>> (la disposition concernant l'intérêt public ne vise que les renseignements fournis par des tiers).

¹⁶⁶ *Act relating to the right of access to documents held by public authorities and public undertakings (Freedom of Information Act) [Norvège]*, 2006, art. 11, en ligne : <<https://lovdata.no/dokument/NLE/lov/2006-05-19-16>>; *Law on Free Access to Information of Public Importance [Serbie]*, (2003), 120104, art. 4, en ligne : <<https://www.rti-rating.org/wp-content/uploads/Serbia.pdf>>; *Right of Access to Information Act [Croatie]*, 172/2003, p. 16.2, en ligne : <<https://www.rti-rating.org/wp-content/uploads/Croatia.pdf>>; *Law on Freedom of Access to Information for Bosnia and Herzegovina [Bosnie-Herzégovine]*, 2000, art. 5, en ligne : <<https://www.rti-rating.org/wp-content/uploads/Bosnia-and-Herzegovina.pdf>>.



prévues dans la Loi sont justifiées par la protection de certains intérêts légitimes, comme la sécurité publique, l'administration de la justice ou les relations internationales. Une disposition relative à l'intérêt public permet plutôt d'assurer un équilibre entre, d'une part, la recherche d'une plus grande transparence des organismes publics et, d'autre part, le besoin d'assurer la confidentialité de certaines informations stratégiques ou sensibles qu'ils détiennent¹⁶⁷. Il s'agit alors d'un mécanisme offrant la souplesse nécessaire pour répondre aux situations que le législateur n'a pas pu anticiper. En somme, l'ajout d'un critère d'intérêt public permet d'assurer l'atteinte des objectifs d'une loi en matière d'accès à l'information dans certaines situations particulières.

Parmi les nombreux exemples de libellés intéressants qui font valoir la primauté de l'intérêt public, la Commission soumet les exemples de l'Ontario, de l'Alberta et de la Colombie-Britannique, exposés dans la section 1.2.1.5.2.

Une disposition relative à la primauté de l'intérêt public en matière d'accès à l'information pourrait contenir certaines balises ou certains facteurs à considérer : les objectifs du gouvernement ouvert, les effets sur l'environnement, la santé ou la sécurité publique ou le fait que les renseignements révèlent des abus de droit à l'encontre d'une personne ou permettraient de protéger le droit à la vie, à la liberté et à la sécurité d'une personne¹⁶⁸.

Pour la Commission, l'inclusion d'une telle disposition dans la Loi sur l'accès serait non seulement un rappel des principes essentiels soutenant cette loi, mais également un moyen de les atteindre. En ce sens, elle permettrait d'établir l'équilibre entre les différents intérêts qui sont en cause en matière d'accès à l'information. Comme pour la recommandation formulée précédemment concernant le test de préjudice, elle encadrerait l'exercice du pouvoir discrétionnaire des responsables de l'accès des organismes publics en leur demandant de vérifier que l'intérêt légitime à protéger est plus important que l'intérêt du public à accéder à l'information. Leurs décisions seraient ainsi mieux motivées, et la Commission pourrait apprécier la pondération des intérêts dans le cadre d'une demande de révision.

¹⁶⁷ Rapport quinquennal 2016, p. 27.

¹⁶⁸ COMMISSAIRE À L'INFORMATION DU CANADA, préc., note 62, p. 40.



Recommandation 7

Introduire à la Loi sur l'accès une disposition d'application générale établissant la primauté de l'intérêt public sur l'ensemble des restrictions au droit d'accès, laquelle :

- oblige un organisme public à donner accès à un renseignement lorsque l'intérêt public l'emporte clairement sur le préjudice potentiel lié à sa divulgation;
- contient une liste non exhaustive de facteurs à considérer dans l'évaluation de l'intérêt public.

1.2.1.4.5. Réviser l'article 87 de la Loi sur l'accès

La Commission estime, avec déférence, que l'interprétation de la Cour supérieure dans l'affaire *Ville de St-Jean-sur-Richelieu (Service de police) c. Cour du Québec*¹⁶⁹ doit mener à des modifications législatives pour maintenir la portée du droit d'accès aux renseignements personnels.

Il est à noter que l'interprétation mise de l'avant dans ce jugement de la Cour supérieure fait l'objet de certaines dissidences doctrinales¹⁷⁰ :

« Avec grand respect, nous ne pouvons partager l'opinion du juge [...] et nous nous rallions plutôt à la jurisprudence majoritaire quant à l'interprétation des articles 28 et 87 de la Loi sur l'accès.

Rappelons-nous que lorsqu'une demande d'accès est déposée par une personne qui veut obtenir communication de renseignement la concernant, c'est l'article 83 qui s'applique [...]. Le responsable de l'accès peut alors invoquer les restrictions prévues aux articles 86 à 94. L'article 87 lui permet également d'invoquer les articles 18 à 41.3. C'est donc par le jeu de l'article 87 que le responsable peut invoquer l'article 28. [...]

À notre avis, la Cour supérieure a mis trop d'emphase sur les termes « doit refuser » au début de l'article 28 et a omis de considérer le fait que l'article 87 débute quant à lui par « peut refuser ». Reprenons la lecture de l'article 87 en commençant par la deuxième partie afin de mieux en comprendre la portée : « dans la mesure où la communication de cette information (le renseignement personnel) révélerait un renseignement dont la communication **doit ou peut être refusée** en vertu de la section II du chapitre II », « un organisme public **peut refuser de confirmer l'existence ou de donner communication à une personne d'un renseignement personnel la concernant** ». Il apparaît alors clairement que l'organisme a le pouvoir discrétionnaire, et non l'obligation, d'invoquer quelque restriction prévue à la section II du chapitre II. [...]

À l'instar de la jurisprudence majoritaire et de la Cour du Québec, nous sommes d'avis que non seulement le texte de l'article 87, mais la structure même de la Loi sur l'accès confirme que

¹⁶⁹ *Ville de St-Jean-sur-Richelieu (Service de police) c. Cour du Québec*, préc., note 119.

¹⁷⁰ Caroline BEAULNE, « Fin de la valse-hésitation : L'article 28 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels est une disposition impérative peu importe la nature des renseignements demandés », *Wolters Kluwer* (13 janvier 2025), en ligne : <<https://www.wolterskluwer.com/fr-ca/expert-insights/fin-de-la-valse-hesitation>> (consulté le 20 mars 2026); les caractères gras et italiques sont initialement présents; nous soulignons.

l'article 28 perd son caractère impératif dans les cas où la demande d'accès est déposée en vertu de l'article 83 et qu'il doit ainsi être invoqué dans les délais prévus à l'article 98.

Dans son analyse, la Cour supérieure s'attarde également aux conséquences absurdes que pourrait entraîner cette double interprétation selon le type de demande d'accès. Elle se rallie ainsi à l'argumentaire du service de police qui soumet que cela pourrait avoir comme effet de permettre à un membre du crime organisé d'avoir accès à des renseignements le concernant tels des confirmations d'enquête, des rapports de filatures ou des confirmations de mise sous écoute, dans le cas où un responsable de l'accès omettrait, sans motifs raisonnables, d'invoquer l'article 28.

Avec égard pour l'opinion contraire, nous nous permettons ces quelques commentaires. Bien que l'objectif de l'article 28 soit de protéger la confidentialité des renseignements qui ont notamment des incidences sur l'administration de la justice ou la sécurité de l'État, la Loi sur l'accès a un caractère quasi constitutionnel et son objectif premier est de favoriser la démocratie et la communication des renseignements détenus par le gouvernement. Il est effectivement peu souhaitable que ce type de renseignements puissent être dévoilés. Par contre, dans une société libre et démocratique comme la nôtre, certains droits ont un statut fondamental, sinon quasi constitutionnel. Le droit d'un justiciable d'avoir accès à des renseignements le concernant ne saurait être tributaire de la compétence d'un responsable de l'accès et encore moins de son incompréhension de la Loi. Nous ne pouvons donc nous rallier aux propos du juge [...] qui semblent avaliser le fait que les responsables de l'accès ne sont habituellement pas juristes et qu'ils peuvent ainsi commettre des erreurs de bonne foi, notamment en raison de leur mauvaise compréhension de la Loi. Tel que le veut l'adage, nul n'est censé ignorer la Loi, *a fortiori* une personne chargée de son application.

Enfin, la restriction prévue à l'article 88 de la Loi sur l'accès, laquelle est impérative, pourrait possiblement être invoquée à tout moment pour limiter, sinon empêcher, la communication de certains extraits et ainsi pallier l'omission d'avoir invoqué l'article 28 dans les délais. »

L'interprétation antérieure de l'article 87 de la Loi sur l'accès devrait y être codifiée afin de permettre une clarification du droit applicable, d'une manière d'ailleurs compatible avec l'esprit de ce que recommandait la Commission Paré dès 1981¹⁷¹.

Si, dans le cadre d'une révision de l'ensemble des restrictions au droit d'accès comme celle recommandée aux sections 1.2.1.4.1 et 1.2.1.4.3, une ou plusieurs restrictions obligatoires demeurent, celles-ci devraient donc être facultatives lorsqu'elles concernent une demande d'une personne d'accéder à ses propres renseignements.

¹⁷¹ « Comme pour l'accès aux documents administratifs, le principe de l'accès d'un individu à son dossier personnel doit souffrir d'un certain nombre d'exceptions. [...] Les restrictions doivent s'appliquer à des types de renseignements lorsque la sécurité d'une personne, la sécurité publique, la prévention et la lutte contre les activités criminelles sont en jeu. Elles doivent être de nature facultative, c'est-à-dire que l'Administration doit pouvoir refuser l'accès d'un individu à un renseignement le concernant, mais ne pas y être tenue. » COMMISSION D'ÉTUDE SUR L'ACCÈS DU CITOYEN À L'INFORMATION GOUVERNEMENTALE ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, préc., note 1, p. 74.



Recommandation 8

Modifier le libellé de l'article 87 de la Loi sur l'accès afin de codifier clairement que les restrictions obligatoires au droit d'accès aux documents deviennent facultatives lorsqu'une personne demande l'accès à ses renseignements personnels.

1.2.1.5. Pour aller plus loin

Pour illustrer certains de ses propos, la Commission présente dans cette section des exemples concrets de dispositions de la Loi sur l'accès dont la rédaction devrait, selon elle, être révisée. Elle évoque aussi des dispositions dans des lois canadiennes qui peuvent servir d'inspiration pour la codification de la primauté de l'intérêt public. Enfin, un tableau de toutes les restrictions actuelles est présenté à titre de référence.

1.2.1.5.1. Des exemples de restrictions qui devraient être révisées

Selon la Commission, les exemples suivants montrent certaines imprécisions ou redondances dans les restrictions actuellement prévues à la Loi sur l'accès.

1.2.1.5.1.1. Les restrictions protégeant les affaires intergouvernementales

Les articles 18 et 19 de la Loi sur l'accès stipulent ce qui suit :

18. Le gouvernement ou un ministère peut refuser de communiquer un renseignement obtenu d'un gouvernement autre que celui du Québec, d'un organisme d'un tel gouvernement ou d'une organisation internationale.

Il en est de même du lieutenant-gouverneur, du Conseil exécutif et du Conseil du trésor.

19. Un organisme public peut refuser de communiquer un renseignement lorsque sa divulgation porterait vraisemblablement préjudice à la conduite des relations entre le gouvernement du Québec et un autre gouvernement ou une organisation internationale.

Ces deux dispositions visent à protéger des intérêts qui, pour un néophyte, peuvent à première vue paraître similaires. Cette personne pourrait avoir du mal à identifier la disposition qui s'applique à sa situation et les différences entre les renseignements protégés par chacune d'entre elles, alors que leur objectif commun est la protection des renseignements ayant une incidence sur les relations intergouvernementales. Il semblerait profitable, dans une visée de simplification, de les réunir en un seul article bonifié.

De plus, la restriction prévue par l'article 18 de la Loi sur l'accès est imprécise et a une portée trop large. En effet, elle s'applique peu importe la nature du document et ne nécessite pas la démonstration d'un préjudice relatif à la divulgation du document, comme l'a déjà souligné la Commission¹⁷² :

[24] L'application de cette restriction ne dépend pas de la nature du renseignement lui-même, ni même sur les effets de sa divulgation, mais plutôt de son origine.

¹⁷² *Lincourt c. Ministère de l'Enseignement supérieur*, 2023 QCCA 68, en ligne : <<https://canlii.ca/t/jx2xf>>.



[25] Le rôle de la Commission se limite ainsi à vérifier l'origine de ces renseignements, étant donné que cette disposition confère une entière discrétion à un organisme public de donner ou de refuser l'accès aux renseignements qu'il a obtenus d'un autre gouvernement.

Par exemple, un organisme public pourrait invoquer cette restriction pour refuser l'accès à un simple communiqué de presse d'un organisme public fédéral ou encore d'une organisation internationale.

1.2.1.5.1.2. Les restrictions protégeant les processus décisionnels

Un second exemple est celui des articles 37 et 38 de la Loi sur l'accès, qui stipulent :

37. Un organisme public peut refuser de communiquer un avis ou une recommandation faite depuis moins de dix ans, par un de ses membres, un membre de son personnel, un membre d'un autre organisme public ou un membre du personnel de cet autre organisme, dans l'exercice de leurs fonctions.

Il peut également refuser de communiquer un avis ou une recommandation qui lui ont été faits, à sa demande, depuis moins de dix ans, par un consultant ou par un conseiller sur une matière de sa compétence.

38. Un organisme public peut refuser de communiquer un avis ou une recommandation que lui a fait un organisme qui en relève ou qu'il a fait à un autre organisme public, jusqu'à ce que la décision finale sur la matière faisant l'objet de l'avis ou de la recommandation ait été rendue publique par l'autorité compétente.

Il en est de même pour un ministre en ce qui concerne un avis ou une recommandation que lui a fait un organisme qui relève de son autorité.

Premièrement, les articles 37 et 38 de la Loi sur l'accès visent à protéger le processus décisionnel des organismes publics. Ils pourraient être regroupés en un seul article visant cet intérêt légitime¹⁷³.

Deuxièmement, la portée de l'article 37 de la Loi sur l'accès est large, puisqu'il s'applique à tous les « avis » et à toutes les « recommandations », des termes très englobants.

Troisièmement, la Commission estime que le délai d'inaccessibilité de 10 ans, prévu au deuxième alinéa de cet article, n'est pas justifié pour protéger l'intérêt légitime visé. L'article 37 a pour objectif de protéger le processus décisionnel d'un organisme public de deux façons :

- Permettre aux conseillers des organismes publics d'exprimer leur point de vue sans retenue.
- S'assurer que les dirigeants ne s'abstiennent pas de demander des avis qui explorent toutes les possibilités, y compris celles qui sont contraires aux politiques officielles¹⁷⁴.

La Commission reconnaît l'importance de ces objectifs. Elle estime toutefois que cette disposition justifie l'introduction d'une évaluation du risque de préjudice découlant de la divulgation d'un document ou l'ajout d'exclusions à l'application de cette restriction. En effet, limiter l'application de cette restriction à la nature d'un document ne permet pas de favoriser la transparence des organismes publics. De plus, une fois la décision rendue, il n'est plus nécessaire de protéger le processus décisionnel. Dans une ère où l'absence d'information officielle laisse place à la spéculation, voire à la désinformation¹⁷⁵, les citoyens devraient être

¹⁷³ Une autre disposition vise des documents de cette nature : Loi sur l'accès, art. 27 al. 2.

¹⁷⁴ Voir le Rapport quinquennal 2016, p. 23.

¹⁷⁵ Voir la récente résolution commune de la Commission et de ses homologues canadiens à cet égard : COMMISSAIRES ET OMBUDS FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX RESPONSABLES DE L'ACCÈS À L'INFORMATION, préc., note 14.



en mesure d'accéder immédiatement après la prise d'une décision aux justifications ainsi qu'aux différentes considérations relatives à celle-ci.

À titre d'exemple, la législation de l'Ontario prévoit des exceptions permettant de limiter l'application d'une restriction analogue, reproduite ci-après¹⁷⁶.

« Conseils au gouvernement

13 (1) La personne responsable peut refuser de divulguer un document qui aurait pour effet de révéler les conseils ou les recommandations émanant d'un fonctionnaire, d'une personne employée par une institution ou d'un expert-conseil dont les services ont été retenus par cette institution.

Exceptions

(2) Malgré le paragraphe (1), la personne responsable ne doit pas refuser, en vertu de ce paragraphe, de divulguer un document qui comporte l'un des éléments suivants :

- a) de la documentation portant sur des faits;
- b) un sondage statistique;
- c) le rapport d'un estimateur, que ce dernier soit ou non un dirigeant de l'institution;
- d) un rapport sur d'éventuelles répercussions sur l'environnement ou un document semblable;
- e) le rapport qui porte sur l'essai d'un produit relié à la mise à l'épreuve de pièces d'équipement appartenant au gouvernement ou le résultat d'un test mené à l'intention des consommateurs;
- f) le rapport ou le résultat d'une étude relative au rendement ou à l'efficacité d'une institution, que ce rapport ou cette étude soient d'ordre général ou portent sur un programme ou une politique en particulier;
- g) une étude de faisabilité ou autre étude technique, y compris une estimation des coûts, reliée à une politique ou à un projet gouvernemental;
- h) le rapport qui comporte les résultats d'une recherche effectuée sur le terrain préalablement à la formulation d'une politique proposée;
- i) la proposition ou le plan définitifs en vue de la modification d'un programme existant ou de l'établissement d'un nouveau programme d'une institution, y compris son estimation budgétaire, que cette proposition ou ce plan soient subordonnés ou non à une approbation quelconque, sauf s'ils doivent être présentés au Conseil exécutif ou à ses comités;
- j) le rapport du groupe de travail d'un comité interministériel ou d'une entité semblable ou celui d'un comité ou d'un groupe de travail internes d'une institution chargés de dresser un rapport sur une question précise, sauf si ce rapport doit être présenté au Conseil exécutif ou à ses comités;
- k) le rapport d'un comité, d'un conseil ou d'une autre entité liés à une institution et constitués dans le but de mener des enquêtes suivies de rapports ou de recommandations destinés à cette institution;
- l) les motifs à l'appui de la décision, de l'arrêté, de l'ordonnance, de l'ordre ou de la directive définitifs du dirigeant d'une institution et rendus à la fin ou au cours de l'exercice d'un

¹⁷⁶ *Loi sur l'accès à l'information et la protection de la vie privée [Ontario]*, L.R.O. 1990, c. F-31, art. 13, en ligne : <https://www.ontario.ca/fr/lois/loi/90f31>.



pouvoir discrétionnaire conféré par un texte législatif ou un projet mis en application par cette institution, ou en vertu de ceux-ci, qu'il soit permis ou non aux termes du texte législatif ou du projet d'interjeter appel de ces décisions, arrêtés, ordonnances, ordres ou directives. Ce qui précède s'applique, que ces motifs :

- (i) figurent ou non dans une note de service qui émane de l'institution ou dans la lettre d'un dirigeant ou d'un employé de cette institution, destinée à une personne donnée,
- (ii) aient été ou non exposés par le dirigeant qui a rendu cette décision ou directive ou cet ordre que ces motifs y soient incorporés par renvoi ou non.

Idem

(3) Malgré le paragraphe (1), la personne responsable ne doit pas refuser, en vertu de ce paragraphe, de divulguer un document si le document date de plus de vingt ans ou si la personne responsable l'a publiquement mentionné comme ayant servi de fondement à une décision ou à la formulation d'une politique. »

1.2.1.5.1.3. Les documents du cabinet

Un troisième exemple est celui de l'article 34 de la Loi sur l'accès, qui mériterait aussi, selon la Commission, d'être reformulé. Cette disposition se lit comme suit :

34. Un document du bureau d'un membre de l'Assemblée nationale ou un document produit pour le compte de ce membre par les services de l'Assemblée n'est pas accessible à moins que le membre ne le juge opportun.

Il en est de même d'un document du cabinet du président de l'Assemblée, d'un membre de celle-ci visé dans le premier alinéa de l'article 124.1 de la Loi sur l'Assemblée nationale (chapitre A-23.1) ou d'un ministre visé dans l'article 11.5 de la Loi sur l'exécutif (chapitre E-18), ainsi que d'un document du cabinet ou du bureau d'un membre d'un organisme municipal ou scolaire.

Cette restriction, en raison de son imprécision, est susceptible de donner lieu à une application arbitraire. En effet, elle ne comporte aucune évaluation du préjudice pouvant découler de la divulgation du document et relève entièrement de la discrétion d'une personne autre que le responsable de l'accès aux documents de l'organisme concerné. Elle ne présente par ailleurs aucune limite de temps pour son application.

Pour circonscrire cette restriction, le législateur québécois pourrait notamment s'inspirer de la loi britanno-colombienne. Celle-ci regroupe en une seule disposition des restrictions protégeant les mêmes intérêts que ceux de divers articles de la Loi sur l'accès, dont l'article 34¹⁷⁷. Cette disposition est cependant plus précise, et sa durée d'application est limitée dans le temps¹⁷⁸ :

« Cabinet and local public body confidences

12 (1) The head of a public body must refuse to disclose to an applicant information that would reveal the substance of deliberations of the Executive Council or any of its committees, including any advice, recommendations, policy considerations or draft legislation or regulations submitted or prepared for submission to the Executive Council or any of its committees.

(2) Subsection (1) does not apply to

¹⁷⁷ Les autres dispositions concernées sont les articles 30, 30.1, 33 et 36 de la Loi sur l'accès.

¹⁷⁸ FIPPA de la Colombie-Britannique, art. 12.



- (a) information in a record that has been in existence for 15 or more years,
 - (b) information in a record of a decision made by the Executive Council or any of its committees on an appeal under an Act, or
 - (c) information in a record the purpose of which is to present background explanations or analysis to the Executive Council or any of its committees for its consideration in making a decision if
 - (i) the decision has been made public,
 - (ii) the decision has been implemented, or
 - (iii) 5 or more years have passed since the decision was made or considered.
- (3)** The head of a local public body may refuse to disclose to an applicant information that would reveal
- (a) a draft of a resolution, bylaw or other legal instrument by which the local public body acts or a draft of a private Bill, or
 - (b) the substance of deliberations of a meeting of its elected officials or of its governing body or a committee of its governing body, if an Act or a regulation under this Act authorizes the holding of that meeting in the absence of the public.
- (4)** Subsection (3) does not apply if
- (a) the draft of the resolution, bylaw, other legal instrument or private Bill or the subject matter of the deliberations has been considered in a meeting open to the public, or
 - (b) the information referred to in that subsection is in a record that has been in existence for 15 or more years.
- (5)** The Lieutenant Governor in Council by regulation may designate a committee for the purposes of this section.
- (6)** A committee may be designated under subsection (5) only if
- (a) the Lieutenant Governor in Council considers that
 - (i) the deliberations of the committee relate to the deliberations of the Executive Council, and
 - (ii) the committee exercises functions of the Executive Council, and
 - (b) at least 1/3 of the members of the committee are members of the Executive Council.
- (7)** In subsections (1) and (2), "committee" includes a committee designated under subsection (5). »

1.2.1.5.2. Des dispositions intéressantes en matière d'intérêt public

D'autres lois prévoient des dispositions plus robustes concernant la primauté de l'intérêt public, lesquelles pourraient servir d'inspiration en vue d'un tel ajout dans la Loi sur l'accès.

Ainsi, la loi ontarienne prévoit une obligation de diffusion de l'information dans l'intérêt public, et ce, dans les meilleurs délais¹⁷⁹.

¹⁷⁹ Loi sur l'accès à l'information et la protection de la vie privée [Ontario], préc., note 176, art. 11.



« Obligation de divulguer un document

11 (1) Malgré toute autre disposition de la présente loi, la personne responsable qui a des motifs raisonnables et probables de croire qu'il y va de l'intérêt public, divulgue au public ou aux personnes intéressées dans les meilleurs délais, compte tenu des circonstances, le document révélateur d'un grave danger pour la santé ou la sécurité du public ou pour l'environnement.

Avis

(2) La personne responsable fait aviser dans la mesure du possible toutes les personnes concernées par les renseignements que contient le document visé au paragraphe (1) avant d'en divulguer la teneur.

Teneur de l'avis

(3) L'avis comporte :

- a) une déclaration portant que la personne responsable a l'intention de communiquer la totalité ou une partie d'un document et que cette divulgation peut avoir une incidence sur les intérêts de la personne;
- b) une description de la teneur du document ou de la partie du document qui concerne cette personne;
- c) une déclaration portant que la personne responsable tiendra compte des observations que lui présentera sans délai cette personne, si cette dernière expose les motifs pour lesquels le document ne devrait pas être divulgué, même en partie.

Observations

(4) La personne qui reçoit l'avis visé au paragraphe (2) peut présenter sans délai à la personne responsable ses observations exposant les motifs pour lesquels ce document ne devrait pas être divulgué, même en partie. »

Les lois de l'Alberta¹⁸⁰ et de la Colombie-Britannique¹⁸¹ prévoient elles aussi une obligation semblable, en utilisant presque le même libellé. La disposition albertaine est reproduite ci-après.

¹⁸⁰ Access to Information Act [Alberta], préc., note 165, art. 37.

¹⁸¹ FIPPA de la Colombie-Britannique, art. 25.

**« Information must be disclosed if in the public interest**

37(1) Whether or not a request for access is made, the head of a public body must, without delay, disclose to the public, to an affected group of people, to any person or to an applicant

- (a) information about a risk of significant harm to the environment or to the health or safety of the public, of the affected group of people, of the person or of the applicant, or
- (b) information the disclosure of which is, for any other reason, clearly in the public interest.

(2) Subsection (1) applies despite any other provision of this Act.

(3) Before disclosing information under subsection (1), the head of a public body must, where practicable,

- (a) notify any third party to whom the information relates,
- (b) give the third party an opportunity to make representations relating to the disclosure, and
- (c) notify the Commissioner.

(4) If it is not practicable to comply with subsection (3), the head of the public body must give written notice of the disclosure to

- (a) the third party, and
- (b) the Commissioner. »

1.2.1.5.3. Le portrait des restrictions actuelles

Les tableaux suivants présentent les restrictions au droit d'accès actuellement prévues par la Loi sur l'accès en précisant si elles sont obligatoires ou facultatives. Les restrictions exigeant la démonstration d'un préjudice figurent dans un premier tableau, suivi de celles qui ne reposent que sur la nature des documents visés.

Restrictions à l'accès exigeant la démonstration d'un préjudice par l'organisme public

Restriction	Nature	Préjudice
Conduite des relations avec un autre gouvernement ou une organisation internationale (art. 19)	Facultative	Préjudice à la conduite des relations
Négociation en cours avec un autre organisme public (art. 20)	Facultative	Entrave à la négociation
Emprunt, projet d'emprunt, transaction ou projet de transaction, projet de tarification, projet d'imposition ou de modification d'une taxe ou d'une redevance (art. 21)	Facultative	- Avantage indu à une personne, préjudice sérieux à une personne - Atteinte sérieuse aux intérêts économiques de l'organisme public ou de la collectivité



Restriction	Nature	Préjudice
Renseignement industriel, financier, commercial, scientifique ou technique (art. 22)	Facultative	- Entrave à une négociation en vue de la conclusion d'un contrat, perte à l'organisme - Avantage appréciable à une autre personne - Risque de nuire de façon substantielle à la compétitivité ou de révéler un projet ou une stratégie de diverses natures
Renseignement d'un tiers (art. 24)	Obligatoire	- Entrave à la négociation en vue de la conclusion d'un contrat - Perte à un tiers, avantage appréciable à une autre personne - Nuisance substantielle à la compétitivité du tiers
Tout renseignement (art. 27 al. 1)	Facultative	Révélation d'un mandat ou d'une stratégie de négociation de convention collective ou de contrat
Renseignement détenu dans l'exercice d'une fonction de prévention, de détection ou de répression du crime ou des infractions aux lois (art. 28)	Obligatoire	- Entrave au déroulement d'une procédure devant une personne ou un organisme exerçant des fonctions juridictionnelles - Entrave au déroulement d'une enquête - Révélation d'une méthode d'enquête, d'une source confidentielle d'information, d'un programme ou d'un plan d'action destiné à prévenir, détecter ou réprimer le crime ou les infractions aux lois - Mise en péril de la sécurité d'une personne - Préjudice à une personne qui est l'auteur du renseignement ou qui en est l'objet - Révélation des composantes d'un système de communication destiné à l'usage d'une personne chargée d'assurer l'observation de la loi - Révélation d'un renseignement transmis à titre confidentiel par un corps de police ayant compétence hors du Québec - Favorisation de l'évasion d'un détenu - Atteinte au droit d'une personne à une audition impartiale de sa cause
Tout renseignement (art. 28.1)	Obligatoire	Dont la divulgation aurait pour effet de porter atteinte à la sécurité de l'État
Tout renseignement (art. 29 al. 2)	Obligatoire	Dont la divulgation aurait pour effet de réduire l'efficacité d'un programme, d'un plan d'action ou d'un dispositif de sécurité
Renseignement contenu dans une décision rendue dans l'exercice de fonctions juridictionnelles (art. 29.1 al. 2)	Obligatoire	Dont l'existence ou la communication doit être refusée en vertu de la Loi sur l'accès



Restriction	Nature	Préjudice
Analyse (art. 32)	Facultative	Effet sur une procédure judiciaire
Tout renseignement (art. 41)	Facultative	- Entrave à une opération de vérification - Révélation d'un programme ou d'un plan d'activité de vérification - Révélation d'une source confidentielle d'information relative à une vérification - Atteinte au pouvoir d'appréciation du vérificateur général

Restrictions à l'accès basées sur la nature du document, sans égard à la démonstration d'un préjudice par l'organisme public

Restriction	Nature
Renseignements d'un autre gouvernement ou d'une organisation internationale (art. 18)	Facultative
Secret industriel de l'organisme public (art. 22)	Facultative
Secret industriel d'un tiers ou renseignements industriels, financiers, commerciaux, scientifiques, techniques ou syndicaux fournis par un tiers et habituellement traités de façon confidentielle par ce tiers (art. 23)	Obligatoire
Étude préparée en vue de l'imposition d'une taxe, d'un tarif, d'une redevance (art. 27 al. 2)	Facultative
Renseignements portant sur une méthode ou une arme susceptible d'être utilisée pour commettre un crime ou une infraction à la loi (art. 29 al. 1)	Obligatoire
Renseignements d'une décision juridictionnelle visés par une ordonnance de non-publication, de non-divulgence ou de non-diffusion (art. 29.1 al. 2)	Obligatoire
Renseignements révélant le délibéré lié à l'exercice de fonctions juridictionnelles (art. 29.1 al. 3)	Obligatoire
Décret dont la publication est différée ou décision résultant des délibérations du Conseil exécutif ou décision du Conseil du trésor (art. 30)	Facultative
Tout renseignement dont la divulgation aurait pour effet de révéler une politique budgétaire du gouvernement avant que le ministre des Finances ne la rende publique (art. 30.1)	Facultative
Opinion juridique (art. 31)	Facultative



Restriction	Nature
Diverses communications, recommandations ou analyses du Conseil exécutif, d'un de ses membres, du Conseil du trésor ou d'un comité ministériel ou les mémoires ou les comptes rendus des délibérations du Conseil exécutif ou d'un comité ministériel ou une liste de titres de documents comportant des recommandations au Conseil exécutif ou au Conseil du trésor ou l'ordre du jour d'une réunion du Conseil exécutif, du Conseil du trésor ou d'un comité ministériel ou les mémoires des délibérations du comité exécutif d'un organisme municipal, les recommandations qui lui sont faites par ses membres ainsi que les communications entre ses membres (art. 33)	Obligatoire
Document du bureau d'un membre de l'Assemblée nationale ou d'un cabinet politique ou du cabinet ou du bureau d'un membre d'un organisme municipal ou scolaire (art. 34)	Facultative
Mémoires de délibérations d'une séance du conseil d'administration ou des membres d'un organisme public (art. 35)	Facultative
Version préliminaire ou projet de texte législatif ou réglementaire ou analyse s'y rapportant (art. 36)	Facultative
Avis ou recommandation (art. 37 et 38)	Facultative
Analyse à l'occasion d'une recommandation dans le cadre d'un processus décisionnel (art. 39)	Facultative
Épreuve destinée à l'évaluation des connaissances, des aptitudes, de la compétence ou de l'expérience d'une personne (art. 40)	Facultative



1.2.2. La consultation non systématique des tiers

Sommaire

Certains types de renseignements fournis par un tiers, comme des secrets industriels, ne peuvent être communiqués en réponse à une demande d'accès par les organismes publics sans le consentement du tiers. Plusieurs responsables de l'accès refusent l'accès à de tels renseignements sur la base de ces restrictions sans avoir contacté le tiers. Cette situation a des effets indésirables, comme l'allongement indu, pour des raisons de pure procédure, du délai total requis pour que le citoyen accède à des documents qui pourraient éventuellement lui être accessibles.

Dans une optique d'efficience, la Commission soumet quelques pistes de solutions législatives à explorer pour diminuer ces effets :

- Obliger la consultation systématique du tiers par le responsable de l'accès lorsque ces restrictions s'appliquent.
- Obliger l'identification du tiers dans la décision rendue par le responsable de l'accès de l'organisme public, sauf exception.

1.2.2.1. Contexte

L'application des restrictions au droit d'accès aux documents portant sur certains types de renseignements fournis par un tiers¹⁸² suit des modalités particulières. Celles-ci amènent leur lot d'enjeux relatifs aux délais d'accès pour les demandeurs. Les démarches requises pour assurer le dénouement des demandes impliquant ces restrictions sont menées beaucoup plus rondement et efficacement en amont, par le responsable de l'accès. Il convient donc d'imposer qu'elles le soient, au bénéfice de la célérité de l'accès et d'une saine utilisation des ressources de la section juridictionnelle de la Commission.

1.2.2.2. Situation actuelle

La Loi sur l'accès restreint le droit d'accès à des documents des organismes publics lorsqu'ils contiennent certains types de renseignements fournis par un tiers, soit :

- un secret industriel ou un renseignement industriel, financier, commercial, scientifique, technique ou syndical de nature confidentielle et habituellement traité par ce tiers de façon confidentielle¹⁸³;

¹⁸² Il est à noter que la notion de « tiers » réfère à des « [...] personnes physiques et morales qui exercent leurs activités à l'extérieur de l'État » et « [...] qu'il semble maintenant avéré en jurisprudence qu'un organisme public qui a fourni des renseignements à un autre organisme public ne peut se qualifier comme tiers ». Raymond DORAY et François CHARETTE, *Accès à l'information: loi annotée, jurisprudence, analyse et commentaires*, MAJ 64, 10/2025, volume 1, Cowansville, Éditions Yvon Blais, 2001, sect. LAI-500 / 23:1 et LAI-510-511 / 23.9.

¹⁸³ Loi sur l'accès, art. 23.



- un renseignement dont la divulgation risquerait vraisemblablement d'entraver une négociation en vue de la conclusion d'un contrat, de causer une perte à ce tiers, de procurer un avantage appréciable à une autre personne ou de nuire de façon substantielle à la compétitivité de ce tiers¹⁸⁴.

Dans le cas d'une demande d'accès portant sur un document pour lequel tous les critères d'application de la restriction sont satisfaits, le responsable de l'accès de l'organisme public doit refuser de le communiquer, à moins d'obtenir le consentement du tiers concerné¹⁸⁵.

Avant de communiquer un renseignement industriel, financier, commercial, scientifique, technique ou syndical, le responsable de l'accès de l'organisme public doit aviser le tiers concerné de son intention pour lui permettre de présenter ses observations¹⁸⁶. Dans ce cas, l'avis au tiers doit, notamment :

- être fait par écrit;
- être fait dans les 20 jours suivant la date de réception de la demande d'accès concernée;
- permettre au tiers de présenter ses observations écrites et lui indiquer le délai imparti pour le faire, soit 20 jours¹⁸⁷.

À défaut d'une réponse à cet avis, le tiers est réputé avoir consenti à ce que l'accès au document soit donné.

Une fois les observations du tiers reçues ou le délai de réponse écoulé, le responsable de l'accès dispose d'un délai maximal de 15 jours pour rendre sa décision et en donner avis au tiers concerné, s'il a présenté des observations¹⁸⁸.

Ce processus d'avis n'a pas à être appliqué dans les cas où :

- le renseignement a été fourni à l'organisme public en application d'une loi qui prévoit que ce renseignement peut être communiqué;
- le tiers concerné a renoncé à l'avis en consentant à la communication du renseignement ou autrement¹⁸⁹.

Il est important de souligner qu'un organisme public qui n'a pas l'intention de divulguer les renseignements provenant d'un tiers, notamment lorsqu'il envisage d'invoquer d'autres restrictions pour refuser la communication des renseignements en cause, n'est pas tenu de donner un avis au tiers concerné¹⁹⁰.

1.2.2.3. Enjeux

La Commission relève plusieurs enjeux en lien avec le processus en place concernant le traitement des demandes d'accès impliquant des renseignements fournis par un tiers et visés par les restrictions mentionnées ci-dessus¹⁹¹.

Principalement, puisqu'ils n'en ont pas l'obligation formelle, certains responsables de l'accès ne consultent pas les tiers, surtout lorsqu'une demande en touche plusieurs à la fois. Ils refusent alors tout simplement

¹⁸⁴ *Id.*, art. 24.

¹⁸⁵ *Id.*, art. 23-24.

¹⁸⁶ *Id.*, art. 25.

¹⁸⁷ *Id.*, art. 49.

¹⁸⁸ *Id.*

¹⁸⁹ *Id.*, art. 25.

¹⁹⁰ R. DORAY et F. CHARETTE, préc., note 182, sect. LAI-636 / 25-1.

¹⁹¹ La Commission faisait des constats similaires en 2015. Voir : COMMISSION D'ACCÈS À L'INFORMATION, préc., note 152, p. 26 et 27.

l'accès aux documents sur la base des restrictions concernées, sans autres démarches. Dans presque tous les cas, les décisions rendues ne comportent ni le nom ni les coordonnées des tiers concernés.

Lorsqu'une demande de révision de la décision est ensuite déposée devant la Commission, cette dernière doit prendre les mesures pour aviser les tiers ayant des intérêts dans le dossier et les inviter à participer à l'instance¹⁹². Lorsque les tiers ne sont pas identifiés, la Commission doit communiquer avec le responsable de l'accès de l'organisme concerné pour obtenir leur identité ainsi que leurs coordonnées. Cette démarche prend du temps, et certaines demandes de ce type demeurent sans réponse. Le nouveau processus de gestion hâtive des dossiers juridictionnels mis en place par la Commission, présenté dans la section 1.2.3.3.1.3, apporte temporairement une solution à ces situations : un juge administratif peut exiger rapidement que l'organisme identifie les tiers. La Commission peut alors compléter ses démarches pour les en aviser.

Les tiers contactés par la Commission n'ont souvent aucune idée de la procédure en cours, ce qui peut susciter des questions que la Commission doit ensuite gérer. En toute logique, ce type d'intervention devrait plutôt être assumé par l'organisme public à qui le tiers a fourni le document, lequel entretient déjà avec lui une certaine relation et est en mesure de fournir des éléments de contexte.

Ultimement, plusieurs tiers contactés par la Commission acceptent tout simplement la divulgation des renseignements visés par la demande d'accès. D'autres, à terme, ne se présentent pas à l'audience. Sous réserve d'autres motifs qui pourraient être invoqués par l'organisme public concerné, la démarche aboutit alors à la divulgation des documents demandés, mais seulement plusieurs mois après la demande d'accès. Dans ces cas, plusieurs démarches administratives supplémentaires auraient pu être évitées si les tiers concernés avaient été consultés dès le début par l'organisme public.

Les démarches évoquées ci-dessus demandent des ressources et du temps : elles peuvent occasionner, dans certains cas, des ralentissements de quelques mois dans la démarche des demandeurs pour obtenir accès à des documents visant des renseignements fournis par des tiers. Le citoyen voit ainsi s'allonger le délai pour accéder à des documents s'ils lui sont, ultimement, accessibles.

1.2.2.4. Recommandations

Afin de minimiser les délais et pour une meilleure efficience, la Commission invite le législateur à considérer deux pistes de solution.

Premièrement, elle estime que la consultation des tiers par les organismes publics devrait être obligatoire lorsqu'ils sont susceptibles d'invoquer les restrictions concernant des renseignements fournis par un tiers. La Loi sur l'accès prévoit déjà du temps pour que cette démarche soit menée¹⁹³. Cette obligation devrait donc être introduite sans modification au délai d'avis au tiers. En effet, la rapidité d'obtention des documents par un citoyen doit demeurer acceptable, et ce, même si un tiers est impliqué. La Commission considère toutefois qu'il y a lieu de s'assurer que l'introduction de cette obligation n'entraîne aucun délai supplémentaire d'accès, notamment lorsque l'application des articles 23 ou 24 est manifeste.

Deuxièmement, la Commission juge qu'il y a lieu d'obliger les organismes publics à identifier les tiers concernés dans leur décision rendue en réponse à une demande d'accès. Dans certains cas, il pourrait y

¹⁹² Loi sur l'accès, art. 137; *Règles de preuve et de procédure de la Commission d'accès à l'information*, RLRQ, c. A-2.1, r. 6, art. 8.

¹⁹³ Loi sur l'accès, art. 49.



avoir un enjeu de confidentialité lié au fait même d'identifier un tiers dans la décision transmise au demandeur. Pour ces situations, en cas de demande de révision, la Loi pourrait obliger les organismes publics à communiquer les coordonnées du tiers à la Commission et à lui préciser les motifs justifiant que son identité soit traitée de façon confidentielle.

Recommandation 9

Obliger les organismes publics à consulter de manière systématique les tiers concernés lorsqu'ils sont susceptibles d'invoquer les restrictions prévues aux articles 23 et 24 de la Loi sur l'accès.

Recommandation 10

Obliger les organismes publics à identifier le ou les tiers concerné(s) dans leur décision ou, lorsqu'il y a un enjeu de confidentialité associé à cette identification, les obliger à communiquer à la Commission, en cas de demande de révision, les coordonnées des tiers concernés dans un délai fixé par la Loi, accompagnées des motifs justifiant que leur identité soit traitée de façon confidentielle.



1.2.3. Les délais de traitement des demandes par les organismes publics

Sommaire

Les organismes publics doivent généralement traiter les demandes d'accès à l'information dans un délai de 20 jours, extensible à 30 jours advenant le cas où le traitement pourrait nuire au déroulement normal de leurs activités. Le non-respect de ces délais constitue cependant un problème important au Québec : seulement au sein des ministères, en 2024-2025, 27 % des demandes d'accès ont été traitées en plus de 30 jours. Cette situation constitue une atteinte majeure au droit à l'information des citoyens : tout retard correspond dans les faits à un refus d'accès. Le non-respect des délais rompt ainsi avec l'esprit de célérité de la Loi sur l'accès.

Dans cette section, la Commission constate :

- qu'un important volume de demandes d'accès n'est pas traité dans les délais légaux;
- que le non-respect des délais de traitement dépend de nombreux facteurs, qui relèvent tant des organismes publics que de l'exercice du droit d'accès par certains demandeurs.

La Commission rappelle que plusieurs recommandations formulées dans le présent rapport contribueraient à faire diminuer les délais de traitement. Elle formule en outre des recommandations visant à :

- prévoir des conséquences explicites pour les organismes publics ne respectant pas les délais légaux;
- permettre à la Commission d'interdire à des demandeurs abusifs de formuler des demandes d'accès sans son autorisation;
- entamer une réflexion approfondie sur l'opportunité de réviser les délais légaux.

1.2.3.1. Contexte

La Commission est préoccupée par le niveau élevé de non-respect des délais de traitement des demandes d'accès aux documents¹⁹⁴ au Québec. Cette situation, qui perdure depuis de nombreuses années, empêche le public d'avoir accès à l'information en temps utile, ce qui compromet la pertinence du droit à l'accès à l'information – mais aussi l'imputabilité des organismes publics, la participation des citoyens aux processus démocratiques et l'examen indépendant de l'action publique. Retarder l'accès revient à refuser l'accès.

Il y a lieu de remédier à cette situation, sans quoi le droit d'accès risque d'être privé de toute la force que lui a conférée le législateur.

¹⁹⁴ La Commission concentre son propos sur les demandes d'accès aux documents, mais il est également applicable aux demandes d'accès aux renseignements personnels.

1.2.3.2. Situation actuelle

La Loi sur l'accès prévoit que le responsable de l'accès aux documents d'un organisme public doit rendre avec diligence une décision quant aux demandes qu'il reçoit, au plus tard dans les 20 jours qui suivent leur réception¹⁹⁵. Sa décision doit comprendre les motifs de refus, s'il y a lieu, et doit donc faire référence aux restrictions au droit d'accès qui ont été invoquées¹⁹⁶.

Dans le cas où le traitement de la demande en 20 jours « ne lui paraît pas possible sans nuire au déroulement normal des activités de l'organisme public », le responsable peut, avant l'expiration de ce délai, le prolonger d'au plus 10 jours et doit en aviser le demandeur par écrit¹⁹⁷.

En somme, les demandeurs peuvent généralement s'attendre à recevoir une décision au plus tard 30 jours civils après avoir formulé leur demande d'accès.

La seule exception à ces délais s'applique dans le cas où un tiers doit être avisé qu'une demande d'accès concerne des renseignements qu'il a fournis¹⁹⁸. Le responsable dispose alors de 20 jours, à compter de la réception de la demande, pour en aviser le tiers¹⁹⁹. Le tiers a lui-même 20 jours pour présenter ses observations²⁰⁰. À l'expiration de ce délai, le responsable doit transmettre sa décision finale au demandeur et au tiers dans les 15 jours²⁰¹.

La figure suivante résume ainsi les délais de traitement maximaux prévus par la Loi sur l'accès, selon la situation.



¹⁹⁵ Loi sur l'accès, art. 47.

¹⁹⁶ *Id.*, art. 50.

¹⁹⁷ *Id.*, art. 47 al. 2.

¹⁹⁸ *Id.*, art. 25 et 49.

¹⁹⁹ *Id.*, art. 49, al. 1.

²⁰⁰ *Id.*, art. 49, al. 2.

²⁰¹ *Id.*, art. 49, al. 4.



Si le responsable ne transmet pas sa décision concernant une demande d'accès formulée par écrit dans les délais prescrits par la Loi, il est réputé avoir refusé la demande²⁰². Le demandeur peut alors introduire un recours en révision à la Commission²⁰³.

Un organisme public qui estime que le traitement d'une demande « serait susceptible de nuire sérieusement [à ses] activités » peut demander à la Commission, dans le même délai que celui dont il disposerait normalement pour rendre sa décision²⁰⁴, l'autorisation de ne pas tenir compte de la demande²⁰⁵. Dans ces cas, la Commission peut donner droit au recours, restreindre la demande ou prolonger le délai de traitement²⁰⁶.

1.2.3.3. Enjeux

La Commission dresse deux constats principaux concernant les délais de traitement des demandes d'accès. Premièrement, un important volume de demandes est traité tardivement. Deuxièmement, les facteurs pouvant expliquer les longs délais de traitement sont nombreux et plus étendus que ceux auxquels les organismes publics font couramment référence.

1.2.3.3.1. Un important volume de demandes d'accès n'est pas traité dans les délais légaux

La Commission constate que les organismes publics font trop souvent défaut de traiter les demandes d'accès dans les délais prévus par la Loi sur l'accès. Cette situation mine le droit d'accès et contraint les citoyens à introduire des recours auprès de la Commission.

1.2.3.3.1.1. Plusieurs indicateurs révèlent un enjeu de délais

En 2022, la Commission a réalisé une étude sur les délais de traitement des demandes d'accès auprès d'un échantillon de 33 organismes publics²⁰⁷. Même si elle portait notamment sur la période pandémique, alors que les organismes peinaient plus qu'à l'ordinaire à respecter leurs obligations en matière d'accès à l'information, cette étude a révélé de longs délais de traitement au sein de plusieurs d'entre eux. En temps normal, le délai de traitement moyen excédait 20 jours pour environ la moitié des organismes examinés, et 30 jours pour 16 % d'entre eux : cette dernière proportion a ensuite doublé en contexte d'urgence sanitaire.

Un examen des données présentées dans les rapports annuels de gestion les plus récents d'une cinquantaine de ministères et de grands organismes hors des réseaux municipal, de l'éducation et de la santé²⁰⁸ montre que cette tendance inquiétante perdure. Quelque 25 % de ces organismes, dont quatre des cinq qui reçoivent le plus de demandes à l'échelle du gouvernement, traitent au moins 15 % des demandes d'accès aux documents au-delà du délai maximal de 30 jours prescrit par la Loi sur l'accès.

²⁰² *Id.*, art. 52.

²⁰³ *Id.*, art. 135.

²⁰⁴ *Id.*, art. 137.1 al. 3.

²⁰⁵ *Id.*, art. 137.1.

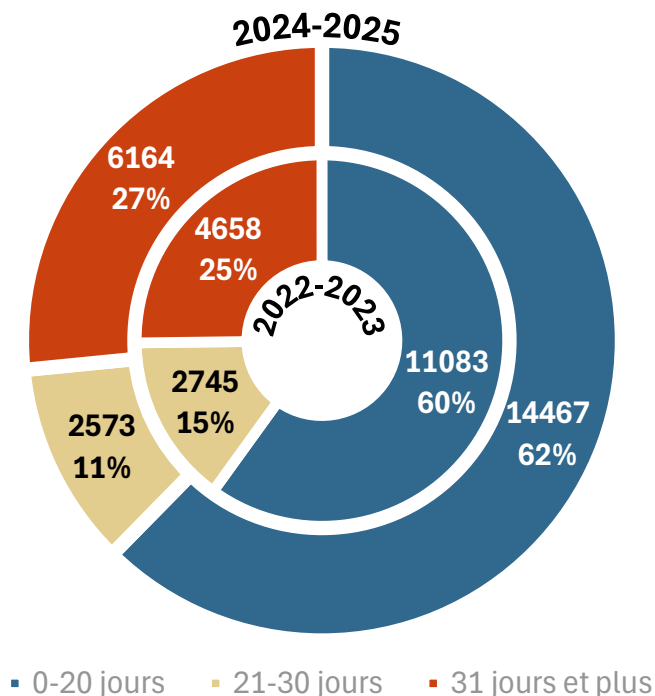
²⁰⁶ *Id.*

²⁰⁷ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97.

²⁰⁸ La Commission a utilisé les chiffres diffusés dans le rapport annuel 2024 ou 2024-2025, selon le cas, des 23 ministères et de 29 organismes en application du *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*, RLRQ, c. A-2.1, r. 2, art. 2 al. 3 [ci-après *Règlement sur la diffusion*].

Il y a deux ans, des journalistes avaient réalisé un exercice du même genre, qui menait à des constats similaires²⁰⁹. La figure suivante compare les résultats des deux compilations pour les ministères²¹⁰.

Nombre de demandes d'accès aux documents administratifs et répartition selon leur délai de traitement par les 23 ministères en 2022-2023 et en 2024-2025



Bon nombre des demandes d'accès traitées tardivement n'aboutissent pas en révision devant la Commission : comme le montre le graphique ci-dessus, 6 164 d'entre elles ont été traitées en plus de 30 jours par les ministères en 2024-2025. Or pour la même année, la Commission a reçu 565 demandes de révision pour motif de non-respect des délais à travers tous les organismes publics, représentant néanmoins une part importante des recours qu'elle examine en matière d'accès aux documents. Comme l'illustre le tableau ci-dessous, depuis 2015-2016, leur proportion a varié entre le cinquième et le tiers de toutes les demandes de révision en accès aux documents²¹¹. Le pic de 42 % atteint en 2024-2025 tend à montrer que la pandémie ne saurait être l'unique cause de la situation.

²⁰⁹ Thomas GERBET et Daniel BOILY, « Le ministère de l'Éducation du Québec, mauvais élève de l'accès à l'information », *Radio-Canada* (18 avril 2024), en ligne : <<https://ici.radio-canada.ca/nouvelle/2065858/ministere-education-acces-information-sante-quebec>> (consulté le 23 avril 2024).

²¹⁰ Notons que la compilation de Radio-Canada portait exclusivement sur les ministères. Dans la figure, les chiffres de 2024-2025 sont issus de la compilation de la Commission et ceux de 2022-2023, de celle de Radio-Canada.

²¹¹ Il faut noter que des tendances en tous points concordantes sont observables pour les demandes de révision concernant l'accès à des renseignements personnels. Elles aussi concernent une proportion allant de 25 à 35 % de l'ensemble des recours en cette matière introduits à la Commission, chaque année depuis 2015-2016.

**Évolution du nombre et de la proportion de recours en révision en matière d'accès aux documents administratifs présentés à la Commission en raison d'une absence de réponse dans les délais légaux**

Indicateur	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	2021-2022	2022-2023	2023-2024	2024-2025	2025-2026 (estimation) ²¹²
Nombre de recours en accès aux documents administratifs faisant suite à une absence de réponse dans les délais légaux	293	284	210	238	258	349	394	346	362	565	424
Nombre total de recours en accès aux documents administratifs	1 128	1 239	961	1 027	1 091	1 058	1 220	1 115	1 277	1 365	1 548
Proportion impliquant le non-respect des délais	26 %	23 %	22 %	23 %	24 %	33 %	32 %	31 %	28 %	42 %	27 %

Les journalistes, grands utilisateurs du droit d'accès à l'information, font état depuis des années des problèmes vécus à cet égard. Un sondage mené en 2022 par la Fédération professionnelle des journalistes du Québec auprès de 147 de ses membres révèle que le dépassement des délais légaux est de loin le problème le plus fréquemment rencontré en accès, étant nommé par 41 % des répondants²¹³.

1.2.3.3.1.2. Les conséquences des délais sont importantes

Lorsque les organismes publics ne respectent pas les délais légaux de réponse aux demandes d'accès, le droit à l'information en souffre. D'une part, chaque demandeur subit une atteinte à son propre droit; d'autre part, à l'échelle de la société, c'est l'un des fondements de la démocratie qui s'érode, au détriment de la confiance du public en ses institutions.

Le respect des délais revêt une importance cardinale puisque la valeur de l'information s'inscrit dans un contexte temporel. L'intérêt pour une information émerge dans des circonstances et à un moment donnés. Il peut par exemple découler d'un projet de construction en cours, d'un événement dans l'actualité, d'une situation pouvant entraîner des conséquences en matière d'environnement, d'une décision d'affaires à prendre ou d'un litige à venir. Ainsi, les retards dans l'obtention de documents ont de réelles conséquences. Il importe que la documentation concernant les justifications ou les effets de certaines décisions gouvernementales ne soit pas rendue accessible que plusieurs années après les faits, au moment où il n'est plus possible de changer le cours des choses. En parallèle, lorsqu'il s'agit d'accès aux

²¹² Il s'agit d'une estimation, la compilation finale n'étant pas achevée à la date de finalisation de ce rapport.

²¹³ FÉDÉRATION PROFESSIONNELLE DES JOURNALISTES DU QUÉBEC, *Sondage accès à l'information réalisé entre les mois de janvier 2022 et juin 2022*, 2022, en ligne : <https://cdn.ca.yapla.com/company/CPY9xhmJrXC8hpGUQ5ssMX3n/asset/files/Sondage%20Acces%CC%80s%20information.pdf>, question 7.

renseignements personnels, les effets d'un non-respect des délais peuvent aussi être majeurs, pouvant notamment mettre en péril les recours des citoyens se sentant lésés par des décisions de l'administration publique.

Lorsque les demandeurs ne reçoivent pas de décision dans les délais prescrits, leur demande d'accès est présumée refusée dans sa totalité. En l'absence d'une décision, ils n'ont aucun détail sur les motifs de refus. S'ils souhaitent faire respecter leurs droits, ils peuvent soit attendre une décision sans certitude qu'elle vienne, soit présenter une demande de révision à la Commission sans connaître les arguments qui pourraient être soulevés par l'organisme public concerné. Cette démarche est en soi une conséquence importante pour le demandeur. Pour la plupart des gens, une démarche devant un tribunal constitue un stress non négligeable. Pour les demandeurs agissant à titre professionnel, elle nécessite parfois certains coûts, notamment en représentation juridique. Soulignons que la section juridictionnelle de la Commission consacre des énergies importantes pour le traitement des quelque 25 à 30 % de recours en révision qui concernent uniquement le non-respect des délais. Il est raisonnable de croire qu'une certaine proportion des demandes de cette nature ne se traduiraient pas par des recours si le demandeur obtenait en temps utile une décision du responsable de l'accès aux documents.

1.2.3.3.1.3. La Commission s'est mise en action

La Commission a entrepris diverses actions en lien avec le non-respect des délais en accès aux documents. À la suite de son étude sur les délais d'accès en 2022, elle a ciblé 5 des 33 organismes visés par l'étude afin de réaliser des inspections sur leurs pratiques de traitement des demandes d'accès. En mars 2025, les rapports d'inspection ont été finalisés et transmis aux organismes visés, et des suivis sont effectués pour s'assurer que des correctifs soient apportés.

En parallèle, depuis juillet 2025, la Commission a progressivement implanté un processus de gestion hâtive de l'ensemble des recours déposés devant la Commission. Cette initiative vise entre autres à mieux gérer l'afflux de dossiers de sa section juridictionnelle, dont ceux qui découlent du non-respect des délais légaux. La gestion hâtive prévoit l'examen initial rapide et sommaire des faits du dossier par un juge administratif peu après son ouverture au greffe de la Commission. Concrètement, elle implique que les parties soient rapidement convoquées pour assister à une séance de gestion préliminaire. Dans le cas des organismes publics, un conseiller juridique doit comparaître au dossier. Une séance de gestion hâtive permet de traiter au moins 24 dossiers par jour.

À l'occasion de ce premier contact entre la Commission et les intervenants, le juge administratif s'assure que tout soit en place pour la suite du dossier, entre autres en faisant en sorte qu'il soit complet et en ciblant rapidement l'objet du litige. Dans le cas des demandes de révision déposées pour non-respect des délais, le processus de gestion hâtive permet de demander au représentant de l'organisme public de soumettre sa position au soutien du refus de la demande d'accès en cause. Dans plusieurs cas, l'organisme public donne ainsi accès aux documents demandés et le demandeur se désiste de son recours. Si l'accès est refusé en tout ou en partie, le demandeur a, à tout le moins, accès aux motifs invoqués par l'organisme. Il peut les juger raisonnables et, là encore, se désister. S'il en est insatisfait, ces motifs restent essentiels à sa préparation pour une éventuelle séance de médiation ou pour l'audience portant sur son recours. **La Commission estime que son nouveau processus de gestion hâtive lui permettra de faire prendre conscience plus rapidement aux organismes publics de l'importance de rendre une décision dans les délais. Il évitera une longue démarche de recours pour les demandeurs d'accès dans plusieurs cas. Malgré cela, il demeure essentiel que les demandeurs reçoivent une décision dans les délais légaux, sans avoir à introduire de recours pour ce motif.**

1.2.3.3.2. Le non-respect du délai de traitement dépend de nombreux facteurs

La question des délais de traitement des demandes d'accès aux documents est multifactorielle. Le temps pris pour rendre une décision en accès peut notamment dépendre de plusieurs éléments relevant du contexte des organismes, mais aussi de la façon dont le droit d'accès est utilisé par certains demandeurs et du cadre légal.

1.2.3.3.2.1. Les facteurs liés aux effectifs

L'une des principales causes mentionnées par les organismes publics pour expliquer le dépassement des délais légaux est le manque d'effectifs²¹⁴. D'aucuns évoquent aussi des disparités dans la formation du personnel impliqué dans le traitement des demandes d'accès, en raison notamment du fort taux de roulement dans les équipes soutenant les responsables de l'accès aux documents.

« 64 % des organismes interrogés indiquent que des problèmes liés aux ressources humaines minent leur capacité à respecter systématiquement les délais légaux. Entre autres, ils soulignent que la petite taille des équipes les rend moins résilientes dans des périodes de fort volume de demandes, lors des vacances annuelles ou en cas d'absence prolongée de l'un des employés. Plusieurs mentionnent également la difficulté d'embaucher et de garder des employés qualifiés dans le domaine de l'accès à l'information et de la protection des renseignements personnels et le temps de formation important qu'il faut investir pour qu'un nouvel employé soit efficace dans ses fonctions²¹⁵. »

Comme elle en fait état plus avant dans la section 1.3.1, la Commission estime que de nombreux organismes publics ne disposent pas suffisamment de ressources pour le traitement des demandes d'accès à l'information, et que la formation présente des lacunes.

Par ailleurs, la répartition des demandes d'accès dans l'année constitue un facteur fréquemment évoqué par les organismes publics. Il existe des périodes de pointe où davantage de demandes sont reçues. Par ailleurs, l'absence d'une bonne partie du personnel pendant les fêtes de fin d'année ou la période estivale compromettrait aussi le respect des délais. Les activités relatives à la fin d'année financière, comme la préparation de l'étude des crédits ou du rapport annuel, peuvent également fortement mobiliser les équipes, au détriment du respect des délais, en particulier dans les petits organismes.

1.2.3.3.2.2. Les facteurs liés au volume des demandes

Plusieurs organismes publics affirment faire face à un volume accru de demandes d'accès, lesquelles viseraient aussi davantage de documents. Certains signes montrent en effet que le nombre de demandes d'accès croît progressivement, comme le montrent les chiffres présentés dans le graphique de la section 1.2.3.3.1.²¹⁶ Cette situation peut s'expliquer de nombreuses façons, y compris par l'augmentation de la population, l'accès accru aux technologies de l'information ou un intérêt croissant pour les documents détenus par l'administration publique. Les organismes publics soutiennent néanmoins qu'elle a un effet sur le traitement des demandes d'accès qu'ils reçoivent. Dans ce contexte, le décalage entre les besoins et les ressources octroyées s'accroît.

²¹⁴ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97, p. 11 à 20, et plus particulièrement 17.

²¹⁵ *Id.*, p. 13-14.

²¹⁶ La Commission souligne qu'en l'absence d'un portrait statistique détaillé et probant à l'échelle de l'administration publique, question qu'elle aborde en détail à la section 1.4, il n'est pas aisé de confirmer ou d'infirmer une tendance globale, au-delà des ministères, à l'augmentation du nombre de demandes d'accès, ni d'en quantifier l'ampleur le cas échéant.

En ce qui a trait à l'accroissement potentiel du volume de documents à examiner pour chaque demande, comme la Commission l'expose dans la section 1.3.2, elle observe depuis des années que la gestion de l'information dans les organismes publics n'a pas suivi le rythme de l'évolution numérique. **Or les organismes publics, s'ils bénéficient des avantages du numérique à de nombreux égards, doivent aussi ajuster en contrepartie leur gestion de l'information, notamment en ce qui a trait aux règles de classification et de conservation des documents.** En appliquant des politiques modernisées, entre autres sur le clavardage, les courriels ou les documents intermédiaires, les organismes publics pourraient vraisemblablement mieux juguler la masse documentaire qu'ils détiennent. Ils pourraient ainsi exercer un certain contrôle sur l'effet du volume documentaire sur les délais, en contribuant à abaisser le nombre moyen de documents repérés pour chaque demande d'accès. Rappelons qu'une grande proportion du temps consacré au traitement des demandes d'accès est voué au repérage des documents, mais également à leur analyse : des opérations qui prennent plus de temps lorsque le nombre de documents est important.

1.2.3.3.2.3. Les facteurs liés à l'exercice du droit d'accès par les demandeurs

La façon dont les demandeurs exercent leur droit d'accès constitue un autre facteur pouvant avoir un effet sur les délais.

LA COMPLEXITÉ ET LA PRÉCISION DES DEMANDES

Des organismes publics font état de demandes qui seraient de plus en plus complexes²¹⁷. Elles comprendraient par exemple des termes peu spécifiques, comme « tout document », ou viseraient de grandes périodes ou des documents dont la nature induit une complexité sur le plan du repérage, comme des échanges de courriels, de messages instantanés ou de messages textes. Un certain manque de précision dans les informations recherchées serait également constaté dans plusieurs cas.

Ces facteurs peuvent effectivement compliquer l'analyse de la demande et le repérage des documents, allongeant ainsi le délai de traitement. La Commission rappelle cependant que les demandeurs n'ont pas nécessairement une connaissance fine des types de documents détenus par les organismes publics ni de la manière dont ils sont classés. Les organismes assujettis au Règlement sur la diffusion doivent publier proactivement leur plan de classification²¹⁸, et dans tous les cas, celui-ci, ou une liste de classement équivalente, doit être disponible sur demande²¹⁹. Il reste que ce type de document donne davantage un aperçu de l'étendue des activités des organismes plutôt que de la nature des documents détenus²²⁰.

LES DEMANDES ABUSIVES

De nombreux organismes publics font face à un afflux de demandes de la part de demandeurs persistants. Certains citoyens convaincus d'être dans leurs droits se trouvent ainsi, par le biais de demandes complexes, imprécises, répétées, parfois menées avec une attitude hostile, à accaparer à eux seuls une part importante des ressources des organismes publics dédiées au bon traitement des demandes d'accès. Cette situation se manifeste également dans les recours qui peuvent être déposés à la Commission à la suite de telles demandes.

²¹⁷ Voir COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97, p. 18 et 25.

²¹⁸ Règlement sur la diffusion, art. 4 par. 4.

²¹⁹ Loi sur l'accès, art. 16 al. 3.

²²⁰ Les responsables de l'accès aux documents ont d'ailleurs le devoir de prêter assistance aux demandeurs pour les aider à préciser leur demande : *Id.*, art. 42 et 95.



Ces cas ne sont pas rares. Les démarches à effectuer pour gérer les demandes d'accès abusives ou les demandes de révision qui en découlent peuvent nuire aux activités en accès à l'information et allonger les délais de traitement de toutes les demandes, notamment lorsqu'il s'agit de petits organismes. Certains demandeurs visent même plusieurs organismes publics avec des demandes récurrentes et similaires²²¹.

Le droit d'accès aux documents et aux renseignements personnels ainsi que les recours qui y sont associés sont protégés et importants dans une société libre et démocratique. Cependant, ils ne sont pas sans limites. C'est pourquoi le législateur a prévu deux mécanismes pour s'assurer qu'une personne ne puisse pas en faire un usage abusif et déraisonnable :

- Lorsqu'ils font face à des demandes « manifestement abusives par leur nombre, leur caractère répétitif ou leur caractère systématique », ou encore lorsque le traitement d'une demande « serait susceptible de nuire sérieusement » à leurs activités, les organismes publics peuvent demander à la Commission l'autorisation de ne pas en tenir compte²²². Ce pouvoir permet d'agir à l'égard d'une demande d'accès avant qu'elle ait été traitée, dans l'objectif principal de préserver l'utilisation des ressources de l'organisme public.
- Lorsqu'il y a « des motifs raisonnables de croire que la demande est frivole ou faite de mauvaise foi ou que son intervention n'est manifestement pas utile »²²³, la Commission peut refuser ou cesser d'examiner une affaire. Ce pouvoir vise les demandes de révision et contribue à protéger les ressources de la Commission, mais également celles des organismes publics, indirectement, puisqu'ils doivent se préparer aux démarches devant la section juridictionnelle.

La Commission peut interdire à une personne d'introduire une demande de révision ou de présenter un acte de procédure dans une instance déjà introduite sans avoir obtenu l'autorisation préalable de la présidence de la Commission²²⁴. En somme, un organisme public impliqué dans des demandes de révision frivoles ou faites de mauvaise foi peut demander à la Commission d'appliquer ce pouvoir. Ce type de demande a déjà été présenté devant la section juridictionnelle, qui a effectivement interdit à certains demandeurs de déposer de nouvelles demandes de révision²²⁵.

À l'étape du traitement des demandes d'accès, les organismes publics faisant face à des demandeurs abusifs doivent recourir au premier mécanisme décrit ci-haut. Cependant, ils sont tenus de répéter cette exigeante démarche²²⁶ chaque fois que nécessaire, y compris lorsqu'un même demandeur est en cause. Le recours n'est que rétrospectif : il vise les demandes d'accès reçues, et non celles qui pourraient advenir²²⁷.

²²¹ Dans l'affaire *Municipalité Les Coteaux c. Binet*, 2025 QCCA 298, en ligne : <<https://canlii.ca/t/kfzzd>>, huit organismes publics et entreprises ont demandé à la Commission d'agir face aux demandes répétées d'une seule personne.

²²² Loi sur l'accès, art. 137.1.

²²³ *Id.*, art. 137.2.

²²⁴ *Id.*, art. 137.2 al. 2.

²²⁵ Voir *Gagliano c. Ordre des comptables professionnels agréés du Québec*, 2023 QCCA 398, en ligne : <<https://canlii.ca/t/kfzzd>>; *Municipalité Les Coteaux c. Binet*, préc., note 221; voir aussi la décision suivante, où la Commission a refusé de faire usage de ce pouvoir vu les faits au dossier : *Doyon c. CISSS Chaudière-Appalaches*, 2025 QCCA 96, en ligne : <<https://canlii.ca/t/kbv05>>.

²²⁶ Puisque le fait de ne pas tenir compte d'une demande constitue une limitation importante du droit d'accès d'une personne, la Commission s'attend à une démonstration probante du caractère abusif allégué, qui exige donc une préparation sérieuse par les organismes publics.

²²⁷ Voir notamment *Université McGill c. C.B.*, 2013 QCCA 274, par. 38 à 46, en ligne : <<https://canlii.ca/t/g0zr6>>; *Prévost (Ville de) c. L.C.*, 2020 QCCA 123, par. 74 et 75, en ligne : <<https://canlii.ca/t/g7qwx>>; *Ville de Saint-Constant c. Vachon*, 2020 QCCA 61, par. 65 à 70, en ligne : <<https://canlii.ca/t/j6x8v>>.



Par conséquent, certains organismes ont exprimé un intérêt de voir la Commission interdire à un demandeur de *formuler de nouvelles demandes d'accès* auprès d'eux sans avoir obtenu au préalable l'autorisation de sa présidence. Suivant l'interprétation actuelle de la Commission, toutefois, son pouvoir d'imposer une telle préautorisation ne s'applique qu'aux demandes de révision déposées devant sa section juridictionnelle²²⁸.

1.2.3.3.2.4. Le peu de conséquences pour le non-respect des délais

Selon la Commission, il existe une imprécision dans la Loi sur l'accès concernant les conséquences pour les organismes publics en cas de non-respect des délais, qui contribue à ce que certains organismes considèrent qu'il n'est pas nécessaire d'améliorer la situation. Les conséquences principales, comme mentionné précédemment, sont plutôt vécues par les demandeurs d'accès.

Présentement, un organisme public a relativement peu à perdre s'il ignore une demande ou qu'il transmet sa décision hors délai. Si le demandeur n'exerce pas ses recours, l'organisme évite le traitement et, conséquemment, la diffusion des documents demandés. En cas de demande de révision à la Commission, l'organisme étant présumé avoir refusé, un nouveau délai s'écoule avant que sa position au soutien de ce refus ne soit documentée. Il arrive aussi que l'organisme prépare une décision sommaire seulement dans l'objectif de compléter le dossier ultérieurement s'il y a contestation de sa décision.

Actuellement, des organismes transmettent des versions modifiées de leur décision au fur et à mesure de l'évolution du dossier, et ce, même jusqu'à l'audience. Une jurisprudence étoffée²²⁹ s'est développée autour de cette question. Elle concerne principalement l'invocation tardive de restrictions facultatives au droit d'accès²³⁰. En l'état actuel du droit, un organisme n'est pas forcé d'avoir recours à ces restrictions, pour autant qu'il justifie à la Commission des circonstances expliquant son défaut de les avoir invoquées dans le délai initial de traitement de la demande d'accès²³¹. Son rapport quinquennal de 2011 présentait cette situation de manière détaillée²³².

D'une manière analogue, il arrive même qu'un organisme public demande à la Commission l'autorisation de ne pas tenir compte d'une demande d'accès initiale²³³, alors que le demandeur a déjà dû déposer une demande de révision, n'ayant pas obtenu de décision de l'organisme dans les délais prescrits. Là encore, l'organisme doit présenter une demande pour être relevé du défaut d'avoir formulé cette demande d'autorisation dans les délais applicables²³⁴.

Ultimement, même si la Commission tranche en faveur du demandeur au cours de la demande de révision, l'organisme a bénéficié d'une période supplémentaire, écoulée pendant le traitement du recours,

²²⁸ *Gagliano c. Ordre des comptables professionnels agréés du Québec*, préc., note 225, par. 79 à 99.

²²⁹ R. DORAY et F. CHARETTE, préc., note 182, p. LAI-1213 à LAI-1217 (47:5) et LAI-1220 à LAI-1224 (47:8).

²³⁰ Comme mentionné à la section 1.2.1, les restrictions obligatoires, qui protègent des intérêts légitimes particulièrement importants, peuvent être invoquées à n'importe quel moment, voire par la Commission elle-même en cours d'instance si l'organisme omet de le faire.

²³¹ À la suite de jugements de la Cour du Québec, la Commission doit respecter des balises précises dans l'évaluation des justifications présentées, ce qui peut parfois la limiter. Elle reste cependant vigilante et refuse les motifs déraisonnables. Voir par exemple : *Saulnier c. Ministère de la Sécurité publique (Sûreté du Québec)*, 2023 QCCA 18, par. 81 et suivants, en ligne : <<https://canlii.ca/t/jvwwk>>; cette décision a été confirmée en appel par la Cour du Québec : *Procureur général du Québec (Ministère de la Sécurité publique) (Sûreté du Québec) c. Saulnier*, 2024 QCCQ 3799, en ligne : <<https://canlii.ca/t/k67th>> (consulté le 6 février 2026).

²³² Rapport quinquennal 2011, p. 61-62.

²³³ Loi sur l'accès, art. 137.1.

²³⁴ *Id.*, art. 137.1 al. 3.



avant de divulguer les documents. Cette situation présente le risque que certains l'exploitent à des fins dilatoires.

La Commission souligne néanmoins que le processus de gestion hâtive présenté à la section 1.2.3.3.1.3 présente le potentiel d'atténuer la situation décrite ci-haut.

1.2.3.4. Recommandations

Les délais de traitement des demandes d'accès doivent diminuer : il en va de l'efficacité d'un droit essentiel.

Même dans le cadre de la Loi sur l'accès telle qu'elle existe actuellement, les organismes publics pourraient en faire davantage pour améliorer la situation. Entre autres, ils devraient investir davantage de ressources dans le traitement des demandes d'accès²³⁵ et améliorer leur gestion de l'information²³⁶. Par ailleurs, une diffusion proactive accrue, rendant davantage de documents disponibles sans formalités, serait susceptible de faire diminuer le nombre de demandes reçues.

Néanmoins, certaines solutions aux délais de traitement trop longs doivent passer par des modifications législatives. Il convient de prévoir des conséquences au non-respect des délais et d'élargir le pouvoir de la Commission face aux demandes d'accès abusives. Étant donné le caractère multifactoriel des délais, il y a également lieu qu'un ensemble de parties prenantes se penchent plus avant sur la façon dont sont prévus les délais à la Loi sur l'accès.

1.2.3.4.1. Prévoir des conséquences au non-respect des délais

De l'avis de la Commission, l'ajout de conséquences au non-respect des délais constitue un élément clé permettant d'encourager les organismes publics à la célérité.

Comme elle l'a déjà suggéré en 2011²³⁷, puis en 2015²³⁸ et encore en 2022²³⁹, elle préconise que le délai pour invoquer des restrictions facultatives au droit d'accès soit de rigueur, tout comme celui pour demander l'autorisation de ne pas tenir compte d'une demande d'accès. Ainsi, les organismes publics, s'ils sont hors délai, devraient être explicitement forclos de se prévaloir des restrictions facultatives de la Loi sur l'accès ou de présenter un recours concernant les demandes susceptibles de nuire sérieusement à leurs activités, à moins d'être en mesure de démontrer, de manière probante, des circonstances exceptionnelles justifiant l'impossibilité de respecter ce délai. Il s'agirait d'un resserrement du critère, constituant un incitatif renforcé à traiter les demandes dans les délais, sous peine d'une limite des possibilités offertes aux organismes publics pour protéger certains intérêts légitimes. L'invocation de motifs de restrictions obligatoires resterait possible à tout moment de la procédure, vu l'importance des intérêts légitimes en cause.

Puisque des problèmes semblables à ceux abordés précédemment s'appliquent aussi au traitement des demandes d'accès aux renseignements personnels, dans le secteur public comme le secteur privé, la Commission recommande que les changements appropriés soient apportés à l'ensemble des lois concernées, par cohérence.

²³⁵ Voir la section 1.3.1.

²³⁶ Voir la section 1.3.2.

²³⁷ Rapport quinquennal 2011, p. 61-63.

²³⁸ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 152, p. 14-16.

²³⁹ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97, p. 33-34.

Recommandation 11

Modifier la Loi sur l'accès, et, par concordance, la Loi sur le privé et la LRSSS, afin que :

- le délai pour transmettre une décision en réponse à une demande d'accès aux documents ou aux renseignements personnels et motiver un refus sur la base d'une restriction facultative au droit d'accès soit de rigueur et emporte déchéance;
- le délai pour qu'une organisation puisse de mander de ne pas tenir compte d'une demande soit de rigueur et emporte déchéance.

1.2.3.4.2. Permettre à la Commission d'interdire à des demandeurs abusifs de formuler des demandes d'accès sans son autorisation

La Commission estime qu'il pourrait être opportun de modifier la Loi afin d'étendre son pouvoir d'interdire à un demandeur de déposer une demande de révision sans l'autorisation préalable de sa présidence. Ainsi, la Commission pourrait, dans le cas d'un demandeur jugé quérulent suivant les critères applicables, lui interdire de formuler *des demandes d'accès* auprès d'un organisme public sans son autorisation.

La Commission note que la Cour supérieure dispose de ce pouvoir et qu'elle l'a déjà exercé pour interdire à un citoyen au comportement abusif de se prévaloir de son droit d'accès sans l'autorisation du tribunal²⁴⁰.

Dans une affaire tranchée en 2024 portant sur des comportements d'abus du droit d'accès et d'abus de procédure devant les tribunaux, la Cour supérieure a disposé ce qui suit²⁴¹ :

« [131] Si le droit d'accès à l'information est important et si l'accès aux tribunaux est un principe sacré, il s'agit d'un droit comme tout autre dont on ne doit pas abuser. Le comportement du Défendeur dans le cadre de la procédure pour outrage au tribunal démontre non seulement un outrage mais aussi un abus de procédure. [...]

[132] La Ville a déposé d'abondantes preuves à l'appui de ses allégations. Les éléments de preuve pertinents, admissibles et probants démontrent que le Défendeur a abusé de son droit d'accès et de son abus de procédure une fois devant les tribunaux. La preuve et le droit applicable ont chargé le Tribunal de décider quelles seraient les conséquences de l'abus du Défendeur.

[133] Le Défendeur a abusé de son droit de demander accès à l'information et d'ester en justice. En conséquence, il y a lieu de baliser désormais l'exercice des deux droits de sorte qu'il l'utilise à bon escient.

[...]

[151] Cela dit, il n'y a pas de surveillance générale confiée à la Commission en ce qui concerne le comportement d'une personne comme le Défendeur qui abuse de son droit d'accès et de la procédure devant les tribunaux. La plupart des comportements du Défendeur ne relèvent pas de la juridiction de la Commission. Même si certains éléments relevaient de sa

²⁴⁰ *Ville de Saint-Constant c. Vachon*, 2024 QCCS 1079, en ligne : <<https://canlii.ca/t/k3v4m>>.

²⁴¹ *Id.*; références omises.



compétence, la Commission ne dispose pas de l'éventail de mesures dont disposent la Cour du Québec et la Cour supérieure pour rendre leurs ordonnances effectives.

[...]

POUR CES MOTIFS, LE TRIBUNAL :

[...]

INTERDIT [au demandeur] d'introduire, directement ou indirectement, toute demande d'accès à l'information ou autre demande en vertu de la [Loi sur l'accès] auprès de la Ville [...], sans avoir obtenu au préalable l'autorisation écrite du juge en chef de la Cour du Québec ou d'un juge désigné par lui et aux conditions, le cas échéant, prévues par la Cour du Québec si l'introduction d'une demande est autorisée en tout ou en partie; »

Cette possibilité constituerait une solution permettant de décharger les organismes publics en lien avec certains demandeurs ainsi évalués comme étant quérulents. Partant, ils pourraient concentrer leurs ressources sur les demandes d'accès déposées par d'autres citoyens. Une telle mesure, qui ne serait utilisée que dans des cas exceptionnels, permettrait d'éviter la mauvaise utilisation des ressources des organismes publics en matière de traitement des demandes d'accès.

Ici encore, par cohérence, cette modification devrait être faite dans la Loi sur le privé et la LRSSS.

Recommandation 12

Modifier la Loi sur l'accès et, par concordance, la Loi sur le privé et la LRSSS, pour permettre à la Commission d'interdire à une personne démontrant une utilisation abusive et répétée de son droit d'accès de formuler une demande d'accès auprès d'une organisation donnée sans l'autorisation de la présidence de la Commission et selon les conditions que celle-ci détermine.

1.2.3.4.3. Entamer une réflexion approfondie sur l'opportunité de réviser les délais légaux

Pour la Commission, les délais de traitement prévus à la Loi sur l'accès pourraient nécessiter une réévaluation. Cependant, la prudence s'impose. Comme l'illustre la section 1.2.3.3.2, de nombreux facteurs entrent en ligne de compte concernant la capacité des organismes de respecter les délais. La Commission tient à ajouter quelques considérations importantes à ce propos.

Premièrement, les délais de traitement sont susceptibles d'être affectés par une myriade d'autres aspects de la Loi sur l'accès, dont plusieurs font l'objet de recommandations dans ce rapport. Ainsi, le respect des délais actuels pourrait être significativement facilité, notamment par :

- la modernisation du régime des restrictions au droit d'accès, évoquée à la section 1.2.1;
- une meilleure uniformité et une amélioration des pratiques de gestion de l'information, évoquée à la section 1.3.2;
- l'adoption d'un seuil d'effectifs affectés par les organismes publics au traitement des demandes d'accès, évoquée à la section 1.3.1;
- une place accrue pour la diffusion proactive, évoquée à la section 1.3.4;



- des données publiques, facilement accessibles, sur la performance des organismes publics en matière de traitement des demandes d'accès, évoquées à la section 1.4.

La réponse législative qui sera apportée quant à ces aspects pourra affecter la nécessité ou, le cas échéant, les modalités d'une révision des délais prévus dans la Loi sur l'accès.

Deuxièmement, à l'ère numérique, les systèmes et l'information se multiplient, mais les solutions aussi. Au-delà de l'amélioration de la gestion de l'information, le travail des praticiens en accès aux documents est susceptible d'être appuyé par de nouveaux outils, notamment appuyés sur l'IA. Certaines étapes, comme le repérage documentaire ou le prérepérage des renseignements confidentiels, pourraient potentiellement être facilitées par ces technologies. Sans s'y être penchée, la Commission note qu'au moins un organisme public québécois évalue un outil d'IA facilitant le masquage de certains renseignements protégés²⁴². Au palier fédéral, certains organismes ont envisagé des outils similaires²⁴³.

Troisièmement, les délais prévus dans la Loi sur l'accès, soit 20 jours initialement et une prolongation possible de 10 jours, ne concordent pas avec ceux prévus dans la LRSSS, également applicables aux organismes publics, ni avec ceux de la Loi sur le privé, établis à 30 jours sans possibilité d'extension²⁴⁴. Cependant, les régimes prévus dans ces deux autres lois concernent exclusivement l'accès aux renseignements personnels.

Quatrièmement, bien que les responsables de l'accès aux documents doivent disposer avec diligence des demandes d'accès, le délai maximal de base prévu par la Loi sur l'accès, en nombre de jours, constitue un message législatif très clair quant à la célérité attendue des organismes publics. Il ne peut être modifié à la légère.

Cinquièmement, plusieurs réformes en accès à l'information adoptées ou envisagées dans le reste du Canada concernent notamment la question des délais d'accès. Sur la base de certaines considérations semblables à celles évoquées à la section 1.2.3.3.2, en particulier en lien avec le volume des demandes, certaines provinces prévoient l'allongement des délais de traitement en jours civils²⁴⁵ ou un comptage des délais en jours ouvrables²⁴⁶. D'autres envisagent de permettre aux organismes publics de solliciter le

²⁴² Il s'agit du ministère de l'Emploi et de la Solidarité sociale; voir MINISTÈRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE, « Portrait public des utilisations de l'IA dans l'administration publique québécoise », *Données Québec* (2026), en ligne : <<https://www.donneesquebec.ca/recherche/dataset/portrait-public-des-utilisations-de-l-ia-dans-l-administration-publique-quebecoise>> (consulté le 25 mars 2026), projet numéro 2025061.

²⁴³ Voir notamment INNOVATION, SCIENCES ET DÉVELOPPEMENT ÉCONOMIQUE CANADA, « Caviardage automatisé d'enregistrements vidéo aux fins des demandes d'accès à l'information », *Canada.ca* (23 novembre 2020), en ligne : <<https://ised-isde.canada.ca/site/solutions-innovatrices-canada/fr/caviardage-automatise-denregistrements-video-aux-fins-demandes-dacces-linformation>> (consulté le 25 mars 2026); COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE, *L'état du système d'accès à l'information du Canada*, 2023, p. 51, en ligne : <<https://www.ourcommons.ca/documentviewer/fr/44-1/ETHI/rapport-9>>; interrogée dans le cadre des travaux ayant mené à la préparation de ce rapport, la commissaire fédérale à l'information a d'ailleurs recommandé que les institutions fédérales aient davantage recours aux nouvelles technologies en matière d'accès à l'information (p. 59).

²⁴⁴ Loi sur le privé, art. 32; LRSSS, art. 34.

²⁴⁵ Un récent projet de loi ontarien ferait passer ce délai initial de 30 jours civils à 45 jours ouvrables; voir l'annexe 7 dans : Peter BETHLENFALVY, *Loi de 2026 sur le plan pour protéger l'Ontario (mesures budgétaires)*, projet de loi n°97 (présenté en mars 2026), 44^e lég., 1^{re} sess. (Assemblée législative de l'Ontario), en ligne : <<https://www.ola.org/fr/affaires-legislatives/projets-loi/legislature-44/session-1/projet-loi-97>>; la réforme manitobaine, adoptée en 2021, a fait de même : Kelvin GOERTZEN, *The Freedom of Information and Protection of Privacy Amendment Act [Manitoba]*, projet de loi n°49 (sanctionné en mai 2021), 42^e lég., 3^e sess. (Assemblée législative du Manitoba), en ligne : <<https://web2.gov.mb.ca/bills/42-3/b049e.php>>.

²⁴⁶ C'est ce que prévoit la nouvelle loi albertaine : Dale NALLY, *Access to Information Act [Alberta]*, projet de loi n°34 (sanctionné en décembre 2024), 31^e lég., 1^{re} sess. (Assemblée législative de l'Alberta), en ligne : <<https://www.assembly.ab.ca/assembly-business/bills/bill?billinfo=12057&from=bills>>; la nouvelle loi néo-écossaise fait de même : Becky DRUHAN, *Freedom of*



consentement du demandeur pour allonger les délais²⁴⁷, ou ont augmenté les possibilités d'extension des délais²⁴⁸. Ces mesures ont fait l'objet de critiques de la société civile et, parfois, des homologues de la Commission²⁴⁹, compte tenu de l'importance de la célérité et de la perception que des gains demeurent possibles, notamment en matière de gestion de l'information²⁵⁰. Par ailleurs, leur caractère récent commande la prudence sur l'interprétation de leur effet sur les délais dans les provinces concernées. Il y aurait lieu de bénéficier des retours d'expérience de ces autres juridictions pour éclairer toute prise de décision éventuelle à ce sujet au Québec.

En 1981, le rapport final de la Commission Paré indiquait qu'une période initiale de 20 jours ne constituait pas une « contrainte déraisonnable » pour les organismes²⁵¹. On a jugé à l'époque que ce délai devait permettre, à une ère de documentation papier, de traiter la demande, de gérer les copies de documents, de préparer la décision et de l'envoyer par la poste. À l'évidence, de nombreux changements au contexte dans lequel œuvrent les organismes publics sont survenus depuis. Il reste difficile pour la Commission, à la lumière de ce qui précède, de statuer dès maintenant quant à la nécessité de revoir ce choix sans avoir creusé tous les volets de la question.

La réévaluation potentielle des délais prévus à la Loi sur l'accès exige beaucoup de circonspection. Si elle advenait, elle devrait viser un abaissement global du délai moyen de traitement. Ainsi, il importe de garder des délais aussi courts que possible pour garantir un accès rapide à l'information, tout en tenant compte du travail d'analyse des organismes publics et du contexte dans lequel il s'inscrit, puisque les difficultés vécues dans le traitement de certaines demandes peuvent entraîner des répercussions sur la célérité du traitement de l'ensemble d'entre elles.

Compte tenu de ce qui précède, la Commission estime qu'il y a lieu de confier à un groupe de travail, constitué de représentants de l'ensemble des parties prenantes, l'évaluation de la nécessité d'une révision des délais prévus à la Loi sur l'accès.

Information and Protection of Privacy Act [Nouvelle-Écosse], projet de loi n°150 (sanctionné en octobre 2025), 65^e lég., 1^{re} sess. (Assemblée législative de Nouvelle-Écosse), en ligne : <<https://nslslegislature.ca/legislative-business/bills-statutes/bills/assembly-65-session-1/bill-150>>; le projet de réforme ontarien va dans le même sens : *Loi de 2026 sur le plan pour protéger l'Ontario (mesures budgétaires)*, préc., note 245, annexe 7.

²⁴⁷ C'est ce qu'envisage la Colombie-Britannique : Diana GIBSON, *Freedom of Information and Protection of Privacy Amendment Act, 2026 [Colombie-Britannique]*, projet de loi n°9 (présenté - 26 février 2026), 43^e lég., 2^e sess. (Assemblée législative de la Colombie-Britannique), en ligne : <https://www.leg.bc.ca/parliamentary-business/overview/43rd-parliament/2nd-session/bills/1st_read/gov09-1.htm>.

²⁴⁸ *The Freedom of Information and Protection of Privacy Amendment Act [Manitoba]*, préc., note 245; *Access to Information Act [Alberta]*, préc., note 246; *Freedom of Information and Protection of Privacy Amendment Act, 2026 [Colombie-Britannique]*, préc., note 247; MINISTÈRE DES SERVICES AU PUBLIC ET AUX ENTREPRISES ET APPROVISIONNEMENT DE L'ONTARIO, « L'Ontario met à jour son cadre de cybersécurité, de protection de la vie privée et d'accès à l'information afin de s'harmoniser plus étroitement avec les administrations du Canada », *Ontario.ca* (13 mars 2026), en ligne : <<https://news.ontario.ca/fr/release/1007160/lontario-met-a-jour-son-cadre-de-cybersecurite-de-protection-de-la-vie-privee-et-dacces-a-linformation-afin-de-sharmoniser-plus-etroitement-avec-les-administrations-du-canada>> (consulté le 25 mars 2026).

²⁴⁹ Voir notamment, en Alberta : Diane McLEOD, *RE: Commissioner's comments and recommendations regarding Bill 34 – Access to Information Act*, Commissariat à l'information et à la protection de la vie privée de l'Alberta, 2024, en ligne : <https://oipc.ab.ca/wp-content/uploads/2024/11/20241120-Letter-to-Minister-Nally-regarding-Bill-34-the-Access-to-Information-Act-OIPC-comments-and-recommendations_Final-Unsigned.pdf>; au Manitoba : Jill PERRON, *Letter to Minister Goertzen on Bill 49 (FIPPA)*, Ombudsman du Manitoba, 2021, en ligne : <<https://www.ombudsman.mb.ca/wp-content/uploads/2025/03/bill-49-letter-to-minister-2021-04-14.pdf>>.

²⁵⁰ Voir par exemple BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, « 2026 Bill 9 Weakens Access in BC » (26 février 2026), en ligne : <<https://fipa.bc.ca/2026-bill-9-weakens-access-in-bc>> (consulté le 25 mars 2026).

²⁵¹ COMMISSION D'ÉTUDE SUR L'ACCÈS DU CITOYEN À L'INFORMATION GOUVERNEMENTALE ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, préc., note 1, p. 34.



Recommandation 13

Mandater un groupe de travail spécial, incluant notamment la Commission, des organismes publics et des représentants de la société civile, afin d'étudier l'opportunité de réviser les délais de traitement des demandes d'accès en tenant compte de l'équilibre devant être établi entre les attentes des demandeurs à l'information et la réalité opérationnelle des organismes publics dans le traitement effectif des demandes.

1.3. La culture des organismes en matière de transparence

1.3.1. Les ressources dévolues à l'accès à l'information

Sommaire

Le traitement diligent des demandes d'accès aux documents par les organismes publics est tributaire de l'expertise du responsable de l'accès et de son équipe ainsi que des ressources qui leur sont consenties.

Dans la présente section, la Commission s'intéresse :

- aux ressources allouées à l'accès à l'information par les organismes;
- à la formation dispensée aux responsables de l'accès et à leurs collaborateurs;
- à la communication entre les organismes et les demandeurs, plus particulièrement à la motivation des décisions rendues par les responsables.

Afin d'assurer des conditions propices au traitement efficace des demandes d'accès par les organismes publics, la Commission recommande de :

- prévoir des seuils quant aux ressources et à la formation du personnel dans la Loi sur l'accès;
- préciser les obligations relatives à la motivation des décisions rendues par le responsable de l'accès.

1.3.1.1. Contexte

Les organismes publics doivent se doter des moyens nécessaires au respect des obligations que leur impose la Loi sur l'accès. À ce titre, la Commission a pu constater, dans le cadre de ses affaires courantes ainsi que dans son étude *Avoir accès en temps utile*²⁵², des pratiques inégales de traitement des demandes d'accès. Selon elle, les disparités se manifestant entre les organismes publics tiennent en partie à l'attribution des ressources au sein des organismes et à l'expertise qu'ils parviennent à développer et à maintenir. Partant, elle estime que la Loi sur l'accès devrait être plus explicite au sujet de l'allocation suffisante par les organismes publics des ressources humaines, financières, matérielles et informationnelles suffisantes ainsi que sur la formation qu'ils doivent dispenser à leurs équipes.

²⁵² COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97.

1.3.1.2. Situation actuelle

La Loi sur l'accès prévoit que la personne ayant la plus haute autorité au sein d'un organisme public est responsable de l'accès aux documents²⁵³. Elle peut déléguer cette fonction, en tout ou en partie, à un membre de l'organisme public ou de son conseil d'administration, ou encore à un membre du personnel de direction, qui doit pouvoir les exercer de manière autonome²⁵⁴. Généralement, la fonction de responsable de l'accès est déléguée à un membre du personnel de direction de l'organisme, souvent un cadre d'une unité administrative offrant des services à l'ensemble de l'organisme, comme les affaires juridiques, les affaires institutionnelles ou le secrétariat général²⁵⁵.

Le responsable de l'accès aux documents doit traiter les demandes d'accès aux documents adressées à l'organisme public au sein duquel il exerce ses fonctions²⁵⁶. C'est à lui que reviennent les obligations en matière d'accès à l'information de l'organisme²⁵⁷. Le responsable est soutenu par un comité sur l'accès à l'information et la protection des renseignements personnels, qui se compose, outre les responsables de ces matières, toutes les personnes dont l'expertise est requise, notamment les responsables de la sécurité de l'information et de la gestion documentaire, le cas échéant²⁵⁸.

En pratique, selon la taille de l'organisme, le responsable est appuyé par une équipe de quelques employés. L'étude *Avoir accès en temps utile*, à l'occasion de laquelle la Commission a pris le pouls de 33 organismes de tailles et de fonctions variées, montre une composition médiane de trois employés pour ces équipes, ce qui représente généralement moins de 1 % des effectifs totaux des organismes concernés²⁵⁹. Elles sont rarement consacrées entièrement à l'accès, qui représente plutôt une tâche parmi d'autres pour chacun de leurs membres, y compris le responsable lui-même²⁶⁰. Dans les organismes de plus grande envergure, des répondants régionaux ou sectoriels sont aussi désignés²⁶¹.

La Loi sur l'accès prévoit que la personne ayant la plus haute autorité au sein de l'organisme veille à faciliter l'exercice des fonctions du responsable de l'accès²⁶². Cependant, elle ne prévoit aucune obligation relative aux ressources qui doivent être mises à la disposition du responsable ni à la formation du responsable, de ses collaborateurs, et, plus largement, de tout le personnel de l'organisme susceptible d'être impliqué dans le processus de traitement d'une demande d'accès. Cependant, le Règlement sur la diffusion exige des sous-ministres ou dirigeants des organismes publics, dans son champ d'application, qu'ils veillent à la sensibilisation et à la formation des membres du personnel et des membres du personnel de direction ou d'encadrement sur les obligations et les pratiques en matière d'accès à l'information²⁶³. Or, comme l'affirme la Commission à la section 1.3.4.3.1, ce règlement ne s'applique qu'à 7 % des organismes publics.

²⁵³ Il est important de souligner que la Loi sur l'accès prévoit deux responsables : le responsable de l'accès aux documents et le responsable de la protection des renseignements personnels. Même si ces rôles peuvent échoir à la même personne, la Loi sur l'accès les distingue. Le responsable de l'accès aux documents est celui visé dans la présente section, puisqu'il met en œuvre le droit d'accès aux documents de l'organisme au sein duquel il exerce ses fonctions (art. 42 à 52.1 de la Loi sur l'accès). Voir Loi sur l'accès, art. 8 al. 1.

²⁵⁴ *Id.*, art. 8 al. 2.

²⁵⁵ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97, p. 11, constat 3.

²⁵⁶ Loi sur l'accès, art. 42 à 52.1.

²⁵⁷ *Id.*, art. 8 al. 1.

²⁵⁸ *Id.*, art. 8.1.

²⁵⁹ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97, p. 13, constat 5.

²⁶⁰ *Id.*, p. 13.

²⁶¹ *Id.*, p. 12, constat 4.

²⁶² Loi sur l'accès, art. 8.

²⁶³ Règlement sur la diffusion, art. 2.

Par ailleurs, tel que le prévoit le Règlement sur la diffusion, le sous-ministre œuvrant pour le ministre responsable de l'application de la Loi sur l'accès a mis sur pied un réseau des responsables et un programme de formation en matière d'accès à l'information et de protection des renseignements personnels pour les responsables et pour les sous-ministres ainsi que les dirigeants des organismes publics²⁶⁴.

Le traitement complet et efficace d'une demande d'accès suit généralement un processus similaire, d'un organisme public à l'autre.

Réception de la demande : les demandes peuvent être formulées oralement ou par écrit. Un accusé de réception doit être envoyé au demandeur pour toute demande écrite²⁶⁵.

Analyse de la demande : les demandes sont généralement analysées par le personnel spécialisé, qui doit vérifier leur étendue²⁶⁶, leur complexité²⁶⁷ et leur recevabilité²⁶⁸. Dans certaines circonstances, le responsable de l'accès doit diriger le demandeur vers un autre organisme public²⁶⁹ ou, s'il y a lieu, prêter assistance au demandeur²⁷⁰.

Repérage des informations : les équipes d'accès à l'information doivent identifier les unités administratives pouvant détenir des documents visés par la demande et les solliciter. Des recherches sont faites dans les différents systèmes d'information et les archives. Tous les documents repérés doivent en principe être remis à l'équipe d'accès à l'information.

Analyse et application des restrictions : le personnel spécialisé de l'équipe d'accès à l'information analyse tous les documents repérés pour déterminer leur accessibilité. Cette analyse implique généralement l'évaluation de l'application des restrictions au droit d'accès obligatoires et facultatives, abordées dans la section 1.2.1, et le caviardage des passages visés par ces restrictions ou la mise de côté des documents entièrement inaccessibles. Le responsable de l'accès peut également devoir aviser des tiers pour obtenir leurs observations²⁷¹, ou aviser le demandeur d'une extension du délai de traitement, au besoin²⁷².

Transmission de la décision : une fois toutes les étapes précédentes complétées, le responsable de l'accès prépare une décision à adresser au demandeur. Dans cette décision, le responsable doit indiquer si l'accès est accordé en totalité, en partie, ou s'il est refusé, préciser les motifs de refus s'il y a lieu et inclure les documents transmis, le cas échéant²⁷³.

1.3.1.3. Enjeux

Dans le cours de ses activités, la Commission constate une variabilité des cultures et des pratiques en matière d'accès aux documents au sein des organismes publics, ce qui entraîne un traitement inégal des

²⁶⁴ *Id.*, art. 3.

²⁶⁵ Loi sur l'accès, art. 46.

²⁶⁶ Par exemple, une demande d'accès d'un citoyen peut avoir plusieurs volets qui viseront plusieurs types de documents, lesquels pourraient être détenus par plusieurs unités administratives de l'organisme.

²⁶⁷ Plusieurs unités administratives utilisant plusieurs systèmes différents sont susceptibles d'être impliquées dans le repérage.

²⁶⁸ Par exemple, une demande d'accès doit être suffisamment précise pour permettre de retrouver un document. Loi sur l'accès, art. 42 al. 1.

²⁶⁹ *Id.*, art. 48.

²⁷⁰ *Id.*, art. 42.

²⁷¹ *Id.*, art. 25 et 49.

²⁷² *Id.*, art. 47.

²⁷³ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97, p. 14 à 17.



demandes d'accès reçues d'un organisme à l'autre²⁷⁴. Certains organismes assurent un traitement diligent des demandes, alors que d'autres peinent à y répondre adéquatement et dans les délais impartis. La Commission estime que cette disparité relève de plusieurs facteurs, dont le flou entourant la formation nécessaire ainsi que les ressources qui doivent être investies par les organismes afin d'assurer un traitement efficace des demandes.

1.3.1.3.1. Les ressources dévolues aux équipes d'accès aux documents s'avèrent parfois insuffisantes

Le traitement diligent des demandes n'est possible que si le responsable et ses équipes disposent des ressources humaines, financières, matérielles et informationnelles suffisantes. C'est sur le plan de la quantité de personnel qualifié dévolue aux tâches de soutien au responsable que l'on constate les effets les plus tangibles sur la performance en matière de traitement des demandes d'accès²⁷⁵. Or, les enjeux liés aux effectifs sont précisément les plus répandus²⁷⁶. Depuis quelques années, les organismes publics rapportent un accroissement du volume et de la complexité des demandes d'accès, déjà évoqué dans la section 1.2.3. Cette hausse ne s'accompagne pas systématiquement d'une augmentation des effectifs²⁷⁷.

Le fait que les effectifs demeurent limités peut s'expliquer, d'une part, par les difficultés liées à l'embauche et à la rétention du personnel qualifié²⁷⁸. Il peut d'autre part découler, en contexte de restrictions budgétaires, de la tendance des organismes à retrancher d'abord dans les unités dédiées aux tâches administratives plutôt qu'aux unités opérationnelles.

À cet égard, la Commission souligne que l'accès à l'information est un droit essentiel à la préservation d'une saine démocratie.

Par conséquent, le traitement diligent des demandes d'accès des citoyens aux documents des organismes publics ne devrait faire l'objet d'aucun compromis.

Les organismes publics peuvent mutualiser le traitement des demandes d'accès et d'autres obligations imposées par la Loi sur l'accès par le biais d'ententes approuvées par la Commission²⁷⁹. Cette possibilité est peu exploitée : la Commission reçoit très peu d'ententes de mutualisation²⁸⁰. Elle constituerait pourtant un moyen de partage des responsabilités particulièrement intéressant pour les organismes plus modestes, à l'instar des petites municipalités, même si elle ne saurait être la solution à toutes les difficultés liées aux ressources imparties aux responsables de l'accès.

Les ressources matérielles, plus précisément technologiques, sont également un facteur important influençant les performances des équipes d'accès aux documents. En effet, l'adoption d'outils technologiques permettant un repérage efficace des documents n'est pas répandue de manière uniforme au sein des organismes publics. Leur absence peut allonger de manière considérable le repérage, voire

²⁷⁴ Il arrive que des demandes d'accès aux documents identiques soient adressées à plusieurs organismes simultanément. Ces occurrences en particulier permettent à la Commission de constater la variabilité dans les décisions et leurs motivations.

²⁷⁵ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97, p. 13 et 14.

²⁷⁶ *Id.*, p. 17.

²⁷⁷ *Id.*, p. 13.

²⁷⁸ Il s'agit d'un des principaux défis identifiés par les organismes interrogés par la Commission en 2022. Voir *Id.*, constat 13.

²⁷⁹ Loi sur l'accès, art. 172.

²⁸⁰ Plus précisément, elle en a reçu cinq dans les 12 dernières années.

l'empêcher²⁸¹. Une gestion inadéquate de l'information peut également créer un fardeau supplémentaire pour les unités administratives chargées du repérage²⁸². Ces questions sont explorées davantage dans la section 1.3.2.

1.3.1.3.2. La formation offerte par les organismes aux responsables de l'accès aux documents et à leurs équipes reste parfois insuffisante vu leurs responsabilités

Une offre de formation adéquate au personnel impliqué dans le traitement des demandes d'accès constitue un facteur déterminant pour le traitement diligent des demandes²⁸³. Or, la formation offerte aux équipes d'accès aux documents varie de manière importante d'un organisme public à l'autre. Cette variation a une incidence certaine sur l'expertise développée par le responsable de l'accès et ses collaborateurs et, en dernière instance, sur la qualité des décisions rendues.

1.3.1.3.3. La communication entre les organismes et les demandeurs n'est pas optimale

L'adoption de bonnes pratiques de communication est un autre aspect contributif au traitement diligent des demandes selon les organismes qui affichent de courts délais de traitement²⁸⁴. Notamment, une bonne communication avec les demandeurs, dès le début du traitement, et la transmission de décisions claires sont bénéfiques. À ce sujet, la Commission constate régulièrement que des décisions en réponse aux demandes d'accès ne sont pas adéquatement motivées et qu'elles ne comprennent pas les éléments qui les rendraient proprement compréhensibles par les demandeurs.

La Loi sur l'accès exige du responsable de l'accès qu'il motive tout refus de donner communication d'un renseignement et qu'il indique la disposition sur laquelle sa décision repose²⁸⁵. Toutefois, elle ne précise pas de manière détaillée la façon dont une décision doit être motivée.

En pratique, plusieurs responsables ne motivent leur décision que par l'énumération des dispositions invoquées en vrac. Cette approche laconique ne permet pas réellement aux demandeurs de comprendre la décision et d'en évaluer le bien-fondé. Cette situation entraîne plusieurs effets nuisibles à l'accès aux documents :

- Certaines demandes de révision à la Commission pourraient être évitées. En effet, un demandeur ayant accès à des motifs détaillés de décision peut mieux évaluer la possibilité d'en demander la révision.
- Cette latitude permet aux organismes publics de simplement refuser une demande d'accès en invoquant tous les articles susceptibles de s'appliquer.
- Elle ne permet pas à un demandeur de formuler une demande plus précise. Par exemple, si la quantité et la nature des documents visés sont incluses dans la décision, un demandeur pourra recommencer son processus en soulignant qu'il ne souhaite pas obtenir copie de certains documents, ou préciser autrement sa demande.

²⁸¹ Par exemple, il arrive que l'absence d'outils sophistiqués permettant l'interrogation des bases documentaires numériques des organismes soit mentionnée comme un facteur les empêchant de traiter efficacement les demandes, à moins que les demandeurs ne cherchent des documents reliés à des locutions exactes, qui peuvent être utilisées comme mots-clés de recherche.

²⁸² COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97, p. 15, 16 et 19.

²⁸³ *Id.*, p. 29 et 30.

²⁸⁴ *Id.*, p. 29, constat 24.

²⁸⁵ Loi sur l'accès, art. 50.

1.3.1.4. Recommandations

Afin d'améliorer et d'harmoniser les pratiques des organismes publics en matière d'accès aux documents, la Commission émet plusieurs recommandations concernant les ressources humaines, financières, matérielles et informationnelles consacrées à l'accès ainsi que les besoins des organismes en matière de formation. Elle estime que ces recommandations sont propices à l'instauration de cultures organisationnelles où l'accès à l'information est considéré à la hauteur de son importance.

De plus, la Commission estime opportun que la Loi sur l'accès soit modifiée afin d'y préciser des obligations relatives à la motivation des décisions rendues par les responsables de l'accès. Ces précisions devraient améliorer la compréhension des décisions par les demandeurs et contribuer à une communication efficace entre les demandeurs et les organisations.

1.3.1.4.1. Allouer des ressources suffisantes à l'accès et imposer des obligations en matière de formation

La Commission estime qu'il serait opportun que les organismes soient tenus d'ajuster les ressources imparties à l'accès à l'information en fonction du volume de demandes d'accès qu'ils reçoivent ordinairement. À cet effet, la moyenne mobile des demandes reçues, sur une période de trois ans par exemple, pourrait être utilisée afin de déterminer le nombre de ressources à consentir sans variabilité exagérée d'une année à l'autre. Les crédits et les effectifs consentis aux organismes pourraient être adaptés en conséquence.

Par ailleurs, les organismes qui faisaient meilleure figure lors de l'étude sur les délais de traitement menée par la Commission en 2022 identifiaient le maintien d'une expertise de pointe, à jour, ainsi que la sensibilisation des répondants des unités administratives détentrices de documents comme des facteurs importants de leur bonne performance²⁸⁶.

La Commission estime que la valorisation des meilleures pratiques actuelles en matière de formation pourrait permettre de rehausser le niveau de performance général des responsables d'accès et de leurs équipes. À cet effet, les obligations en matière de formation et de sensibilisation prévues au Règlement sur la diffusion devraient être intégrées directement à la Loi sur l'accès afin qu'elles s'appliquent à tous les organismes dans son champ d'application. Le Québec rejoindrait ainsi des juridictions performantes en matière de transparence et d'accès qui ont décidé de codifier une telle obligation²⁸⁷.

Au surplus, le contenu de la formation que doivent offrir les organismes à leur personnel pourrait être précisé : elle ne devrait pas se concentrer uniquement sur le processus de traitement d'une demande, mais aussi sur la rédaction de décisions adéquatement motivées, entre autres. Elle devrait aussi être offerte en temps opportun, compte tenu du roulement de personnel, et comprendre une formation continue, notamment sur l'évolution jurisprudentielle relative aux principes et aux restrictions prévus à la Loi sur l'accès. La Commission juge qu'elle devrait également intégrer une dimension de sensibilisation à l'importance du droit à l'accès et du devoir d'assistance à offrir au demandeur d'accès.

²⁸⁶ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97, p. 29, constat 24.

²⁸⁷ *Law on Free Access to Information of Public Importance [Serbie]*, préc., note 166, art. 35 et 42; *Ley General de Transparencia y Acceso a la Información Pública [Mexique]*, art. 24, 31 et 42, en ligne : <<https://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf>>.



La Commission souligne enfin l'importance, pour les organismes, d'adopter des politiques et des procédures visant à assurer un traitement uniforme, adéquat et diligent des demandes d'accès²⁸⁸. À cet effet, elle est d'avis que le rôle du comité sur l'accès à l'information et sur la protection des renseignements personnels devrait être clarifié dans la Loi sur l'accès afin de préciser qu'il est responsable de produire ces documents encadrants.

Recommandation 14

Prévoir à la Loi sur l'accès :

- un seuil minimal en matière d'allocation des ressources humaines et financières devant être dédiées aux tâches du responsable à l'accès aux documents;
- des obligations de formation initiale et continue du responsable de l'accès aux documents et du personnel qui le soutient, visant notamment des éléments de sensibilisation à l'importance du droit à l'accès et au devoir d'assistance envers le demandeur d'accès;
- des précisions quant au rôle et aux fonctions, en matière d'accès aux documents, du comité sur l'accès à l'information et la protection des renseignements personnels.

1.3.1.4.2. Préciser les obligations relatives à la motivation des décisions

La Commission estime qu'il serait opportun de renforcer l'obligation de motiver les décisions prises par les responsables de l'accès aux documents. Ceux-ci devraient avoir l'obligation de préciser :

- le nombre de documents auquel l'accès est refusé et leur nature;
- le motif de refus pour chaque document ou partie de document auquel l'accès est refusé, et non de manière globale en invoquant une seule fois les dispositions applicables;
- le ou les paragraphes de chaque restriction au droit d'accès invoquée.

Recommandation 15

Modifier l'article 50 de la Loi sur l'accès afin que les décisions rendues par les responsables de l'accès :

- précisent le nombre et la nature des documents auquel l'accès est refusé, sous réserve que ces informations révèlent des informations sujettes à des restrictions obligatoires à l'accès;
- précisent le motif de refus pour chaque document ou partie de document auquel l'accès est refusé;
- précisent les alinéas ou les paragraphes des articles invoqués pour motiver le refus;
- associent des motifs de refus précis à chaque catégorie de documents demandés.

²⁸⁸ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97, p. 14 et 19.



1.3.2. La gestion de l'information

Sommaire

La Commission constate que l'état actuel de la gestion de l'information au Québec constitue un frein important à l'accès à l'information. Le passage au numérique entraîne la création de plus d'informations que jamais, lesquelles sont mises à profit par les organismes publics – et constituent donc autant de documents visés par le droit d'accès. Face à cette nouvelle dynamique, la gestion de l'information accuse du retard.

Dans cette section, la Commission se penche sur les enjeux suivants :

- Les défis liés aux ressources et à la gouvernance en matière de gestion de l'information.
- Le décalage entre la Loi sur les archives et les pratiques actuelles.

Afin de résorber les effets de la gestion inadéquate de l'information pour les besoins de l'accès aux documents, la Commission recommande des modifications législatives visant une plus grande uniformisation des pratiques des organismes publics.

1.3.2.1. Contexte

La gestion de l'information est le socle de l'accès aux documents : on ne peut diffuser que ce que l'on peut organiser et retrouver. Les organismes publics doivent mettre de l'ordre dans la masse considérable de documents qu'ils détiennent, peu importe leur support, pour les classer, les tenir à jour et les repérer adéquatement au moment de traiter une demande d'accès. Cette association fondamentale explique l'adoption contemporaine de la Loi sur l'accès, en 1982, et de la *Loi sur les archives*²⁸⁹, en 1983²⁹⁰.

La Commission constate que les outils et les pratiques en gestion de l'information n'ont pas suivi le rythme des innovations technologiques au sein de l'appareil public québécois. Si des efforts importants de transformation numérique l'ont animé ces dernières années, ils n'ont pas toujours été accompagnés d'investissements et de réflexions à leur mesure en matière de gestion de l'information. Les organismes publics génèrent et exploitent des informations en quantité et en variété inégalées, mais leur capacité à les gérer est insuffisante, tant pour des motifs liés à l'évolution des technologies qu'à la gouvernance. Cette situation menace la célérité et la complétude du repérage documentaire, et, partant, le droit d'accès à l'information.

²⁸⁹ *Loi sur les archives*, RLRQ, c. A-21.1.

²⁹⁰ Diane BAILLARGEON et Vanessa LEJEUNE, « La révision de la Loi sur les archives », (2022) 50-2 *Archives* 5-56, p. 11, DOI : 10.7202/1098123ar.



1.3.2.2. Situation actuelle

Désireuse d'en tirer le plein potentiel pour décrire, comprendre et solutionner les problèmes qui l'intéressent, l'administration publique génère plus de documents et d'informations que jamais²⁹¹. Cette évolution s'explique par les possibilités accrues de quantification offertes par les technologies de l'information, mais aussi par l'intégration d'outils numériques à tous les aspects du travail. Les logiciels et les systèmes contemporains permettent aux fonctionnaires de créer quantité de documents, multipliant du fait même le nombre de « producteurs d'informations » au sein des organismes publics²⁹², en plus de générer eux-mêmes des données et métadonnées en grand volume. Les outils d'**IA**, entre autres, contribuent à créer toutes sortes de documents dont les organismes publics n'ont pas toujours conscience²⁹³.

Une simple séquence d'opérations, typique du travail dans l'administration publique, peut générer un grand volume d'informations et de documents de tous formats, distribués à travers différents outils et bases de données. Considérons la mise en situation suivante.

*Un gestionnaire donne une tâche de rédaction à un professionnel dans un outil de planification collaboratif. L'employé documente la tâche dans une liste de dossiers. Il envoie trois courriels à des collègues pour obtenir plus d'information; ceux-ci lui répondent dans une chaîne de courriels, chacun incluant l'ensemble des échanges précédents. Les collègues tiennent ensuite une réunion où chacun prend des notes et les sauvegarde. Une transcription automatisée est aussi préparée par **IA**, de même qu'un relevé de présences. Pour s'y retrouver quelques jours plus tard, le professionnel formule trois requêtes à un agent conversationnel interne pour extraire certaines informations des notes. Il crée un document et le partage à ses collaborateurs. Lorsque le premier jet est achevé, le professionnel invite ses collègues à relire et à commenter. Tous reçoivent des alertes successives par courriel lorsque des commentaires sont insérés. Chaque modification apportée crée une nouvelle version du document. Tout au long du dossier, le gestionnaire, le professionnel et les collaborateurs s'échangent des messages instantanés sur la tâche en cours.*

La répétition de cette situation des milliers de fois par jour, à l'échelle de tous les organismes publics, sans même considérer toutes les autres activités qui génèrent elles aussi des informations, illustre bien le phénomène de l'abondance informationnelle.

Il est plus aisé que jamais de produire de l'information, mais aussi de la conserver, du fait de son immatérialité relative. En effet, une quantité considérable de données peut être stockée en une fraction de l'espace qui était requis pour la détenir sur des supports physiques.

Cette révolution numérique des dernières décennies s'est accompagnée de nouvelles dispositions législatives visant à en gérer certains effets :

²⁹¹ Daniel J. CARON, *Transformation de l'administration publique vers le numérique et gestion documentaire: revue de la littérature et réflexion sur l'avenir*, Québec, Chaire de recherche en exploitation des ressources informationnelles de l'École nationale d'administration publique, 2021, p. 6, en ligne : <<https://espace.enap.ca/id/eprint/253/>>.

²⁹² *Id.*, p. 20.

²⁹³ *Id.*, p. 15.

- La *Loi concernant le cadre juridique des technologies de l'information*²⁹⁴, adoptée en 2001, concerne tous les documents, quel qu'en soit le support. Les organismes doivent notamment tenir compte, dans leurs pratiques, des obligations de cette loi en matière d'équivalence fonctionnelle et d'intégrité²⁹⁵.
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LGGRI), adoptée en 2011, puis modifiée entre autres en 2018, en 2021 et en 2023, a introduit la vaste notion de *ressources informationnelles*, qui appelle la gestion de l'information²⁹⁶. Cette loi confie entre autres d'importantes fonctions d'orientations au sous-ministre du ministère de la Cybersécurité et du Numérique, qui agit comme dirigeant principal de l'information, gestionnaire des données numériques gouvernementales, comme chef gouvernemental de la transformation numérique et comme chef gouvernemental de la sécurité de l'information²⁹⁷. Il peut notamment demander la diffusion de données ouvertes, et prescrit un modèle de classification de sécurité des données numériques gouvernementales²⁹⁸.

La LGGRI, en particulier, démontre aussi des attentes nouvelles envers les organismes publics en matière de conservation et de valorisation de la manne informationnelle introduite par le tournant numérique²⁹⁹ :

12.10 Les données numériques gouvernementales constituent un actif informationnel stratégique du patrimoine numérique gouvernemental. Leur mobilité et leur valorisation au sein de l'Administration publique à des fins administratives ou de services publics, en tenant compte de leur nature, de leurs caractéristiques et des règles d'accès et de protection qui autrement les régissent, sont d'intérêt gouvernemental. [...]

L'encadrement particulier de la gestion de l'information demeure, pour sa part, inchangé³⁰⁰. Le principal instrument législatif en la matière est la *Loi sur les archives*. Conjointement avec les politiques gouvernementales dont elle prévoit l'établissement³⁰¹, qui contiennent davantage de détails opérationnels³⁰², elle établit les attentes à l'égard des organismes publics. Ces attentes s'articulent notamment autour de deux outils importants, à savoir le plan de classification et le calendrier de conservation. Conjugués, ces outils prévoient des normes de conservation et de gestion applicables aux différents types de documents détenus par les organismes publics.

²⁹⁴ *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1 [ci-après LCCJTI].

²⁹⁵ D. BAILLARGEON et V. LEJEUNE, préc., note 290, p. 20.

²⁹⁶ Selon certains spécialistes en archivistique, les organismes publics ne font pas suffisamment ce lien et l'interprètent surtout comme un synonyme de « systèmes informatiques ». Voir *Id.*, p. 26.

²⁹⁷ *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, RLRQ, c. G-1.03, art. 7.1 [ci-après LGGRI].

²⁹⁸ Éric CAIRE, « Arrêté numéro 2024-05 du ministre de la Cybersécurité et du Numérique en date du 12 décembre 2024 concernant le Modèle de classification de sécurité des données numériques gouvernementales », dans *Gazette officielle du Québec*, 156^e année, numéro 52, Québec, Éditeur officiel du Québec, 2024, p. 7531-7545, en ligne : <https://www.cyber.gouv.qc.ca/publications/MCN-AN_2024-05.pdf>.

²⁹⁹ LGGRI, art. 12.10.

³⁰⁰ D. J. CARON, préc., note 291, p. 18-19; D. BAILLARGEON et V. LEJEUNE, préc., note 290, p. 18.

³⁰¹ *Loi sur les archives*, préc., note 289, art. 4 et 14.

³⁰² BIBLIOTHÈQUE ET ARCHIVES NATIONALES DU QUÉBEC, *Politique administrative concernant la gestion des documents actifs du gouvernement du Québec*, 1985, en ligne : <<https://www.banq.qc.ca/politique-administrative-concernant-la-gestion-des-documents-actifs-du-gouvernement-du-quebec/>> (consulté le 11 décembre 2025); BIBLIOTHÈQUE ET ARCHIVES NATIONALES DU QUÉBEC, *Politique administrative concernant la gestion des documents semi-actifs du gouvernement du Québec*, 1988, en ligne : <<https://www.banq.qc.ca/politique-administrative-concernant-la-gestion-des-documents-semi-actifs-du-gouvernement-du-quebec/>> (consulté le 11 décembre 2025); BIBLIOTHÈQUE ET ARCHIVES NATIONALES DU QUÉBEC, *Politique administrative concernant la gestion des documents inactifs des organismes publics*, 1991, en ligne : <<https://www.banq.qc.ca/politique-de-gestion-des-documents-inactifs-des-organismes-publics/>> (consulté le 11 décembre 2025).

En parallèle, la Loi sur l'accès établit clairement que chaque « organisme public doit classer ses documents de manière à en permettre le repérage », et ce, « pour faciliter l'exercice du droit d'accès »³⁰³. Pour ce faire, elle prescrit l'établissement d'une liste de classement des documents suffisamment précise pour faciliter l'exercice du droit d'accès. À cet égard, le plan de classification évoqué ci-haut tient lieu de liste de classement lorsqu'il existe.

1.3.2.3. Enjeux

La gestion de l'information au Québec se trouve entre modernité et désuétude. Les organismes publics, qui peinent déjà à se conformer au cadre actuel, doivent adopter de nouvelles pratiques pour se plier aux exigences du passage au numérique et de la valorisation de l'information. En bout de piste, la Commission est souvent amenée à constater des lacunes en matière de gestion et de repérage de l'information qui retardent ou empêchent l'accès à l'information.

1.3.2.3.1. La gestion de l'information est déjà en mauvais état

L'abondance informationnelle et la volonté de revaloriser l'information ajoutent de la pression à une gestion de l'information déjà fragilisée au sein de l'administration publique. Plusieurs études laissent voir un investissement insuffisant en ressources ainsi qu'une difficile évolution de la gouvernance pour tenir compte du numérique.

1.3.2.3.1.1. Peu de ressources sont historiquement affectées à la gestion de l'information

Les organismes publics sont tenus d'affecter « les ressources requises à la conception, au développement, à l'implantation, à la mise à jour et à l'évaluation d'un système de gestion des documents actifs » et « à l'application effective et efficace [de ce système] »³⁰⁴. Les statistiques les plus récentes que la Commission a pu retracer au sujet des ressources investies par les organismes publics en gestion de l'information laissent voir une réalité différente. Dans la foulée du précédent rapport quinquennal de la Commission, le désormais défunt Groupe d'expertise en gestion des documents au Gouvernement du Québec faisait état d'une diminution de 8 % de la quantité de personnel affecté à la gestion de l'information entre 2010 et 2017³⁰⁵. Dans son mémoire, ce groupe indiquait qu'en 2013, une ressource soutenait en moyenne 494 employés³⁰⁶. De plus, il déplorait que les fonctions de gestion de l'information soient souvent confiées à du personnel de bureau ou technique, non spécialisé et non dédié à ces tâches³⁰⁷. Un autre sondage mené en 2017 par l'Association des archivistes du Québec, Bibliothèque et Archives nationales du Québec (BAnQ) et le Réseau des services d'archives du Québec soulevait des inquiétudes sur l'état

³⁰³ Loi sur l'accès, art. 16 al. 1.

³⁰⁴ BIBLIOTHÈQUE ET ARCHIVES NATIONALES DU QUÉBEC, préc., note 302.

³⁰⁵ ASSEMBLÉE NATIONALE DU QUÉBEC, « Consultation générale et auditions publiques sur le rapport quinquennal 2016 intitulé « Rétablir l'équilibre – Rapport sur l'application de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de la Loi sur la protection des renseignements personnels dans le secteur privé » », dans *Journal des débats de la Commission des institutions*, 44-207, 2017, en ligne : <https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/ci-41-1/journal-debats/CI-170816.html#_Toc1382328> (consulté le 8 décembre 2025) à partir de 15 h 06.

³⁰⁶ GROUPE D'EXPERTISE EN GESTION DES DOCUMENTS AU GOUVERNEMENT DU QUÉBEC, *Consultation générale et auditions publiques sur le rapport quinquennal 2016 de la Commission d'accès à l'information intitulé « Rétablir l'équilibre » - Mémoire du Groupe d'Expertise en gestion des documents au gouvernement du Québec*, 2017, p. 5, en ligne : <https://www.bibliotheque.assnat.qc.ca/DepotNumerique_v2/AffichageFichier.aspx?id=183711>.

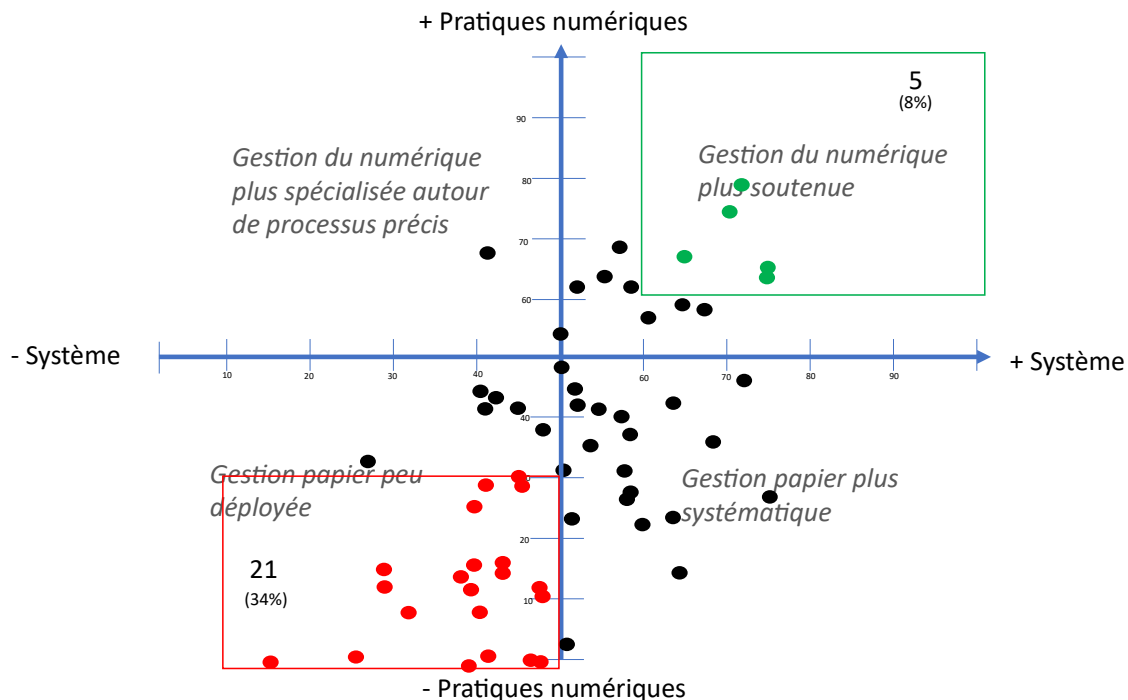
³⁰⁷ *Id.*; en 2025, la présidente de l'Association des archivistes du Québec indiquait que cette situation perdurait dans certains organismes publics : Étienne PARÉ, « La Loi sur les archives doit être revue, estiment des experts », *La Presse* (5 novembre 2025), en ligne : <<https://www.lapresse.ca/arts/2025-11-05/la-loi-sur-les-archives-doit-etre-revue-estiment-des-experts.php>> (consulté le 6 novembre 2025).

des ressources humaines affectées à la gestion de l'information, soulignant en particulier le fait que de nombreux ministères et organismes n'avaient affecté aucun cadre à cette fonction³⁰⁸. Bien que des modifications législatives pouvant justifier un réinvestissement en gestion de l'information aient été adoptées entre-temps, la Commission demeure préoccupée du peu de ressources historiquement consacrées à la fonction.

1.3.2.3.1.2. La gouvernance de l'information numérique accuse du retard

Des constats difficiles s'imposent également en ce qui a trait à la gouvernance. En 2020, une analyse économique des politiques informationnelles de divers organismes publics par le groupe de recherche CIRANO menait au constat que la plupart des politiques de gestion de l'information analysées se concentraient sur les documents physiques et qu'elles affichaient donc une certaine désuétude par rapport aux nouvelles pratiques informationnelles³⁰⁹. Dans la même veine, des données de BAnQ compilées en vue de son plan stratégique 2023-2027 révélaient que la plupart des organismes sondés concentraient encore leur gestion de l'information sur les formats physiques et que les pratiques étaient encore souvent peu systématisées. Ainsi, seuls 8 % des organismes faisaient une gestion plus soutenue des informations numériques, comme l'illustre le graphique suivant, préparé par BAnQ et reproduit avec son aimable autorisation³¹⁰.

Répartition d'un échantillon d'organismes publics en fonction de l'état de leur système de gestion de l'information et de leurs pratiques numériques



³⁰⁸ D. BAILLARGEON et V. LEJEUNE, préc., note 290, p. 17-18.

³⁰⁹ Daniel J. CARON, *Analyse économique des politiques informationnelles du gouvernement québécois*, rapport de projet 2020RP-01, CIRANO, 2020, p. 36-37, en ligne : <<https://cirano.qc.ca/files/publications/2020RP-01.pdf>>.

³¹⁰ BIBLIOTHÈQUE ET ARCHIVES NATIONALES DU QUÉBEC, *Répartition des organismes publics en fonction de l'état de leur système et leurs pratiques numériques*, 2021.

BAnQ a entrepris de suivre les progrès en gestion de l'information numérique des 23 ministères grâce à un indice de capacité, compilé à partir de six indicateurs relatifs à la gouvernance administrative et technologique. Au terme de l'année 2023-2024, cet indice s'établissait à 41 %, démontrant selon l'organisme que « la plupart des ministères ne disposent pas d'un diagnostic en gestion documentaire et archivistique leur permettant d'apporter les correctifs nécessaires, grâce à un plan d'action, pour répondre à leurs obligations en la matière »³¹¹. En particulier, seuls 28 % des ministères disposaient d'un plan d'action en gestion de l'information, 11 % d'un tableau de bord, et 39 % d'un logiciel de gestion de l'information numérique³¹². D'autres travaux nous apprennent en parallèle que la gestion de l'information est souvent traitée de manière décentralisée et diffuse au sein des organismes publics, ce qui aboutit à un casse-tête de documents de gestion et à une gouvernance moins intégrée³¹³.

BAnQ a mis en place plusieurs mesures d'accompagnement des ministères, et son indice de capacité en gestion de l'information est passé à 47 % en 2024-2025, l'objectif étant de 65 % en 2027³¹⁴. Malgré l'augmentation constatée, les chiffres dénotent toujours une capacité insuffisante à assurer la gestion de toute l'information détenue par les organismes. Il y a aussi lieu de croire qu'à travers l'ensemble des organismes publics, qui disposent généralement de ressources moins spécialisées que les ministères, la situation n'est guère plus rassurante, considérant qu'il existe une importante variation des pratiques entre organismes publics³¹⁵.

1.3.2.3.2. La gestion de l'information est prise entre modernité et désuétude

La gestion de l'information souffre à la fois des problèmes reliés à la dynamique nouvelle concernant les données et de l'absence de révision substantielle de la *Loi sur les archives* depuis son adoption, ce qui « concourt à compliquer l'arrimage entre les différentes exigences législatives³¹⁶ ».

1.3.2.3.2.1. L'abondance informationnelle génère de nouveaux enjeux

Le passage au numérique a provoqué une abondance informationnelle qui n'a pas été accompagnée par un souci proportionnel de documentation adéquate³¹⁷. Paradoxalement, les organismes publics possèdent davantage d'informations, au sujet desquelles ils en savent moins. De plus, bien que le régime en matière d'archives envisage un cycle de vie basé essentiellement sur l'âge de l'information en distinguant une phase active, semi-active et inactive, l'information a désormais pour vocation d'être revalorisée en continu, y compris pour des réanalyses rétrospectives, dans une certaine circularité. Certains parlent de gestion axée sur le flux d'information³¹⁸. Cette nouvelle approche secoue les fondements de la gestion de l'information telle qu'elle était envisagée traditionnellement, et telle qu'elle avait été étendue pour traiter également les documents électroniques, en tant que version dématérialisée de documents physiques³¹⁹.

³¹¹ BIBLIOTHÈQUE ET ARCHIVES NATIONALES DU QUÉBEC, *Rapport annuel de gestion 2023-2024*, 2024, p. 69, en ligne : <<https://numerique.banq.qc.ca/patrimoine/details/52327/4745473?docref=pNdHfrR1uQrCSfVGTpxuVw>>.

³¹² BIBLIOTHÈQUE ET ARCHIVES NATIONALES DU QUÉBEC, préc., note 310, p. 5.

³¹³ D. J. CARON, préc., note 291, p. 12.

³¹⁴ BIBLIOTHÈQUE ET ARCHIVES NATIONALES DU QUÉBEC, *Rapport annuel de gestion 2024-2025*, 2025, p. 44, en ligne : <<https://numerique.banq.qc.ca/patrimoine/details/52327/4745473>>.

³¹⁵ D. J. CARON, préc., note 291, p. 12.

³¹⁶ D. BAILLARGEON et V. LEJEUNE, préc., note 290, p. 18.

³¹⁷ D. J. CARON, préc., note 291, p. 15.

³¹⁸ Steve JACOB, Seima SOUSSI et Charlie MARTINEAU, *Intelligence artificielle et transformations des métiers de la gestion documentaire*, Chaire de recherche sur l'administration publique à l'ère numérique, 2022, p. 2, en ligne : <https://bibliopiaf.ebsi.umontreal.ca/bibliographie/8WWN5HAY/download/SDIBUXKJ/ia_et_metiers_de_la_gestion_documentaire.pdf>.

³¹⁹ D. J. CARON, préc., note 291, p. 18.

Ces nouveaux paramètres de la création et de la valorisation de l'information entraînent divers enjeux³²⁰, dont les suivants :

- La fragmentation et la modification permanentes des documents, ce qui soulève des difficultés pour assurer l'intégrité, la qualité et l'authenticité de l'information³²¹, de même que pour « reconstituer les étapes de l'élaboration d'un document, enjeu crucial [...] pour sa contextualisation et lisibilité institutionnelle, mais aussi [...] pour l'imputabilité de son ou ses créateurs³²² ».
- Les pratiques « personnelles et parallèles » de gestion de l'information à travers les outils collaboratifs, menant à une hétérogénéité dans le classement des documents entre employés et entre unités administratives d'un organisme et à l'échappement de certains documents à l'enregistrement institutionnel³²³.
- La gestion plus complexe de la sécurité des accès et de la protection des renseignements personnels.
- L'incertitude sur la manière dont doit se faire l'archivage ou le moment auquel il doit advenir.

Il s'ensuit une relative inadéquation des outils jusqu'ici fondamentaux de la gestion de l'information, tels que les plans de classification et les calendriers de conservation³²⁴. Le processus manuel d'évaluation, de sélection et d'examen des informations pour en déterminer la valeur s'effrite aussi³²⁵. De fait, on tend à se tourner vers des outils automatisés pour accomplir une partie de ces tâches³²⁶, ce qui n'est pas sans soulever des risques de destruction accidentelle de documents et de fuite de données confidentielles ou de renseignements personnels³²⁷. Ces initiatives rencontrent également des obstacles en raison de la forte variabilité des formats de l'information³²⁸.

1.3.2.3.2.2. La Loi sur les archives est en décalage

La *Loi sur les archives* n'a pas connu de modernisation substantielle depuis son adoption³²⁹. De même, les politiques qui en découlent n'ont pas été revues depuis plus de 30 ans.

Ces instruments ont été adoptés à une époque fondamentalement différente d'aujourd'hui en ce qui a trait au traitement de l'information. Puisqu'elle n'a pas été revue, la *Loi sur les archives* ne s'arrime pas aux pièces législatives connexes plus récentes, et elle n'en partage pas les tendances. Par exemple, elle n'attribue pas la responsabilité de la gestion de l'information à une personne désignée au sein de chaque organisme public, alors que la Loi sur l'accès prévoit des responsables de l'accès et de la protection des renseignements personnels et que la LGGRI confie à un dirigeant de l'information l'application des mesures en ressources informationnelles³³⁰. Par ailleurs, elle impose peu d'obligations substantielles aux organismes et repose surtout sur l'établissement d'un plan de classification et d'un calendrier de

³²⁰ *Id.*, p. 4.

³²¹ *Id.*, p. 16.

³²² *Id.*, p. 23.

³²³ Siham ALAOUI, « L'intelligence artificielle et la gestion documentaire : quels apports? Quels enjeux? », (2024) 46-2 *The Canadian Journal of Information and Library Science* 1-20, p. 2-3, DOI : 10.5206/cjils-rcsib.v46i2.16695.

³²⁴ D. J. CARON, préc., note 291, p. 16-17.

³²⁵ S. JACOB, S. SOUISSI et C. MARTINEAU, préc., note 318, p. 2.

³²⁶ *Id.*, p. 4 à 7; voir aussi le tableau de synthèse dans S. ALAOUI, préc., note 323, p. 9.

³²⁷ S. ALAOUI, préc., note 323, p. 9-10.

³²⁸ S. JACOB, S. SOUISSI et C. MARTINEAU, préc., note 318, p. 10.

³²⁹ BIBLIOTHÈQUE ET ARCHIVES NATIONALES DU QUÉBEC, « Une nouvelle Loi sur les archives pour le citoyen et pour l'État » (2024), en ligne : <<https://www.banq.qc.ca/notre-institution/archives-nationales/nouvelle-loi-sur-les-archives-pour-le-citoyen-et-pour-letat/>> (consulté le 8 décembre 2025).

³³⁰ Paradoxalement, la Loi sur l'accès fait directement référence à un « responsable de la gestion documentaire » au sein des organismes publics, lequel devrait siéger au comité sur l'accès à l'information et la protection des renseignements personnels. Voir la Loi sur l'accès, art. 8.1.



conservation – dont seule la constitution, et non l'application effective, est obligatoire³³¹. Ce décalage nuit fondamentalement à la mise en place généralisée d'une gestion de l'information efficace et en phase avec le contexte actuel.

1.3.2.3.3. L'état de la gestion de l'information nuit à l'accès à l'information

Les pratiques non optimales de gestion de l'information ont un sérieux effet sur le droit d'accès aux documents et le traitement des recours associés :

- Elles allongent le temps de traitement des demandes d'accès par les organismes publics³³², tant pour ce qui est du repérage que, dans le cas où on trouve trop d'information, pour ce qui est de l'analyse de l'accessibilité.
- Elles peuvent mener à la transmission d'informations incomplètes aux demandeurs parce que les documents pertinents n'ont pas été repérés, ou encore à la transmission de trop d'information, comme dans le cas de chaînes de courriels comprenant des cascades de doublons parce que chaque message reprend l'historique entier des échanges.
 - À cet égard, plus le volume de documents potentiellement pertinents repéré par les organismes publics est grand, plus ils sont susceptibles d'introduire un recours à la Commission afin de ne pas tenir compte d'une demande ou de la circonscrire³³³.

Ces effets sont régulièrement constatés par la Commission. Les recours en révision qu'elle examine impliquent souvent des enjeux de repérage complet et sérieux de l'information. Ce peut être le cas lorsque les recours font suite à une décision de l'organisme selon laquelle :

- tous les documents répondant à la demande d'accès ont été transmis;
- aucun document détenu ne répond à la demande : cas environ deux fois plus fréquent dans les demandes de révision.

Depuis une dizaine d'années, la proportion de ces recours s'établit à près de 25 % du nombre total de recours en révision en accès aux documents, comme l'illustre le tableau ci-dessous.

³³¹ D. BAILLARGEON et V. LEJEUNE, préc., note 290, p. 18.

³³² COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97, p. 16.

³³³ Loi sur l'accès, art. 137.1.

Évolution du nombre et de la proportion de tous les recours en révision en matière d'accès aux documents administratifs présentés à la Commission pouvant impliquer un enjeu de repérage

Indicateur	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	2021-2022	2022-2023	2023-2024	2024-2025	2025-2026 ³³⁴ (estimation)
Nombre de recours en accès aux documents administratifs impliquant un enjeu de repérage	182	285	241	258	257	253	318	280	292	319	394
Nombre total de recours en accès aux documents administratifs	1 128	1 239	961	1 027	1 091	1 058	1 220	1 115	1 277	1 365	1 548
Proportion impliquant un enjeu de repérage	16 %	23 %	25 %	25 %	24 %	24 %	26 %	25 %	23 %	23 %	25 %

Lorsque ces dossiers aboutissent devant la Commission, la question centrale est souvent de déterminer si l'organisme public a posé les actions nécessaires pour être en mesure de retrouver efficacement l'ensemble des documents visés par une demande d'accès aux documents parmi tous ceux qu'il détient.

À cet égard, la jurisprudence de la Commission démontre que les organismes invoquent régulièrement la complexité des méthodes de gestion de l'information, le classement déficient des documents ou encore des enjeux relatifs à la formation du personnel ou aux ressources humaines disponibles³³⁵ pour justifier le défaut de transmettre tous les documents pertinents ou leur demande de ne pas tenir compte des demandes d'accès³³⁶. Ces lacunes alléguées en matière de repérage et de gestion de l'information contraignent les membres de la Commission à ordonner aux organismes de se livrer à de nouvelles recherches. Comme ces derniers ont le devoir d'adopter et de classer leurs documents afin d'en permettre le repérage en vertu de la Loi sur l'accès, ils ne peuvent se soustraire à des demandes d'accès sous motif d'un manque de ressources ou de difficultés reliées à une gestion de l'information trop complexe.

Les nouvelles recherches effectuées par les organismes leur permettent souvent de retrouver davantage de documents pertinents, mais elles induisent des délais et des démarches supplémentaires qui grèvent l'exercice du droit d'accès. Lorsqu'elles ne sont pas concluantes, la Commission doit se fier à la preuve

³³⁴ Il s'agit d'une estimation, la compilation finale n'étant pas achevée à la date de finalisation de ce rapport.

³³⁵ Les décisions suivantes sont données à titre d'exemples de cette tendance : *Désabrais c. Municipalité de Grand-Remous*, 2019 QCCA 400, en ligne : <<https://canlii.ca/t/j47d8>>; *Tribunal administratif du logement c. Forest*, 2023 QCCA 298, en ligne : <<https://canlii.ca/t/k15wm>>; *Hénault c. Municipalité de Franklin*, 2024 QCCA 223, en ligne : <<https://canlii.ca/t/k6slp>>. Il faut aussi noter que des arguments similaires font surface du côté des entreprises privées lorsqu'elles sont impliquées dans des recours en examen de mécontentement concernant l'accès à des renseignements personnels. Ainsi, la déficience des pratiques de gestion documentaire n'est pas exclusive au secteur public.

³³⁶ Loi sur l'accès, art. 137.1.



présentée en audience. Or, il n'est pas exclu que les documents soient conservés de manière inadéquate, devenant ainsi « invisibles » pour l'organisme public.

1.3.2.4. Recommandation

Une meilleure gestion de l'information s'impose tant pour améliorer l'accès aux documents que pour des considérations de valorisation de l'information et même de protection des renseignements personnels. La Commission estime que des changements tant culturels que législatifs sont requis en réponse aux enjeux évoqués ci-haut.

Du côté culturel, les dirigeants d'organismes publics doivent veiller à renforcer et à harmoniser leurs pratiques de gestion de l'information en tenant compte des différents cadres légaux applicables et de l'évolution du monde de l'information. **La Commission les y invite dans le même esprit qu'elle le faisait en 2022 dans son étude sur les délais d'accès aux documents : « le leadership et l'engagement des dirigeants d'organismes sont essentiels pour favoriser le respect de la Loi sur l'accès. Ils devraient notamment s'assurer de déployer les outils et les ressources nécessaires³³⁷. »** La Commission revient sur ce thème dans la section 1.3.1.

Les organismes publics devraient également concevoir et respecter leur calendrier de conservation de façon à ne pas conserver d'informations sans réflexion préalable sur leur pertinence relative à leurs activités courantes ou au respect de leurs obligations légales. Ils doivent cependant documenter rigoureusement les informations qu'ils choisissent de garder, notamment pour en faciliter le repérage. Le recours à des professionnels compétents en matière de gestion de l'information semble incontournable. Enfin, les grands jalons mesurés par BANQ, comme l'adoption d'outils technologiques adaptés pour la gestion de l'information numérique et de politiques organisationnelles unifiées en la matière, doivent servir de guide aux organismes.

Du côté législatif, BANQ, qui voit à l'application de la *Loi sur les archives*, de même que plusieurs groupes³³⁸ plaident pour l'abrogation de cette loi. Ils estiment qu'elle doit être remplacée par un nouveau cadre qui consoliderait celui établi par la LGGRI, la LCCJTI et la Loi sur l'accès³³⁹. La désignation d'un responsable de la gestion de l'information, la modernisation du vocabulaire, la mise en place d'un cadre plus contraignant et celle d'autres mécanismes d'imputabilité figurent parmi les principaux changements demandés. Plusieurs acteurs espèrent aussi un rôle de normalisation et de surveillance plus actif pour BANQ³⁴⁰. À l'heure actuelle, cet organisme a surtout un pouvoir concernant les documents à valeur patrimoniale, prêts à l'archivage³⁴¹. Il ne peut véritablement intervenir concernant les pratiques de gestion de l'information activement utilisée au sein des ministères et organismes publics, lesquels jouissent d'une grande latitude dans leurs actions.

Quant à elle, la Commission juge essentiel d'imposer des standards aux organismes publics en matière de gestion de l'information afin de faire diminuer la variabilité des pratiques. Le modèle de classification des données numériques gouvernementales en lien avec la LGGRI est un bon exemple de la direction à emprunter. Sa mise en œuvre implique que les organismes publics connaissent bien les documents et les

³³⁷ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97, p. 32.

³³⁸ D. BAILLARGEON et V. LEJEUNE, préc., note 290; É. PARÉ, préc., note 307.

³³⁹ Anne MILOT, Martin LAVOIE et Hélène LAVERDURE, *Loi sur les archives - Une modernisation qui s'impose!*, Bibliothèque et Archives nationales du Québec, 2022, p. 2, en ligne : <https://www.banq.qc.ca/sites/default/files/2023-01/LoiSurLesArchives_Orientations_version%2Bcompl%C3%A8te%2B20200516.pdf>.

³⁴⁰ D. BAILLARGEON et V. LEJEUNE, préc., note 290, p. 35-43.

³⁴¹ *Id.*, p. 17.



données qu'ils possèdent pour être en mesure de leur attribuer un profil de mesures de sécurité ou un marquage, entre autres à des fins de protection des renseignements confidentiels et personnels. La Commission souhaite toutefois préciser que le marquage des données devrait s'accompagner d'une révision périodique, considérant que l'accessibilité à certaines informations peut varier en fonction du temps et des changements de contexte.

Recommandation 16

Assurer une uniformité en matière de gestion de l'information à l'échelle de l'administration publique par la modernisation de la *Loi sur les archives* ou, à défaut, par des modifications au cadre législatif en accès aux documents.

1.3.2.5. Pour aller plus loin

Le Québec n'est pas le seul État où des enjeux de repérage documentaire sont constatés par le milieu de l'accès à l'information. Un rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes du Canada sur l'état du système fédéral d'accès à l'information relève une situation analogue³⁴². De même, une récente étude d'une association œuvrant en accès à l'information menée auprès de ministères et organismes publics de la Colombie-Britannique montre que dans cette province aussi, la gestion de l'information est généralement décentralisée et les pratiques sont hautement variables entre organismes. Elle suggère aussi que si les documents liés aux missions fondamentales des organismes sont gérés suivant des processus relativement clairs, ceux relevant des obligations administratives générales ne le sont pas³⁴³.

Plusieurs fois au cours des dernières années, la Commission et ses homologues canadiens ont donc rappelé l'importance de la gestion de l'information comme fondation de la transparence.

³⁴² COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE, préc., note 243, p. 62-64.

³⁴³ Spencer IZEN, *Access Regimes 2025 Preliminary Report*, Freedom of Information and Privacy Association, 2025, p. 10-12, en ligne : <<https://fipa.bc.ca/aa/preliminary-report-2025/>>.



« [...] [L]'organisation et la conservation de cette documentation d'une manière qui permet d'y accéder rapidement sont au cœur des principes d'un gouvernement ouvert, transparent et responsable³⁴⁴. »

« À titre d'organisations offrant des services à la population, les institutions et organismes publics des quatre coins du pays ont la responsabilité essentielle de documenter leurs décisions et leurs actions, de gérer leurs documents de manière adéquate et efficiente, et de fournir l'information qui est dans l'intérêt public³⁴⁵. »

« Les autorités de contrôle [...] demandent également aux institutions et organismes publics de veiller à la consignation, à l'accessibilité et à l'intégrité des informations publiques et de renforcer la confiance du public par les moyens suivants : [...] Consigner les informations intégralement et avec exactitude, et les conserver de façon à en favoriser l'accessibilité en temps opportun et la transparence, en évitant des pratiques qui entravent la recherche d'informations comme l'emploi de mots codés et le stockage de documents sur différents systèmes officiels et personnels³⁴⁶. »

³⁴⁴ COMMISSAIRES ET OMBUDSMAN FÉDÉRAUX, PROVINCIAUX ET TERRITORIAUX À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE, *Renforcer le droit à la vie privée et à l'accès à l'information pendant et après une pandémie – Résolution des commissaires fédéraux, provinciaux et territoriaux à l'information et à la protection de la vie privée*, 2021, p. 3, en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-territoires/res_210602/> (consulté le 15 août 2022).

³⁴⁵ COMMISSAIRES À L'INFORMATION CANADIENS ET OMBUDS FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX, préc., note 112.

³⁴⁶ COMMISSAIRES ET OMBUDS FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX RESPONSABLES DE L'ACCÈS À L'INFORMATION, préc., note 14, recommandation 6.



1.3.3. L'absence d'une obligation de documenter

Sommaire

Le régime d'accès aux documents présuppose que les informations pertinentes sont adéquatement consignées et conservées par les organismes publics. Son efficacité est tributaire de l'existence de l'information.

Présentement, l'inexistence de documents liés à certaines décisions de l'administration publique entraîne le rejet de demandes d'accès. Une obligation générale de documenter, qui n'existe pas actuellement, contribuerait à assurer une meilleure transparence au Québec.

Dans cette section, la Commission :

- survole les causes de l'inexistence de documents alléguée par les organismes publics en réponse à certaines demandes d'accès;
- explore le problème de la documentation inconstante des décisions publiques tel que le mentionnent plusieurs acteurs en accès à l'information depuis plusieurs années.

Considérant que l'inexistence de documents demeure problématique, la Commission recommande :

- l'intégration d'une obligation générale de document au corpus législatif québécois;
- des sanctions en cas de non-conformité.

1.3.3.1. Contexte

Certaines décisions prises par les organismes publics sont inadéquatement documentées, en ce qui concerne tant le processus suivi que les éléments les ayant appuyées. Ce phénomène constitue une barrière à l'accès à l'information et partant, à l'imputabilité, à la participation citoyenne, à la confiance du public à l'endroit des institutions et à la lutte contre la désinformation qu'elle permet.

Pour le bien de la transparence, il importe que le secteur public veille à documenter les informations susceptibles d'avoir une importance saillante, notamment celles relatives aux décisions qui touchent directement des personnes ou qui ont une incidence sur les opérations gouvernementales. Les décisions, les actions et les politiques prises par les organismes publics devraient être dûment documentées, de même que les faits et les arguments invoqués pour les justifier.



1.3.3.2. Situation actuelle

La Loi sur l'accès prévoit un droit d'accès aux documents détenus par les organismes publics dans l'exercice de leurs fonctions³⁴⁷. Conséquemment, ce droit ne s'étend pas aux documents qui ne sont pas détenus, notamment s'ils n'existent pas. Les organismes publics ne sont pas tenus de créer un document pour donner suite à une demande d'accès, comme le reconnaît la jurisprudence de la Commission³⁴⁸.

Plusieurs lois québécoises ont pour effet, expressément ou indirectement, de contraindre les organisations publiques à créer des documents qui établissent la teneur de certaines ententes ou décisions. C'est le cas, par exemple, de la plupart des contrats établis par les ministères et organismes, qui, comme ils doivent être signés par des personnes habilitées, doivent être scellés par écrit³⁴⁹. Toutefois, il n'existe pas de régime imposant une obligation générale de documenter.

1.3.3.3. Enjeux

L'inexistence de documents est régulièrement invoquée dans les décisions en réponse aux demandes d'accès. Parmi les dossiers de cette nature soumis en révision à la Commission entre les exercices 2015-2016 et 2024-2025, les organismes publics ont affirmé dans 15,4 % des cas qu'il n'existait aucun document administratif visé par la demande.

Dans ces circonstances, sous réserve que l'organisme fasse la preuve qu'un exercice de repérage complet et sérieux n'a pas permis de repérer un document répondant à la demande d'accès, la Commission n'a d'autre choix que de rejeter les demandes de révision qui lui sont soumises. Comme mentionné précédemment, le droit d'accès ne s'étend pas aux documents inexistants, et la Commission ne peut en ordonner la création.

Par surcroît, si un organisme démontre, dans le cadre d'une demande de révision, avoir mené en vain un repérage complet et sérieux dans l'objectif de répondre à la demande d'accès, il revient au demandeur de soumettre des éléments concrets pouvant constituer un début de preuve relatif à l'existence du document recherché. Comme les personnes n'ont pas accès aux fins détails de la gestion de l'information des organismes publics, cet exercice peut s'avérer particulièrement complexe. Le défaut de créer les documents pertinents peut faire en sorte que les organismes publics échouent à leur devoir de transparence.

Parmi les facteurs pouvant être soulevés pour expliquer la fréquence à laquelle les organismes publics concluent qu'ils ne détiennent pas les documents demandés, la Commission note en particulier :

- **une culture de l'oralité** : l'accès à l'information peut en pâtir lorsque les échanges menant à des décisions sont menés de vive voix. Notamment, il est possible que les organismes publics prennent moins de temps pour documenter leurs processus décisionnels et les arguments considérés dans les contextes où le rythme du travail est soutenu.
- **le recours aux technologies de l'information et à de nouveaux canaux de communication** : l'utilisation des technologies de l'information peut entraîner des difficultés uniques en matière de gestion de l'information. Ainsi, le recours aux courriels et aux plateformes de messagerie instantanée,

³⁴⁷ Loi sur l'accès, art. 1 et 9.

³⁴⁸ Voir notamment les décisions *Walsh c. Commission d'accès à l'information*, [1990] C.A.I. 259 (C.Q.), *Antonius c. Hydro-Québec*, [1998] C.A.I. 531 (C.Q.) et *J. G. c. Ville de Montréal*, 2011 QCCA 235.

³⁴⁹ *Règlement sur la signature de certains actes, documents ou écrits émanant du Secrétariat du Conseil du trésor*, RLRQ, c. A-6.01, r. 8.



où les messages sont nombreux et d'ordinaire conservés moins longtemps, peut complexifier à la fois la reconstitution des échanges et la conservation des informations pertinentes. De plus, l'utilisation de canaux de communication autres que ceux fournis ou approuvés par les organismes, par exemple des courriels personnels ou des applications de messagerie cryptée, empêche les responsables de l'accès à l'information d'y avoir accès. Même les canaux officiels, mais perçus comme plus informels, tels que les messages textes échangés sur des appareils officiels, présentent le risque d'échapper aux mécanismes réguliers de gestion de l'information.

1.3.3.4. Recommandation

La Commission et ses homologues canadiens le soutiennent depuis de nombreuses années, comme en fait état la section 1.3.3.5 : la solution à mettre en place en réponse aux enjeux d'inexistence de documents est une obligation de documenter.

Cette obligation devrait être prévue à même la Loi sur l'accès étant donné son caractère prépondérant et sa portée. L'obligation devrait ensuite être précisée par des standards et des politiques qui permettent aux organismes gouvernementaux de cibler les informations devant être documentées en fonction de leurs activités, de leurs responsabilités en matière d'imputabilité et des attentes du public.

Puisqu'elle ne concernerait que les informations ayant une pertinence saillante, cette obligation ne devrait pas mener à imposer aux organismes publics le fardeau de la création toujours plus nombreuse de dossiers. Plutôt, elle ne devrait concerner que la création et la conservation d'informations pertinentes. En plus d'assurer leur existence, elle aurait le mérite de faire en sorte qu'elles soient aisément retraçables sous forme d'ensembles complets et cohérents, ce qui faciliterait d'autant plus l'exercice du droit d'accès à l'information.

Afin d'assurer que les organisations s'acquittent de cette nouvelle obligation, des sanctions devraient être prévues en cas de non-conformité. C'est ce que préconisait la Commission lors de son dernier rapport quinquennal³⁵⁰, de même qu'à l'occasion d'une déclaration commune sur le sujet avec ses homologues canadiens³⁵¹. À cet égard, l'omission de produire des documents conformément à l'obligation pourrait s'ajouter à la liste des infractions pénales concernant le refus ou l'entrave à l'accès aux documents ou aux renseignements accessibles en vertu de la Loi³⁵².

Recommandation 17

Intégrer à la Loi sur l'accès une disposition générale obligeant les organismes publics à documenter le processus menant à leurs décisions et à leurs actions importantes.

³⁵⁰ Rapport quinquennal 2016, recommandation 6.

³⁵¹ COMMISSAIRES À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Déclaration des commissaires à l'information et à la protection de la vie privée du Canada sur l'obligation de documenter », *Commissaire à l'information du Canada* (2016), en ligne : <<https://www.oic-ci.gc.ca/fr/declaration-des-commissaires-linformation-et-la-protection-de-la-vie-privee-du-canada-sur>> (consulté le 27 février 2026).

³⁵² Loi sur l'accès, art. 158.



1.3.3.5. Pour aller plus loin

L'inexistence de documents contenant des informations stratégiques sur les processus décisionnels publics n'est pas une problématique nouvelle ni propre au Québec. Elle est fréquemment soulevée par la Commission ainsi que ses homologues fédéral, provinciaux et territoriaux. À titre d'exemple, depuis la parution du dernier rapport quinquennal de la Commission, cinq déclarations communes, dont la dernière est aussi récente que novembre 2025, ont exhorté les gouvernements à imposer des obligations de documenter³⁵³.

« Les autorités de contrôle FPT en matière d'accès à l'information demandent à leurs gouvernements respectifs de favoriser un écosystème informationnel plus solide par les moyens suivants :

1. Moderniser les lois sur l'accès à l'information sur leur territoire de compétence, notamment en imposant expressément aux institutions et organismes publics l'obligation de documenter et en prévoyant des exigences minimales à respecter quant à la divulgation proactive d'informations et de documents au public³⁵⁴. »

À l'instar des autorités de contrôle responsables de l'accès à l'information, des comités parlementaires chargés de la révision des lois sur l'accès à l'information ont eux aussi cerné le problème dans les dernières années. Par exemple, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes recommandait, dans un rapport paru en juin 2023, que la *Loi sur l'accès à l'information* du Canada soit modifiée pour y intégrer une obligation de documenter assortie de sanctions appropriées en cas de non-respect³⁵⁵. Similairement, en Écosse, un rapport parlementaire de 2022 rappelait au gouvernement le caractère crucial de la documentation des informations pertinentes. Il estimait nécessaire que « le secteur public accorde beaucoup plus d'importance à la création adéquate de traces écrites, telles que les ébauches pertinentes, les notes de service, les courriels, les correspondances et les procès-verbaux, qui montrent comment les décisions clés ont été prises³⁵⁶ ».

Malgré les demandes répétées des autorités de contrôle canadiennes en accès à l'information, la Colombie-Britannique demeure la seule province canadienne ayant prévu une obligation générale de documenter à ce jour. Le *Information Management Act* prévoit que le responsable de la gestion

³⁵³ COMMISSAIRES À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 351; COMMISSAIRES ET OMBUDS À L'INFORMATION FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX, préc., note 112; COMMISSAIRES FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE, « Pour une législation efficace sur la protection des renseignements personnels et l'accès à l'information dans une société guidée par les données », *Commissariat à la protection de la vie privée du Canada* (6 novembre 2019), en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-territoires/res_191001/> (consulté le 11 mars 2025); COMMISSAIRES À L'INFORMATION CANADIENS ET OMBUDS FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX, préc., note 112; COMMISSAIRES ET OMBUDS FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX RESPONSABLES DE L'ACCÈS À L'INFORMATION, préc., note 14.

³⁵⁴ COMMISSAIRES ET OMBUDS FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX RESPONSABLES DE L'ACCÈS À L'INFORMATION, préc., note 14.

³⁵⁵ COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE, préc., note 243, recommandation 17.

³⁵⁶ PUBLIC AUDIT AND POST-LEGISLATIVE SCRUTINY COMMITTEE, *Post-legislative scrutiny: Freedom of Information (Scotland) Act 2002*, Parlement de l'Écosse, 2020, p. 5, en ligne : <<https://bprcdn.parliament.scot/published/PAPLS/2020/5/19/Post-legislative-scrutiny--Freedom-of-Information--Scotland--Act-2002/PAPLS052020R2.pdf>>, notre traduction.



documentaire d'une entité gouvernementale peut produire des directives et des lignes directrices concernant notamment la création de documents afin de conserver des traces des décisions qui ont été prises³⁵⁷. La voie empruntée par la Colombie-Britannique représente certes un pas en avant, mais comporte certaines contreparties. En effet, comme cette obligation n'est pas intégrée à la loi sur l'accès à l'information de la province, elle n'est pas soumise à l'examen d'une autorité de contrôle indépendante, et elle ne s'applique ni aux municipalités ni aux organismes publics locaux³⁵⁸. Au surplus, elle ne s'accompagne pas de seuils ou d'une liste précise des types de décisions qui doivent être documentées.

En dehors du Canada, des obligations similaires sont prévues aux États-Unis³⁵⁹, en Nouvelle-Zélande³⁶⁰, ainsi que dans plusieurs États australiens³⁶¹.

³⁵⁷ *Information Management Act [Colombie-Britannique]*, SBC 2015, c. 27, art. 6 et 19, en ligne : <<https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/15027>>.

³⁵⁸ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, *Duty to Document*, 2021, en ligne : <<https://www.infoandprivacy.ca/wp-content/uploads/2021/05/FIPA-on-Duty-to-Document-2021.pdf>> (consulté le 24 mars 2026).

³⁵⁹ *Records management by agency heads; general duties [États-Unis]*, 44 USC § 3101, art. 3101, en ligne : <<https://www.law.cornell.edu/uscode/text/44/3101>>.

³⁶⁰ *Public Records Act 2005 [Nouvelle-Zélande]*, 2005 n. 40, art. 17, en ligne : <<https://www.legislation.govt.nz/act/public/2005/40/en/latest/>>.

³⁶¹ *Public Records Act 1973 [Victoria]*, 8418/1973, art. 12, en ligne : <<https://content.legislation.vic.gov.au/sites/default/files/2025-02/73-8418aa043-authorized.pdf>>; *State Records Act 1998 [Nouvelle-Galles du Sud]*, art. 12, en ligne : <<https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1998-017>>.



1.3.4. La diffusion proactive

Sommaire

La diffusion proactive de documents et de données librement accessibles au public, en dehors du cadre formel d'une demande d'accès, contribue à une véritable transparence par défaut des activités de l'administration publique. Le Règlement sur la diffusion prévoit la mise en œuvre d'une diffusion standardisée. Mais plusieurs obstacles liés à la portée et aux modalités de ce règlement empêchent la diffusion proactive d'apporter tous les bénéfices escomptés au sein des organismes publics.

En parallèle, dans le contexte du déploiement accru de l'IA, le gouvernement a mis en place les premiers jalons d'une diffusion proactive concernant les systèmes d'IA dans le secteur public. Cette initiative prometteuse renferme un fort potentiel, mais des pas supplémentaires peuvent être faits pour une meilleure transparence, essentielle lorsqu'il s'agit d'IA.

Dans cette section, la Commission revient sur divers enjeux liés à la diffusion proactive en général, et à celle sur l'IA en tant qu'exemple particulier :

- Le Règlement sur la diffusion ne vise que peu d'organismes.
- Les pratiques de diffusion proactive manquent d'uniformité.
- La quantité et la variété d'informations rendues disponibles restent à parfaire.

Afin de renforcer la diffusion proactive au bénéfice de la transparence, la Commission recommande :

- d'étendre la portée du Règlement sur la diffusion;
- d'uniformiser les pratiques de diffusion et de créer un portail centralisé pour l'accès à l'information diffusée par les organismes publics;
- d'accroître la diffusion proactive en général, mais aussi en particulier en ce qui concerne le déploiement de l'IA;
- de formaliser la gouvernance de la diffusion proactive par les organismes.

1.3.4.1. Contexte

Il y a maintenant près de 20 ans que les dispositions régissant la diffusion proactive de documents ont fait leur entrée en droit québécois de l'accès à l'information. Les ministères et organismes gouvernementaux doivent publier automatiquement certains documents fondamentaux sur leur site Web. En parallèle, certains organismes diffusent de leur propre chef d'autres documents d'intérêt public, en plus de ceux dont la publication est formellement prescrite.



L'intention derrière la diffusion proactive est d'atténuer les obstacles associés à la transparence réactive, c'est-à-dire en réponse à une demande d'accès formelle, et de cheminer vers une véritable transparence par défaut³⁶² :

Plutôt que d'attendre la demande d'accès à un document, l'organisme devrait voir à la publication ou à la diffusion de l'information dès sa création. En fait, le principe général devrait être la publication automatique de l'information alors que la demande d'accès formulée auprès du responsable de l'accès deviendrait l'exception.

La diffusion proactive ne remplace pas la transparence réactive : cette dernière conserve toute sa pertinence pour les demandes plus précises ou circonstanciées, pour celles qui visent des dossiers actifs ou sensibles du gouvernement ou pour les demandes de complément d'information en lien avec des documents déjà diffusés. Malgré tout, l'approche proactive présente des avantages non négligeables :

- Pour les citoyens, le délai et les formalités administratives pour accéder à l'information diminuent nettement, ce qui renforce considérablement le droit d'accès.
- Pour les organismes publics, dans un contexte où le volume de demandes d'accès peut être important, la diffusion proactive peut offrir plus de prévisibilité du point de vue de l'utilisation des ressources :
 - Ils peuvent analyser l'accessibilité des documents d'une manière plus planifiée.
 - Le nombre de demandes d'accès reçues peut diminuer.
 - Pour les demandes restantes, le responsable peut rendre plus facilement sa décision en renvoyant aux documents déjà accessibles³⁶³.

En dépit de ses avantages, la Commission constate que la diffusion proactive est encore loin d'avoir atteint son plein potentiel. Le régime actuel, s'il constitue une bonne base, est nettement perfectible. Dans la foulée de la réforme de la Loi sur l'accès qui s'impose, la Commission estime qu'il faut aussi améliorer rapidement la diffusion proactive.

1.3.4.2. Situation actuelle

La Commission décrit ci-après les concepts auxquels elle fait référence dans la suite du texte, de même que le cadre légal actuellement applicable en matière de diffusion proactive au Québec. Elle présente aussi une initiative gouvernementale en matière de transparence de l'IA dans le secteur public.

1.3.4.2.1. Les concepts

Dans ce rapport, la Commission utilise le terme « diffusion proactive », au sens large, pour évoquer toute publication de documents et de données librement accessibles au public en dehors du cadre d'une réponse à une demande d'accès, que cette publication soit prescrite ou non par la Loi.

Selon cette vision, le terme englobe deux concepts différents :

- **La diffusion automatique**, qui concerne les documents et les renseignements dont le cadre réglementaire décrit ci-bas prescrit la diffusion.
- **La diffusion proactive au sens propre**, c'est-à-dire la publication, à l'initiative d'un organisme public, de documents et de renseignements supplémentaires à ceux dont la diffusion automatique est prévue.

³⁶² Rapport quinquennal 2002, p. 35.

³⁶³ Loi sur l'accès, art. 13.



Dans une vision large, il est également possible de rattacher le concept de la diffusion proactive à celui de la diffusion de données ouvertes, une approche qui consiste pour les organismes publics à rendre disponibles des jeux de données structurées documentant certaines des activités de l'appareil public. Il s'agit là, en revanche, d'une approche en général plus axée sur l'innovation que sur la reddition de comptes.

1.3.4.2.2. Le cadre légal

La Loi sur l'accès prévoit que les organismes publics diffusent sur leur site Web certains documents prévus par règlement³⁶⁴. Le gouvernement a ainsi adopté en 2008, et bonifié en 2015, le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*³⁶⁵. Celui-ci assujettit un peu moins de 200 organismes publics, soit les ministères et organismes gouvernementaux, à des obligations de diffusion automatique. Conséquemment, les organismes des catégories suivantes en sont actuellement exclus³⁶⁶ :

- Les organismes du secteur municipal, qui constituent près des trois quarts de l'ensemble des organismes soumis à la Loi sur l'accès.
- Les organismes du réseau de l'éducation et de l'enseignement supérieur.
- Les organismes du réseau de la santé et des services sociaux.
- Les ordres professionnels.

La mesure phare du Règlement sur la diffusion est l'obligation pour chaque organisme visé de publier jusqu'à 28 types de documents différents sur son site Web³⁶⁷, concernant :

- **l'organisme, sa structure et sa gouvernance** : organigramme, nom et titre des dirigeants et des cadres, nom et coordonnées du responsable de l'accès aux documents et de la protection des renseignements personnels, plan de classification, inventaire de fichiers de renseignements personnels, registre des communications de renseignements personnels sans consentement;
- **les dépenses de l'organisme** : renseignements relatifs aux engagements financiers, frais de déplacement, dépenses liées aux véhicules de fonction, contrats de publicité, de promotion, de formation et de télécommunication mobile, baux, indemnités, salaires et allocations annuels, subventions discrétionnaires des ministres, etc.;
- **le cadre légal, réglementaire et interne appliqué** : lois, règlements, politiques, directives, projets de règlement;
- **les services de l'organisme** : registres que l'organisme doit maintenir en vertu d'une loi, description de ses services et des programmes qu'il met en œuvre;
- **les autres documents d'intérêt public** : documents et décisions transmis dans le cadre d'une demande d'accès, documents transmis à l'Assemblée nationale (rapports annuels, plans stratégiques, mémoires...) et études, rapports de recherche et statistiques.

Des exceptions sont prévues pour les informations qui conserveraient un caractère confidentiel, notamment en vertu des restrictions obligatoires de la Loi sur l'accès, de celles liées à des tiers ou d'autres dispositions de confidentialité prévues dans une loi³⁶⁸. Les documents ci-haut doivent être diffusés avec diligence, parfois à l'intérieur de certains délais, dans une section dédiée à cette fin accessible à partir de

³⁶⁴ *Id.*, art. 16.1.

³⁶⁵ Règlement sur la diffusion.

³⁶⁶ *Id.*, art. 1.

³⁶⁷ *Id.*, art. 4.

³⁶⁸ *Id.*, art. 4 al. 1 par. 8 et al. 2.



la page d'accueil du site Web de l'organisme. Ils doivent demeurer en ligne tant qu'ils sont à jour ou jusqu'à ce qu'ils deviennent semi-actifs suivant le calendrier de conservation de l'organisme³⁶⁹.

Ni le Règlement sur la diffusion ni la Loi sur l'accès n'encadrent davantage la diffusion proactive d'autres documents, ses modalités étant donc laissées à la discrétion de chaque organisme.

1.3.4.2.3. Zoom sur le portrait de l'utilisation de l'IA

Parmi les initiatives de données ouvertes, la Commission souhaite attirer l'attention sur le portrait de l'IA dans l'administration publique, sur lequel elle reviendra ci-bas.

À la suite d'une recommandation du Conseil de l'Innovation du Québec allant en ce sens³⁷⁰, le gouvernement du Québec a pris un arrêté afin de mettre en place³⁷¹, tant « dans une perspective de transparence [que de gestion de la] cohérence de l'action gouvernementale en matière d'IA³⁷² », un mécanisme de recensement des systèmes d'IA utilisés par l'administration publique. Le ministère de la Cybersécurité et du Numérique (MCN) exige donc des organismes publics qu'ils déclarent, sur une base annuelle, leurs actifs informationnels et tout projet ou initiative en matière de ressources informationnelles visant l'utilisation de l'IA. Ces données servent à alimenter un portrait annualisé des utilisations de l'IA dans l'administration publique, dont les données brutes peuvent être consultées sur le portail Données Québec³⁷³.

1.3.4.3. Enjeux

La Commission considère que la diffusion proactive est une œuvre inachevée au Québec. Le Règlement sur la diffusion constitue un socle intéressant. Cependant, sa portée est trop limitée. Par ailleurs, les organismes qui y sont assujettis démontrent des pratiques variables et inégales notamment dans la présentation et la sélection des documents diffusés. La Commission remarque aussi que la transparence naissante autour du recours à l'IA par l'administration publique reste timide. Enfin, elle constate que la gouvernance de la diffusion proactive manque de formalisation.

1.3.4.3.1. La grande majorité des organismes publics ne sont pas soumis au Règlement sur la diffusion

Le Règlement sur la diffusion ne vise actuellement que les ministères et organismes du gouvernement, soit un peu moins de 200 organismes. La Loi sur l'accès, elle, en vise plus de 2 600.

Autrement dit, actuellement, seuls 7 % des organismes soumis à la Loi sur l'accès ont des obligations formelles de diffusion proactive.

Plusieurs des organismes assujettis au Règlement sur la diffusion exercent des fonctions importantes dont la portée est vaste au sein de l'administration publique. Néanmoins, des organismes dispensant des

³⁶⁹ *Id.*, art. 5.

³⁷⁰ CONSEIL DE L'INNOVATION DU QUÉBEC, *Prêt pour l'IA - Répondre au défi du développement et du déploiement responsables de l'IA au Québec*, 2024, p. 95, en ligne : <https://conseilinnovation.quebec/wp-content/uploads/2024/02/Rapport_IA_CIQ.pdf>, recommandation complémentaire 21.

³⁷¹ ÉRIC CAIRE, « Arrêté numéro 2024-01 du ministre de la Cybersécurité et du Numérique en date du 28 février 2024 - Exigences en matière de ressources informationnelles au regard de l'utilisation de l'intelligence artificielle par les organismes publics », dans *Gazette officielle du Québec*, 156^e année, n° 11, Québec, Éditeur officiel du Québec, 2024, p. 1355-1356, en ligne : <https://www.publicationsduquebec.gouv.qc.ca/fileadmin/gazette/pdf_encrypte/lois_reglements/2024F/82689.pdf>.

³⁷² MINISTÈRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE, préc., note 242.

³⁷³ *Id.*



services aussi essentiels que ceux en santé et services sociaux et en éducation ne sont pas visés. Ils gèrent pourtant d'importantes sommes publiques, emploient des centaines de milliers de personnes et exercent des activités d'intérêt public manifeste sur lesquelles la population est susceptible de vouloir en savoir davantage.

Quant aux ordres professionnels, ils sont partiellement assujettis à la Loi sur l'accès dans le cadre de leur rôle de contrôle de l'exercice d'une profession³⁷⁴. Les documents qu'ils détiennent en lien avec ce rôle sont visés par le droit d'accès, mais pas par des obligations de diffusion proactive.

Mais surtout, le secteur municipal est lui aussi exclu de la portée du Règlement sur la diffusion, alors que les organismes municipaux représentent près des trois quarts de l'ensemble de ceux soumis à la Loi sur l'accès.

C'est donc tout un palier de gouvernement qui échappe à ces règles, alors même qu'il administre des fonds publics et des questions de première importance pour les citoyens, et que la diffusion proactive faciliterait leur participation à la démocratie municipale.

« ATTENDU QUE les municipalités exercent des fonctions essentielles et offrent à leur population des services qui contribuent à maintenir un milieu de vie de qualité, sécuritaire et sain, notamment dans un contexte de développement durable, de réduction des émissions de gaz à effet de serre et d'adaptation aux changements climatiques;

ATTENDU QU'au sein des gouvernements de proximité, la participation et l'engagement des citoyens et des groupes qui les représentent, ainsi que l'accès à l'information, sont nécessaires pour définir une vision concertée du développement et assurer sa durabilité sur les plans environnemental, social et économique³⁷⁵; »

S'il est vrai que certaines grandes villes ont mis sur pied des initiatives de données ouvertes, le déficit de transparence – y compris proactive – du secteur municipal n'en reste pas moins majeur et préoccupant pour la Commission. L'intérêt des citoyens pour accéder aux documents appuyant les décisions et témoignant de la gestion des affaires municipales est patent : la Commission le constate à travers de nombreux recours en révision qui lui sont soumis.

Des lois municipales prévoient l'accessibilité sur demande de certaines informations et de certains documents municipaux³⁷⁶, pourvu qu'elles fassent partie des archives municipales : « Les dispositions où l'on utilise le terme "archives" dans les lois municipales ont pour objectif de permettre la participation citoyenne à la vie municipale, voire accroître la transparence au sein des organismes municipaux³⁷⁷. »

Au fil de son histoire, la Commission s'est souvent penchée sur la notion d' « archives municipales ». De nombreuses municipalités en font une interprétation restrictive, limitant la transparence. Par exemple, des conseils municipaux tiennent des séances décisionnelles à huis clos, estimant que les documents sur lesquels ils délibèrent à l'occasion de ces rencontres ne

³⁷⁴ Loi sur l'accès, art. 1.1; *Code des professions*, préc., note 49, art. 108.1.

³⁷⁵ Préambule de la *Loi visant principalement à reconnaître que les municipalités sont des gouvernements de proximité et à augmenter à ce titre leur autonomie et leurs pouvoirs*, LQ 2017, c. 13.

³⁷⁶ C'est notamment le cas pour les livres de comptes du greffier-trésorier, les pièces justificatives de ses dépenses et pour tout registre ou document faisant partie des archives de la municipalité. Voir notamment le *Code municipal du Québec*, RLRQ, c. C-27.1, art. 208 et 209; *Loi sur les cités et les villes*, RLRQ, c. C-19, art. 114.2.

³⁷⁷ Yvon DUPLESSIS et Jean HÉTU, *L'accès à l'information et la protection des renseignements personnels - Loi indexée, commentée et annotée*, MAJ 01/09/2018, Brossard, Québec, Wolters Kluwer Québec Ltée, 2018, par. 381.2.1.



font pas partie des archives municipales. Des décisions récentes de la Commission, qui ont dressé un tour d'horizon historique de la jurisprudence sur cette question, ont plutôt réitéré que tous les documents accessoires aux délibérations d'un conseil municipal constituent des documents d'archives de la municipalité et que les rencontres à huis clos ne sont pas prévues aux lois municipales³⁷⁸.

Il reste généralement nécessaire de formuler une demande pour accéder à ces documents. Une approche proactive éliminerait cette démarche dans un grand nombre de cas, améliorant la transparence municipale et facilitant le traitement des demandes d'accès par les municipalités³⁷⁹.

En somme, la portée limitée du Règlement sur la diffusion ne participe pas à établir une véritable culture de la transparence à l'échelle de toute l'administration publique. Rappelons que l'obligation de diffuser certains documents facilite certes l'accès des citoyens à ceux-ci, mais envoie également un message aux organismes visés quant à l'importance de la transparence et peut stimuler l'amélioration de nombreuses pratiques qui la favorisent, notamment en matière de gestion de l'information³⁸⁰.

1.3.4.3.2. Les pratiques de diffusion ne sont pas uniformes

La Commission constate un important manque d'uniformité dans l'application du Règlement sur la diffusion par les organismes publics, de même que certaines pratiques qui vont à l'encontre de l'esprit de la réglementation.

1.3.4.3.2.1. La section dédiée à la diffusion de l'information est souvent difficile d'accès

Contrairement à ce que prévoit le Règlement sur la diffusion, il n'existe aucune section dédiée à l'accès à l'information ou à la diffusion proactive sur le site de certains petits organismes publics qui y sont assujettis. Lorsque cette section existe, elle n'est pas toujours facilement repérable :

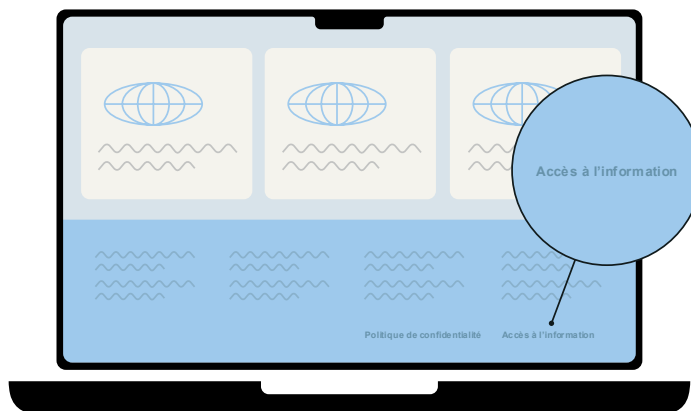
- Il devrait y avoir un lien sur lequel on peut cliquer directement à partir de la page d'accueil du site Web de l'organisme, mais ce n'est pas toujours le cas.
- Lorsque le lien est présent, il est souvent présenté dans le pied de page, en petits caractères, ce qui le rend peu visible. Il peut aussi être nécessaire, pour y accéder, de naviguer vers d'autres pages en effectuant plusieurs clics.
- Le lien s'intitule généralement « Accès à l'information » et peut renvoyer directement vers une section concernant la démarche formelle d'accès aux documents, comme expliqué ci-dessous.

³⁷⁸ *Clennett c. Ville de Gatineau*, 2025 QCCAI 302, par. 30 à 44, en ligne : <<https://canlii.ca/t/kfzzm>> (en appel devant la Cour du Québec; déclaration d'appel reçue le 5 novembre 2025, dossier n° 550-80-005960-253); *Gowling WLG c. Ville de Mascouche*, 2025 QCCAI 310, par. 54 à 71, en ligne : <<https://canlii.ca/t/kg2nz>>.

³⁷⁹ Voir notamment *Municipalité de Vaudreuil sur-le-Lac c. Lefebvre*, 2024 QCCAI 339, par. 61-62, en ligne : <<https://canlii.ca/t/k970g>>; dans cette affaire, la demande d'accès dont la municipalité demandait l'autorisation de ne pas tenir compte portait en partie sur des renseignements qu'elle diffusait normalement de manière proactive. La cessation momentanée de cette publication a forcé la municipalité à traiter une demande d'accès volumineuse, qu'elle aurait autrement pu éviter en redirigeant le citoyen vers des documents déjà accessibles.

³⁸⁰ La Commission aborde ce sujet plus en détail à la section 1.3.2.

L'illustration fictive suivante représente une situation typique en ce qui a trait à la visibilité du lien vers la section susceptible de contenir les documents diffusés proactivement.



1.3.4.3.2.2. Les documents peuvent être disséminés dans plusieurs sections

Les organismes visés consacrent souvent au moins deux sections distinctes à l'accès à l'information : l'une sur la procédure pour les demandes d'accès, et l'autre sur la diffusion proactive. Cependant, l'information est parfois disséminée dans un plus grand nombre de sections sans qu'un fil conducteur clair permette de s'y retrouver aisément. Il arrive qu'une partie des documents dont la diffusion automatique est prévue par le Règlement sur la diffusion soit présentée dans la section « Accès à l'information », et une autre dans la section « Diffusion de l'information ».

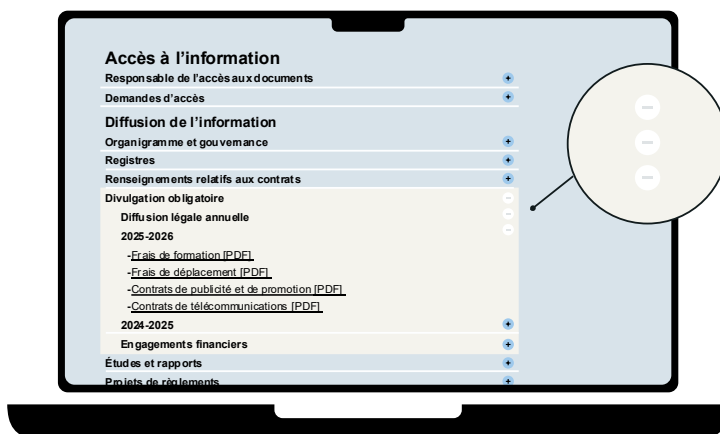
Plus concrètement, l'intégralité des documents dont la diffusion est prévue par le Règlement sur la diffusion est rarement recensée dans la section dédiée à la diffusion de l'information. Il n'est pas nécessaire que celle-ci soit l'unique « contenant » des documents visés par le Règlement sur la diffusion, lesquels peuvent être insérés à travers le site Web aux emplacements pertinents³⁸¹. **En revanche, elle devrait à tout le moins faire office de répertoire contenant au minimum des hyperliens directs vers les sections où on peut les consulter, et idéalement des hyperliens vers les documents eux-mêmes.**

1.3.4.3.2.3. Certains documents sont cachés derrière des catégories aux noms peu explicites

Les libellés utilisés pour classer les documents en catégories varient d'un organisme à l'autre. Par exemple, certains réunissent les « Frais et dépenses » sous un même titre au sein de leur section concernant la diffusion de l'information, alors que d'autres classent les informations financières dans des catégories beaucoup moins explicites, comme « Diffusion obligatoire », « Divulcation légale » ou « Autres documents ».

³⁸¹ Par exemple, l'organigramme pourrait être reproduit dans une section « À propos »; les lois et règlements, dans une section « Cadre légal et réglementaire ».

L'image fictive suivante représente un cas possible où il faut déplier plusieurs menus peu intuitifs pour parvenir aux informations financières.



1.3.4.3.2.4. Les documents déjà transmis à la suite d'une demande d'accès peuvent être difficilement repérables

La façon de présenter les documents transmis à la suite de demandes d'accès varie elle aussi substantiellement d'un organisme à l'autre.

Premièrement, si plusieurs organismes s'alignent sur les lignes directrices du Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité (SRIDAIL) et indiquent tant l'objet de la demande que ses dates de réception, de transmission et de diffusion³⁸², certains n'indiquent plutôt aucune date, voire aucun objet. Dans ce dernier cas, il est impossible de savoir ce que visait la demande sans télécharger les documents. Cette situation vide la diffusion de son sens : elle est censée permettre à d'autres personnes d'avoir accès à une information déjà jugée publique, laquelle doit pouvoir être retrouvée autrement que par hasard ou après de multiples essais.

³⁸² SECRÉTARIAT À L'ACCÈS À L'INFORMATION ET À LA RÉFORME DES INSTITUTIONS DÉMOCRATIQUES, *Lignes directrices de mise en application - Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*, 2015, p. 12, en ligne : <https://cdn-contenu.quebec.ca/cdn-contenu/adm/org/secretariat-institution-democratiques/acces-information/reglement-diffusion/Lignes_directrices_Application_2015.pdf>.

L'image fictive suivante illustre cette pratique.



Deuxièmement, les documents transmis à la suite d'une demande d'accès ne sont pas toujours classés de manière à en favoriser le repérage, par exemple en ordre antéchronologique ou année par année. Dans certains cas, il n'est possible d'afficher qu'un petit nombre de demandes par page sans devoir cliquer sur un bouton de chargement, ce qui empêche la recherche et le repérage. Il arrive même qu'un tableau recensant les demandes antérieures soit lui-même un document PDF contenant des liens vers les documents transmis. Ces mesures nuisent de manière importante à la facilité d'accès au contenu, un objectif pourtant fondamental de la diffusion proactive.

Troisièmement, certains organismes diffusent des décisions négatives par rapport à des demandes d'accès. Cette pratique ne s'aligne pas à l'esprit du Règlement sur la diffusion, et elle n'est pas utile : les personnes qui voudraient à l'avenir avoir accès à l'information demandée ne l'obtiennent pas davantage par cette diffusion.

Enfin, la fonction de recherche des sites Web permet rarement de repérer des documents au format PDF recensés dans la liste des documents transmis à la suite de demandes d'accès. Ces documents peuvent donc devenir difficiles à trouver sans connaître leur emplacement et, de manière générale, l'accès aux informations qu'ils contiennent s'en trouve compliqué.

1.3.4.3.3. La quantité et la variété de documents diffusés restent à parfaire

Malgré le Règlement sur la diffusion, plusieurs documents d'intérêt public restent dans les dossiers internes des organismes publics plutôt que d'être diffusés proactivement, ce qui freine le potentiel de cette pratique.

1.3.4.3.3.1. Le critère de « l'intérêt pour l'information du public » semble appliqué restrictivement

Le Règlement sur la diffusion prévoit la diffusion d'études et de rapports de recherches ou de statistiques, produits par l'organisme public ou pour son compte, « dont la diffusion présente un intérêt pour le public³⁸³ ». Il y a lieu de souligner leur faible nombre dans les faits : même pour des organismes aussi importants que des ministères, on en retrouve peu tant dans les sections dédiées à la diffusion de l'information que dans d'autres emplacements des sites Web. Ils sont pourtant parmi les seuls documents, dans la liste prévue par le Règlement sur la diffusion, qui portent plus directement sur la mission des

³⁸³ Règlement sur la diffusion, art. 4 par. 7.

organismes publics plutôt que sur leur structure ou leur administration générale. **Si la pertinence des informations liées à la performance de l'administration publique et à la reddition de comptes est évidente, il n'en reste pas moins que celles ayant trait aux activités fondamentales des organismes revêtent un intérêt tout particulier pour l'examen de l'action gouvernementale.**

1.3.4.3.3.2. Les périodes de disponibilité sont parfois très courtes

La période d'accessibilité des documents diffusés automatiquement varie considérablement d'un organisme à l'autre. Par exemple, certains publient les documents transmis à la suite de demandes d'accès depuis l'année 2015-2016, d'autres uniquement pour les deux derniers exercices financiers. Il en va de même pour les frais et dépenses : ces derniers sont même parfois accessibles uniquement pour l'année en cours.

La Commission reconnaît que le calendrier de conservation des organismes détermine la durée de maintien en ligne de ces informations³⁸⁴. Elle se questionne néanmoins sur des durées aussi courtes³⁸⁵.

1.3.4.3.3.3. Les données ouvertes et les tableaux de bord sont bénéfiques, mais ne suffisent pas à une vraie diffusion proactive

Peu d'organismes publics diffusent des documents au-delà de ceux dont la publication est prescrite par le Règlement sur la diffusion. Dans les dernières années, le gouvernement a plutôt concentré ses efforts de diffusion proactive sur la publication de jeux de données ouvertes sur la plateforme Données Québec³⁸⁶, qui en recense désormais plus de 1 500, suivant l'adoption d'instruments de politique sur la question³⁸⁷. Il a confirmé son intention de poursuivre son travail en ce sens dans sa *Stratégie gouvernementale de cybersécurité et du numérique 2024-2028*³⁸⁸.

La volonté d'augmenter la participation citoyenne et de « favoriser l'accès de l'information fiable »³⁸⁹ est certes louable. Néanmoins, la Commission rappelle que l'accroissement des données ouvertes ne suffit pas à atteindre tous les objectifs de la diffusion proactive. L'objectif poursuivi par l'ouverture des données est souvent davantage lié à l'innovation qu'à la reddition de comptes, bien qu'elle puisse avoir cet effet³⁹⁰ :

Cette approche consiste à diffuser des jeux de données permettant la diffusion du plus grand nombre de données en format ouvert afin de les réutiliser sans restriction, notamment dans le but d'encourager l'innovation, pour stimuler l'économie et simplifier leur

³⁸⁴ *Id.*, art. 5.

³⁸⁵ La durée de conservation de deux ans qui était auparavant la norme au fédéral a d'ailleurs été dénoncée par certains acteurs comme étant beaucoup trop courte; voir COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE, préc., note 243, p. 73.

³⁸⁶ DONNÉES QUÉBEC, « À propos », en ligne : <<https://www.donneesquebec.ca/a-propos/>> (consulté le 12 janvier 2026).

³⁸⁷ Voir notamment COMITÉ DE GOUVERNANCE EN RESSOURCES INFORMATIONNELLES, *Énoncé d'orientations pour les données ouvertes*, 2018, en ligne : <https://cdn-contenu.quebec.ca/cdn-contenu/gouvernement/SCT/vitrine_numeriQc/gouvernement_ouvert/orientations_donnees_ouvertes.pdf>; SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Guide de mise en oeuvre des énoncés d'orientations pour les données ouvertes*, 2018, en ligne : <https://cdn-contenu.quebec.ca/cdn-contenu/gouvernement/SCT/vitrine_numeriQc/gouvernement_ouvert/guide_mise_oeuvre.pdf>.

³⁸⁸ GOUVERNEMENT DU QUÉBEC, *Stratégie gouvernementale de cybersécurité et du numérique 2024-2028*, 2024, en ligne : <<https://www.quebec.ca/gouvernement/ministere/cybersecurite-numerique/publications/strategie-gouvernementale-cybersecurite-et-numerique-2024-2028>>, objectif 4.3.

³⁸⁹ *Id.*, objectif 4.3.

³⁹⁰ SECRÉTARIAT À LA RÉFORME DES INSTITUTIONS DÉMOCRATIQUES, À L'ACCÈS À L'INFORMATION ET À LA LAÏCITÉ, *Diffusion automatique et proactive*, s. d., en ligne : <https://cdn-contenu.quebec.ca/cdn-contenu/adm/org/secretariat-institution-democratiques/acces-information/reglement-diffusion/diffusion_auto-proactive.pdf>.



utilisation et le croisement de donnée[s] tout en protégeant le droit à la vie privée de la population visée

Corollairement, les données ouvertes ne rejoignent pas toute la population³⁹¹ :

[L]a compréhension, l'interprétation et l'utilisation des données ouvertes requièrent une certaine maîtrise des technologies de l'information. Le citoyen ou la citoyenne qui a un niveau de littératie peu élevé et qui ne maîtrise pas ces technologies ne peut être bénéficiaire direct de la divulgation des données ouvertes. Celles-ci ne bénéficieront alors qu'à une partie de la population, notamment les entreprises, les chercheurs et chercheuses, les journalistes experts ainsi que les développeurs et développeuses.

En parallèle, la Commission note la mise en ligne ces dernières années de divers tableaux de bord portant sur des fonctions gouvernementales importantes dans les dernières années : santé³⁹², éducation³⁹³, action climatique³⁹⁴, projets numériques³⁹⁵. Ceux-ci offrent un aperçu d'indicateurs clés relatifs à ces matières. L'intérêt de cette approche ne saurait être nié, mais certaines considérations s'imposent :

- Le choix des indicateurs est à la discrétion des organismes concernés. Ils peuvent fluctuer et être modifiés pour mettre plus ou moins de lumière sur certaines situations, possiblement en fonction d'angles politiques.
- La publication de données quantitatives ne donne qu'un aperçu partiel, peu contextualisé, des travaux de l'administration publique.

Les données ouvertes et les tableaux de bord, malgré leurs qualités, ne peuvent remplacer la diffusion proactive d'études, de rapports, de sommaires décisionnels et d'autres documents qualitatifs ou porteurs d'explications sur les opérations et les choix des organismes publics. La diffusion proactive demeure primordiale pour que la population puisse comprendre la logique de l'action gouvernementale et s'impliquer pour l'influencer.

1.3.4.3.3.4. Les systèmes d'IA sont trop peu documentés

La transparence figure à juste titre parmi les principes essentiels d'une grande majorité des cadres éthiques consacrés à l'IA³⁹⁶. Elle permet de favoriser la confiance des personnes et contribue à faire

³⁹¹ SECRÉTARIAT À L'ACCÈS À L'INFORMATION ET À LA RÉFORME DES INSTITUTIONS DÉMOCRATIQUES, *Orientations gouvernementales pour un gouvernement plus transparent, dans le respect du droit à la vie privée et la protection des renseignements personnels*, Québec, 2015 [ci-après *Orientations gouvernementales pour un gouvernement plus transparent*], p. 22, en ligne : <<https://numerique.banq.qc.ca/patrimoine/details/52327/2468038>>.

³⁹² SANTÉ QUÉBEC, « Tableau de bord – Performance du réseau de la santé et des services sociaux », en ligne : <<https://app.powerbi.com/view?r=eyJrJoiOGlyZWl4NGQtN2FjZC00OGFjLTgwMWYtZmM3N2M3ZjYyNjU2liwidCI6IjA2ZTFmZTI4LTVmOGltNDk3NS1iZjZjLWFmJmRiZTFhNzk5MiJ9>> (consulté le 22 février 2026).

³⁹³ GOUVERNEMENT DU QUÉBEC, « Tableau de bord de l'éducation », en ligne : <<https://app.powerbi.com/view?r=eyJrJoiODMzYTQyYTctNTc5S00YjMlWEZmWQYtYjhjOGUzYTM1MWFmliwidCI6IjJZThmYzE4LWE1YjAtNDhiYy05MjAwLTl4N2E4OTA2ODkwNCJ9>> (consulté le 15 octobre 2025).

³⁹⁴ GOUVERNEMENT DU QUÉBEC, « Tableau de bord de l'action climatique du gouvernement du Québec », en ligne : <<https://app.powerbi.com/view?r=eyJrJoiMzQyMTYzOGltNDMzNC00MmU5LWI2Y2YtMDQwYjU2OWI1YTQ1liwidCI6IjQyNjJkNGVjLTZhNjctNDk1Ny1hYmI2LWJmNzhhY2E2YTZmNSJ9>> (consulté le 15 octobre 2025).

³⁹⁵ GOUVERNEMENT DU QUÉBEC, « Tableau de bord des projets en ressources informationnelles du gouvernement du Québec », en ligne : <<https://www.tableaubordprojetsri.gouv.qc.ca/tableau-de-bord>> (consulté le 15 octobre 2025).

³⁹⁶ Par exemple, la transparence figure dans les principes avancés tant par l'OCDE que par le gouvernement du Québec : ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, « Recommandations du Conseil sur l'intelligence artificielle » (2 février 2024), en ligne : <<https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0449>> (consulté le 29 août 2024); MINISTÈRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE DU QUÉBEC, *Énoncé de principes pour une utilisation responsable de*



comprendre les pratiques. Les systèmes d'**IA** implantés dans le secteur public sont appelés à être des rouages essentiels de la réalisation des missions publiques, de l'administration de programmes à la prestation de services en passant par la prise de décisions partiellement ou entièrement automatisées concernant les administrés. **Dans ce contexte, il est essentiel que les organismes publics rendent compte de leur usage de l'IA. En effet, la publication de détails sur les systèmes d'IA déployés par l'administration publique permet à de nombreux acteurs, que ce soient les utilisateurs, des chercheurs ou des organisations, de s'impliquer dans le développement de la technologie et à d'autres, comme les régulateurs, les journalistes et les élus, d'assurer un contrôle sur les décisions algorithmiques**³⁹⁷.

Compte tenu de ce qui précède, la Commission salue la mise sur pied par le MCN d'un registre de données sur les systèmes d'**IA** envisagés ou déployés par les organismes publics. Il s'agit d'un pas dans la bonne direction pour rendre visible le recours à l'**IA**. L'initiative actuelle souffre toutefois de certaines limites.

Premièrement, le registre n'est édicté que par l'entremise d'un arrêté ministériel. Ce type d'instrument normatif n'atteint pas le degré de pérennité d'un règlement ou d'une loi. Ainsi, la mesure pourrait actuellement être aisément écartée par simple décision exécutive.

Deuxièmement, les données qui alimentent le registre ne doivent être communiquées qu'annuellement et non en continu. En ce sens, il s'agit d'un portrait – comme un cliché – des systèmes d'**IA** utilisés par l'administration publique à un moment dans le temps. En un an, de nombreux systèmes peuvent être mis en service, modifiés ou retirés, si bien que le portrait risque toujours d'être en décalage avec la réalité.

Troisièmement, le registre compte actuellement trop peu d'informations sur chaque système d'**IA** pour assurer un niveau significatif de transparence. Il documente sept métadonnées par système :

- Le portefeuille ministériel concerné.
- L'organisme public qui développe ou utilise le système.
- Le numéro du système, qui semble lié à une date.
- Le nom simplifié du système.
- Sa catégorie.
- Ses bénéfices attendus.
- Son statut, en développement ou en production.

Ainsi, le registre comporte une fonction de répertoire, mais chaque système n'est pas suffisamment documenté par son seul intermédiaire. Il n'existe actuellement aucune obligation de diffusion proactive qui enrichirait ce portrait du côté des organismes publics utilisateurs des systèmes. La section 1.3.4.5.2 ci-bas présente des exemples d'initiatives plus complètes concernant la transparence des systèmes d'**IA** publics.

l'intelligence artificielle par les organismes publics (édition 2025), 2025, en ligne : <https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/cybersecurite_numerique/Publications/Strategie_IA/Enonce_IA.pdf>.

³⁹⁷ Voir Justine BANULS, *La transparence des algorithmes publics*, Observatoire Data Publica, 2023, p. 47, en ligne : <<https://nextcloud.dataactivist.coop/s/tqos5ppqGeArDX/download/Cahier03-Transparence-algorithmique.pdf>>.



1.3.4.4. Recommandations

La Commission est convaincue que la diffusion proactive peut aller beaucoup plus loin au Québec, au service d'un accès à l'information plus fluide et d'une diminution du fardeau administratif lié au traitement des demandes d'accès par les organismes publics.

La Commission et ses homologues canadiens ont insisté sur ce principe dans diverses déclarations ces dernières années.

« La culture des institutions et organismes publics doit reposer sur le principe fondamental selon lequel les renseignements qu'ils détiennent appartiennent aux personnes au service desquelles ils travaillent et [...] ces renseignements devraient être accessibles par défaut, notamment au moyen d'une divulgation proactive [...]»³⁹⁸. »

« Dans [le contexte de la mésinformation], l'accès du public à des informations fiables revêt une importance primordiale. En visant la transparence et en publiant de façon proactive des informations exactes, les institutions publiques peuvent jouer un rôle essentiel pour renforcer notre écosystème informationnel, lutter contre la mésinformation, rehausser la confiance et préserver l'intégrité et la résilience des sociétés démocratiques»³⁹⁹. »

Les sous-ministres ou dirigeants d'organismes publics ont, selon le Règlement sur la diffusion, la responsabilité de s'assurer de sa mise en œuvre effective. Un leadership renforcé de leur part est une première condition essentielle à une meilleure diffusion proactive.

La Commission juge aussi que le cadre légal et réglementaire doit assurer une meilleure cohérence des pratiques et un accès facilité des citoyens aux documents publics. Le Règlement sur la diffusion demeure à ce jour un cadre robuste de formalisation de la diffusion automatique. Par rapport à l'approche de plusieurs provinces du Canada, il a l'avantage d'avoir un caractère contraignant et de prescrire une liste de documents à publier, plutôt que de se limiter à imposer aux organismes l'élaboration d'un plan de diffusion sans en déterminer le contenu minimal. Même s'il vise juste, ce cadre doit être bonifié.

Pour être pleinement efficace, la diffusion proactive doit être réfléchie et structurée de manière à assurer que l'information diffusée, en plus d'être pertinente, soit facilement accessible et pleinement compréhensible. Ainsi, pour que cette diffusion atteigne sa cible, les organismes publics doivent s'assurer que l'information diffusée le soit de manière à en maximiser le potentiel d'utilisation. Par exemple, elle devrait être bien catégorisée et consultable à l'aide d'un moteur de recherche convivial. Elle devrait également être adéquatement contextualisée pour être interprétable. Sur la base de telles conditions, le citoyen sera alors en mesure, de manière autonome, de trouver et de comprendre l'information qui l'intéresse. En matière de documentation, la qualité et la pertinence de l'information diffusée doivent primer sur la simple quantité. Il faut éviter que le volume d'information disponible ne devienne un obstacle au repérage de ce qui intéresse vraiment le citoyen.

1.3.4.4.1. Étendre la portée du Règlement sur la diffusion

Du moment que les organismes publics sont visés par la Loi sur l'accès, ils devraient aussi l'être par le Règlement sur la diffusion. La Commission, comme elle le demande depuis 2011⁴⁰⁰, juge urgent

³⁹⁸ COMMISSAIRES ET OMBUDS À L'INFORMATION FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX, préc., note 112.

³⁹⁹ COMMISSAIRES ET OMBUDS FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX RESPONSABLES DE L'ACCÈS À L'INFORMATION, préc., note 14.

⁴⁰⁰ Rapport quinquennal 2011, p. 60.



d'étendre sa portée afin qu'il vise aussi les organismes municipaux, les ordres professionnels⁴⁰¹ et les organismes du réseau de la santé et des services sociaux et du réseau de l'éducation et de l'enseignement supérieur. Ces organismes gèrent des fonds publics, sont des acteurs de premier plan dans la vie des citoyens et détiennent de nombreuses informations d'intérêt public dont l'accès devrait être grandement facilité. L'assujettissement de tous les organismes publics contribuera à diminuer le nombre global de demandes d'accès à l'information et, conséquemment, les délais de traitement.

Recommandation 18

Étendre la portée du Règlement sur la diffusion afin qu'il vise tous les organismes publics assujettis à la Loi sur l'accès.

1.3.4.4.2. Uniformiser les pratiques de diffusion automatique et créer un portail centralisé

Selon la Commission, l'uniformisation des pratiques de diffusion automatique doit être une priorité. Peu importe l'organisme public auquel il s'intéresse, chaque citoyen devrait pouvoir s'attendre à trouver les mêmes informations de base sous la même forme, entre autres pour pouvoir comparer les organismes. Il devrait aussi pouvoir aisément effectuer des recherches à travers cette documentation. La variabilité actuellement observée dans les pratiques empêche la réalisation de ces objectifs. Elle n'est acceptable ni pour le public ni pour les organismes. Il importe en effet que les ressources que ces derniers consacrent à l'application de leurs obligations de diffusion automatique aient pour effet de rendre les informations réellement accessibles.

Fondamentalement, pour la Commission, la clé de voûte de l'uniformisation et d'une meilleure accessibilité réside dans la création d'un portail centralisé réunissant tous les documents diffusés par les organismes publics québécois en application du Règlement sur la diffusion.

La centralisation de la diffusion des documents permettrait de réellement réunir, en un endroit, un bassin critique d'informations gouvernementales permettant aux citoyens d'examiner l'action des pouvoirs publics.

Un tel portail aurait d'ailleurs l'avantage majeur de permettre une recherche globale plutôt qu'organisme par organisme, ce qui représenterait un gain important en matière de transparence.

La Commission souligne que c'est déjà dans cet esprit qu'a été constitué le portail Données Québec, mais aussi un outil comme le Système électronique d'appel d'offres, qui prévoit une transparence concernant les contrats publics. Plusieurs exemples de portails mis en œuvre à l'extérieur du Québec, présentés dans la section 1.3.4.5.1, permettent de constater le bond en avant en matière d'accessibilité de l'information que génèrent ces initiatives.

D'autres idées porteuses pour uniformiser et améliorer les pratiques de diffusion ont déjà été formulées⁴⁰² et appuyées par la Commission⁴⁰³ dans le passé. Elles concernent notamment la standardisation des

⁴⁰¹ En ce qui concerne la part de leurs activités qui est soumise à la Loi sur l'accès.

⁴⁰² Voir les Orientations gouvernementales pour un gouvernement plus transparent, p. 23, 126-127, 130.

⁴⁰³ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 152, p. 9-10.



formats de diffusion, la tenue d'une liste à jour des documents diffusés et l'uniformisation des hyperliens qui, s'ils pointent vers des sites Web externes à ceux des organismes concernés, devraient mener directement vers les documents plutôt que vers des sections génériques. À cela, la Commission ajoute qu'il y aurait lieu de prescrire l'utilisation et la mise en évidence d'un pictogramme commun et d'un libellé unique pour permettre le repérage facile, sur la page d'accueil du site Web des organismes publics, de la section sur la diffusion proactive.

Recommandation 19

Créer un portail centralisé réunissant tous les documents diffusés par les organismes publics en vertu du Règlement sur la diffusion, mis à jour en continu et interrogeable par des fonctions de recherche.

Recommandation 20

Modifier le Règlement sur la diffusion de manière à uniformiser les pratiques de diffusion automatique, par exemple en :

- standardisant les formats de diffusion des documents et la structure de la section Web sur la diffusion de l'information;
- imposant l'utilisation d'un pictogramme et d'un libellé communs sur la page d'accueil du site Web des organismes publics pour rendre visible la section sur la diffusion de l'information;
- obligeant les organismes publics à tenir à jour, par l'entremise de cette section, une liste de tous les documents diffusés;
- exigeant que les hyperliens pointant vers des sites Web externes mènent directement vers les documents concernés plutôt que vers des sections génériques.

1.3.4.4.3. Accroître la diffusion automatique

La Commission estime également qu'il y a lieu d'accroître la diffusion automatique en ajoutant divers documents d'intérêt public à la liste contenue au Règlement sur la diffusion, d'une part, et en documentant davantage les systèmes d'**IA** utilisés par les organismes publics, de l'autre.

1.3.4.4.3.1. Bonifier la liste de documents contenue dans le Règlement sur la diffusion

Les catégories de documents à diffuser actuellement intégrées au Règlement sur la diffusion constituent un socle solide, mais la Commission croit qu'il y a lieu d'aller plus loin. Une majorité de documents pertinents devrait être diffusée par défaut, sans que le public ait à y demander formellement l'accès.



Différentes catégories de documents pourraient être ajoutées d'emblée au Règlement sur la diffusion, comme les suivantes, proposées en 2015 dans les *Orientations gouvernementales pour un gouvernement plus transparent*⁴⁰⁴ :

- Rapports de sondage.
- Rapports d'évaluation des programmes.
- Documents et rapports produits en lien avec des consultations publiques.
- Liste de comités ministériels, interministériels, de concertation, consultatifs ou de même nature, de même que leur composition.

En outre, afin de pérenniser la bonne pratique développée ces dernières années en matière de diffusion de documents importants comme l'agenda des ministres et de leurs rencontres avec des acteurs non gouvernementaux⁴⁰⁵, ou encore les dossiers soumis au Conseil des ministres⁴⁰⁶, la Commission préconise également de les ajouter à même le Règlement sur la diffusion.

Par ailleurs, les avis, recommandations et analyses, qu'ils émanent du personnel des organismes publics ou de tiers qui les produisent, font fréquemment l'objet de demandes d'accès. Les organismes pourraient avoir l'obligation de diffuser ces documents particulièrement pertinents à la compréhension des décisions de l'administration publique peu après que la décision finale a été rendue publique, sous réserve que leur diffusion n'engendre pas de préjudice démontrable⁴⁰⁷. Cette transparence par défaut permettrait de réduire de façon significative le nombre de demandes d'accès.

Enfin et de manière connexe, en lien avec le constat du faible nombre d'études, de rapports de recherche et de statistiques diffusés par les organismes publics, la Commission juge opportun de supprimer le critère subjectif actuel de « l'intérêt pour l'information du public », vu l'interprétation restrictive qui en est faite⁴⁰⁸.

Rappelons que le Règlement sur la diffusion prévoit que les documents soient mis en ligne « dans la mesure où ils sont accessibles en vertu de la loi »⁴⁰⁹, une balise qui continuerait d'être appliquée dans l'éventualité où ces ajouts étaient faits. C'est donc dire que l'analyse des restrictions de la Loi sur l'accès demeure effective.

En sus de ces catégories générales qui pourraient être intégrées à même le Règlement sur la diffusion, la Commission estime que chaque organisme devrait être tenu d'évaluer périodiquement les documents qui

⁴⁰⁴ Orientations gouvernementales pour un gouvernement plus transparent, p. 125.

⁴⁰⁵ GOUVERNEMENT DU QUÉBEC, « Agenda des membres du Conseil des ministres », *Québec.ca*, en ligne : <<https://www.quebec.ca/gouvernement/gouvernement-ouvert/transparence-performance/agenda-membres-conseil-ministres>> (consulté le 13 janvier 2026).

⁴⁰⁶ GOUVERNEMENT DU QUÉBEC, « Dossiers soumis au Conseil des ministres », *Québec.ca*, en ligne : <<https://www.quebec.ca/premier-ministre/equipe/conseil-des-ministres/memoires-conseil-ministres>> (consulté le 19 janvier 2026).

⁴⁰⁷ Comme le mentionne la Commission dans la section 1.2.1.4.2, toutes les restrictions au droit d'accès incluant celles concernant ces documents, prévues aux articles 37, 38 et 39 de la Loi sur l'accès, devraient être assorties de l'obligation de démontrer un préjudice. Cela laisserait aux organismes la possibilité, se présentant un tel préjudice, de ne pas diffuser les avis, recommandations ou analyses : en effet, le Règlement sur la diffusion prévoit déjà que la diffusion proactive concerne les documents dont il fait la liste « dans la mesure où ils sont accessibles en vertu de la loi ». Voir Règlement sur la diffusion, art. 4, al. 1.

⁴⁰⁸ Orientations gouvernementales pour un gouvernement plus transparent, p. 38-40 et 123-124.

⁴⁰⁹ Règlement sur la diffusion, art. 4.



devraient faire l'objet d'une diffusion proactive, en tenant compte entre autres du nombre de demandes d'accès les concernant⁴¹⁰ et des attentes des parties prenantes et du public.

La Commission est consciente que le défi consiste à trouver le juste équilibre avec l'extension de l'obligation de diffusion, afin de cibler les documents les plus pertinents sans noyer l'information intéressante dans une masse de documents. Pour ce motif, l'uniformisation de la présentation des documents et la création d'un portail centralisé, recommandées dans la section 1.3.4.4.2 ci-dessus, aideraient à mettre de l'ordre dans l'ensemble de ce qui est diffusé.

Recommandation 21

Étendre la liste de documents à diffuser automatiquement contenue au Règlement sur la diffusion en y ajoutant des catégories de documents telles que les suivantes :

- Rapports de sondage.
- Rapports d'évaluation des programmes.
- Documents et rapports produits en lien avec des consultations publiques.
- Liste de comités ministériels, interministériels, de concertation, consultatifs ou de même nature, de même que leur composition.
- Agenda des ministres, y compris leurs rencontres avec des acteurs non gouvernementaux.
- Partie accessible des dossiers soumis au Conseil des ministres.
- Avis, recommandations et analyses, après que la décision qu'ils appuient a été officiellement prise.

Recommandation 22

Retirer le critère subjectif de « l'intérêt pour l'information du public » du Règlement sur la diffusion en lien avec les études et les rapports de recherche ou de statistiques.

Recommandation 23

Exiger des organismes qu'ils évaluent périodiquement les autres documents qui devraient faire l'objet d'une diffusion proactive, par exemple en tenant compte du nombre de demandes d'accès les ayant visés.

⁴¹⁰ La Commission remarque par exemple que la loi américaine prévoit qu'un document dont l'accès a été demandé au moins trois fois devient automatiquement sujet à diffusion proactive: *Freedom of Information Act [États-Unis]*, 5 USC § 552, en ligne : <<https://www.law.cornell.edu/uscode/text/5/552>>.

1.3.4.4.3.2. Augmenter la transparence des systèmes d'IA utilisés dans le secteur public

Considérant la valeur centrale de la transparence en **IA**, la Commission estime qu'il y a lieu de codifier plus durablement la diffusion proactive au sujet des systèmes d'**IA** utilisés par l'administration publique, par un instrument normatif plus pérenne qu'un arrêté ministériel. Elle souligne que le Règlement sur la diffusion pourrait être un véhicule intéressant pour ce faire.

Une documentation plus complète sur chaque système d'**IA** devrait être diffusée proactivement, vu le fort potentiel d'incidence de ces systèmes sur la prestation des services publics. Ainsi, un examen rigoureux des utilisations de l'**IA** pourrait être effectué par des régulateurs ou encore par la société civile, entre autres en ce qui concerne la pertinence et l'efficacité des systèmes ou leur incidence sur les droits fondamentaux.

Plusieurs exemples de registres des algorithmes déjà en place ailleurs dans le monde, évoqués dans la section 1.3.4.5.2, peuvent servir d'inspiration concernant le contenu à diffuser sur chaque système d'**IA** en sus de ce que prévoit déjà la déclaration actuelle au MCN, par exemple :

- les finalités du système d'**IA**;
- la manière dont le système utilise les renseignements personnels, s'il y a lieu;
- les sources de données utilisées pour l'entraînement du modèle d'**IA** sous-jacent;
- des informations sur le type de système utilisé, l'architecture du modèle et les méthodes d'entraînement;
- des informations sur le traitement des données après la mise en service du système;
- des informations sur les risques anticipés et les mesures d'atténuation qui ont été prises, notamment en ce qui concerne la vie privée⁴¹¹, l'équité ou l'environnement;
- des informations concernant la performance du système pour les fins visées.

Dans tous les cas, il conviendrait de ne pas diffuser de renseignements concernant particulièrement les vulnérabilités et les mesures de sécurité des systèmes d'**IA**, de manière à ne pas causer d'incidents.

L'intégration de ces précisions au Règlement sur la diffusion permettrait, si les recommandations précédentes de la Commission sont appliquées, de réunir tous les renseignements sur les systèmes d'**IA** au sein du portail centralisé de transparence de l'administration publique. Dans tous les cas, il y a lieu de s'assurer que ces systèmes d'**IA** soient documentés au sein d'un véritable registre centralisé des algorithmes, mis à jour en continu. La présentation matérielle de ce registre devrait être adaptée aux besoins des différentes parties intéressées⁴¹², par exemple en proposant une forme claire et accessible pour les citoyens, ainsi que des données ouvertes pour les besoins des chercheurs.

⁴¹¹ À ce titre, précisons que la Directive sur la prise de décision automatisée du Canada demande que les EFVP des projets de systèmes d'IA soient publiées. Voir SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, « Directive sur la prise de décisions automatisée », *Canada.ca* (25 avril 2023), en ligne : <<https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=32592>> (consulté le 27 juin 2024).

⁴¹² PARTENARIAT MONDIAL EN INTELLIGENCE ARTIFICIELLE, *Algorithmic Transparency in the Public Sector - A state-of-the-art report of algorithmic transparency instruments*, 2024, p. 19-20, en ligne : <<https://wp.oecd.ai/app/uploads/2024/12/14-Algorithmic-Transparency-in-the-Public-Sector-A-state-of-the-art-report-of-algorithmic-transparency-instruments.pdf>>.



Recommandation 24

Poursuivre les efforts visant la transparence des systèmes d'IA utilisés dans le secteur public en codifiant dans une loi ou un règlement, par exemple dans le Règlement sur la diffusion, les informations devant être diffusées sur chaque système envisagé ou déployé par un organisme public et en garantissant la tenue d'un registre centralisé des algorithmes.

1.3.4.4.4. Formaliser la gouvernance de la diffusion proactive

Le Règlement sur la diffusion est avare de détails concernant divers aspects de la gouvernance de la diffusion proactive, notamment :

- la planification et la gestion de la diffusion proactive au sein de l'organisme;
- les responsabilités en cette matière dévolues au comité sur l'accès à l'information et la protection des renseignements personnels;
- la fréquence et les modalités de mise à jour des documents diffusés.

Ce manque de précision nuit à une réelle incarnation du principe de transparence dès la conception et par défaut, déjà préconisé par la Commission en 2002⁴¹³. Ce principe implique que les organismes publics tiennent compte de la diffusion proactive et de ses impératifs dès la création de documents institutionnels et prennent les mesures nécessaires pour que l'information qu'ils créent ou détiennent puisse, par défaut, être rendue publique. Autrement dit, il s'agit de mettre en place, d'emblée, les conditions permettant une diffusion plus aisée des documents une fois finalisés. De concert avec ses homologues canadiens, la Commission a présenté les mérites de cette approche dans une résolution de 2024, plaidant pour qu'elle devienne une nouvelle norme pour les services gouvernementaux⁴¹⁴.

« 3. La transparence devrait faire partie intégrante de la création et la gestion des nouveaux systèmes et processus administratifs, y compris veiller à ce que l'information critique soit facilement accessible par défaut, et que les données sensibles et non sensibles soient bien distinctes afin de faciliter la recherche d'information. Les Canadiens et Canadiennes doivent pouvoir avoir accès facilement à l'information produite ou gérée par les institutions et les organismes publics.

4. La transparence devrait faire partie des opérations quotidiennes des institutions et organismes publics – autant la collecte et la consignation d'information que le fait de donner accès à celle-ci proactivement ou sur demande. La transparence ferait ainsi partie intégrante de leurs activités quotidiennes à tous les échelons, de la haute direction aux services de première ligne⁴¹⁵. »

La Commission rappelle qu'une gestion en amont des considérations liées à la diffusion proactive serait gagnante tant pour la population que pour les organismes publics. L'administration publique serait d'emblée plus transparente, au bénéfice des citoyens. Les organismes publics traiteraient quant à eux la transparence dans le cours de leurs opérations quotidiennes, à travers tous leurs processus.

⁴¹³ Rapport quinquennal 2002, p. 35.

⁴¹⁴ COMMISSAIRES À L'INFORMATION CANADIENS ET OMBUDS FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX, préc., note 112.

⁴¹⁵ *Id.*



Actuellement, elle est parfois vue comme une obligation à rebours, les documents n'étant pas toujours élaborés dans l'idée qu'ils puissent faire l'objet d'une diffusion publique.

La Commission préconise ainsi une obligation d'adopter un plan de diffusion permettant d'organiser les activités de diffusion proactive de chaque organisme public, lequel pourrait comprendre entre autres :

- les rôles et responsabilités internes;
- les étapes de la diffusion proactive, en commençant par l'identification des documents à publier et en allant jusqu'à leur vérification pour retirer les renseignements dont la divulgation n'est pas permise par la loi;
- des mesures de révision périodique;
- des mesures pour la formation du personnel.

Recommandation 25

Énoncer, dans le Règlement sur la diffusion, le principe de la « transparence dès la conception et par défaut », notamment en introduisant une obligation d'adopter un plan de diffusion proactive.

1.3.4.5. Pour aller plus loin

La Commission présente ci-après quelques exemples intéressants en matière de diffusion proactive dans d'autres juridictions, tant en ce qui concerne les portails centralisés de transparence gouvernementale que les registres algorithmiques.

1.3.4.5.1. Les portails centralisés pour la transparence gouvernementale

Plusieurs juridictions ont mis en place des portails où ils centralisent différents documents que les organismes publics diffusent proactivement.

1.3.4.5.1.1. Le portail du Mexique

Au Mexique, la Plateforme nationale de transparence a été prévue comme infrastructure centrale pour la diffusion proactive et la gestion des demandes d'accès⁴¹⁶. C'est par son entremise que les organismes publics doivent publier et maintenir à jour, tous les trois mois, les informations dont la loi exige la diffusion, en intégrant les fichiers ou les liens correspondants. Les informations doivent être diffusées selon des formats harmonisés définis par le Système national de transparence. Ce mécanisme de coordination à l'échelle du Mexique réunit, de façon organisée, des institutions, des procédures, des outils et des politiques permettant de renforcer la reddition de comptes de l'État. Son rôle central est de coordonner et d'évaluer les actions de transparence et d'accès à l'information dans les trois niveaux de gouvernement⁴¹⁷, de manière à garantir leur fiabilité, leur exhaustivité, leur actualisation, leur accessibilité et leur vérifiabilité.

⁴¹⁶ SISTEMA NACIONAL DE TRANSPARENCIA, « Plataforma Nacional de Transparencia », en ligne : <https://www.plataformadetransparencia.org.mx> (consulté le 13 janvier 2026).

⁴¹⁷ *Ley General de Transparencia y Acceso a la Información Pública [Mexique]*, préc., note 287, art. 23 à 30.



La plateforme prévoit également des exigences en matière d'accessibilité des informations pour les personnes en situation de handicap et pour celles parlant des langues autochtones.

En outre, la plateforme constitue un guichet unique pour toutes les demandes d'accès, quel que soit le niveau de gouvernement. Les demandes peuvent être formulées par d'autres canaux, mais doivent tout de même y être recensées par les organismes publics⁴¹⁸.

Les demandes déjà traitées et les documents transmis par les organismes publics restent accessibles sur la plateforme et peuvent être explorés par un outil de recherche global.

1.3.4.5.1.2. Le portail de la Colombie-Britannique

Le portail de l'information ouverte de la Colombie-Britannique regroupe en un seul endroit les documents de différents types diffusés proactivement par près de 80 ministères et organismes, dont :

- les documents relatifs aux activités des élus et des hauts dirigeants, le matériel préparé à leur intention et les documents relatifs aux dépenses gouvernementales;
- les documents transmis à la suite de demandes d'accès, de même que les décisions anonymisées⁴¹⁹.

The screenshot displays the 'Search the Open Information Catalogue' interface. On the left, there are search filters including 'Sort: Most recent', 'Date range: Anytime', and 'Type: FOI Request'. The main search bar contains the query 'foi request'. The results section shows 'Found 10,000 results' and a list of documents. The first document is titled 'FOI Request - FOR-2024-41389' and includes details such as 'Type: FOI Request', 'Applicant Type: Business', 'Ministry: Ministry of Forests', 'Fees paid by applicant: \$0.00', and 'Publication Date: 2026-02-05'.

Les citoyens peuvent effectuer des recherches globales à travers toutes ces informations, y compris à l'aide de fonctions de recherche avancées, rendant l'information facilement accessible et interrogeable.

⁴¹⁸ *Id.*, art. 124-127.

⁴¹⁹ MINISTÈRE DES SERVICES AUX CITOYENS DE LA COLOMBIE-BRITANNIQUE, « Search the Open Information Catalogue », *Gov.bc.ca*, en ligne : <<https://www2.gov.bc.ca/gov/search?id=9199E7BC9682482EB9EA0B6D6B8D386C&q=ALL&tab=1&targetSource=selectedFacets>> (consulté le 10 février 2026). Pour la capture d'écran : Copyright © Province de la Colombie-Britannique. Tous droits réservés. Reproduit avec l'autorisation de la Province de la Colombie-Britannique.



1.3.4.5.1.3. Le portail du gouvernement du Canada

Le Portail du gouvernement ouvert du Canada réunit lui aussi, pour l'ensemble des ministères soumis à la Directive sur le gouvernement ouvert⁴²⁰ et des autres institutions fédérales qui choisissent de l'appliquer, tous les documents qui doivent être diffusés en vertu de cette directive, comme les frais et dépenses, les informations sur les contrats, les rapports et les trousseaux d'information destinées aux ministres⁴²¹. Le portail recense également les jeux de données ouvertes du gouvernement fédéral. Les métadonnées concernant les demandes d'accès traitées après le 1^{er} janvier 2020 sont listées sur le site, qui comporte des fonctions de recherche globale.

1.3.4.5.2. Des registres de systèmes d'IA prometteurs

Des registres et des standards de transparence relatifs à l'IA se sont progressivement développés dans le monde.

Par exemple, le Royaume-Uni s'est doté d'une norme de documentation algorithmique⁴²². Elle sert de socle au registre des systèmes d'IA⁴²³, lequel prévoit la diffusion proactive d'informations concernant jusqu'à 44 variables relatives :

- à l'identification du système d'IA;
- à l'organisation et aux personnes qui en sont responsables;
- à la description de sa raison d'être;
- au processus décisionnel au sein duquel il s'insère, en mentionnant l'implication d'êtres humains et les mécanismes de recours prévus;
- aux spécifications du système et du modèle sous-jacent;
- aux détails sur les données utilisées (sources, nettoyage, stockage, collecte, etc.);
- aux risques et aux évaluations d'impact.

Outre le modèle britannique, le Partenariat mondial en intelligence artificielle a identifié trois autres registres des algorithmes qui se distinguent par la variété d'informations qu'ils fournissent au sujet des systèmes d'IA, allant jusqu'à 46 points de données⁴²⁴. Ces éléments contribuent à l'explicabilité, à l'imputabilité et à la confiance publique en lien avec l'IA.

⁴²⁰ SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, « Directive sur le gouvernement ouvert », *Canada.ca* (8 octobre 2014), en ligne : <<https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=28108#appC>> (consulté le 13 janvier 2026).

⁴²¹ SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, « Divulgence proactive », *Canada.ca*, en ligne : <<http://ouvert.canada.ca/fr/divulgence-proactive>> (consulté le 13 janvier 2026).

⁴²² GOVERNMENT DIGITAL SERVICE OF THE DEPARTMENT FOR SCIENCE, INNOVATION AND TECHNOLOGY, « Algorithmic Transparency Recording Standard - guidance for public sector bodies », *GOV.UK* (8 mai 2025), en ligne : <<https://www.gov.uk/government/publications/guidance-for-organisations-using-the-algorithmic-transparency-recording-standard/algorithmic-transparency-recording-standard-guidance-for-public-sector-bodies>> (consulté le 12 mars 2026).

⁴²³ CABINET OFFICE, DEPARTMENT FOR SCIENCE, INNOVATION AND TECHNOLOGY, et GOVERNMENT DIGITAL SERVICE, « Find out how algorithmic tools are used in public organisations », *GOV.UK* (14 janvier 2026), en ligne : <<https://www.gov.uk/algorithmic-transparency-records>> (consulté le 12 mars 2026).

⁴²⁴ Il s'agit du Public Sector Tech Watch et du Selected AI cases in the public sector de la Commission européenne, du registre des systèmes de décisions automatisées du secteur public colombien, tenu par l'Université de Rosario, et du registre des algorithmes du secteur public du Royaume-Uni. Voir PARTENARIAT MONDIAL EN INTELLIGENCE ARTIFICIELLE, préc., note 412, p. 15.



Parmi les autres registres et normes de documentation dignes de mention, on retrouve l'initiative d'Eurocities⁴²⁵, les outils de la Commission européenne⁴²⁶, le registre en données ouvertes actuellement développé par le gouvernement canadien⁴²⁷ ou encore le registre des algorithmes néerlandais, qui se présente sous la forme d'un portail simple d'usage et qui recense et documente de manière synthétique plus de 1 300 systèmes d'IA à l'échelle des Pays-Bas.

La capture d'écran suivante donne un aperçu du registre néerlandais⁴²⁸.

The screenshot shows the 'The Algorithm Register' website. The header includes navigation links: Home, Algorithms, Organisations, Templates, and Dashboard. A language selector is set to English. Below the header, a search bar prompts users to 'Find one of the 1379 algorithms' with a search button. The main content area displays '1379 results found' with a pagination bar showing page 6 of 138. On the left, there are filters for 'Choose a organisation type' (Municipality: 848, Organizational unit: 131, Independent administrative body: 75) and 'Choose a organisation' (Dutch Tax and Customs: 67, Administration: 66, Municipality of Amsterdam: 66, Customs: 48). The main result is 'Automated license plate-based enforcement' by the 'Municipality of Amsterdam', with a description of environmental zones and a 'Read more' link. On the right, there are sections for 'Publication category' (Impactful algorithms), 'Impact assessment' (Privacy Quickscan, Privacy Statement), and 'Status' (In use). A footer note indicates the last change on 3rd of February 2026.

⁴²⁵ EUROCITIES, « Algorithmic Transparency Standard », *Algorithm Register*, en ligne : <<https://www.algorithmregister.org/>> (consulté le 1 mars 2024).

⁴²⁶ CENTRE COMMUN DE RECHERCHE DE LA COMMISSION EUROPÉENNE, « Selected AI cases in the public sector », *JRC Data Catalogue* (2026), en ligne : <https://ai-watch.ec.europa.eu/selected-ai-cases-public-sector_en> (consulté le 4 février 2026); COMMISSION EUROPÉENNE, « Public Sector Tech Watch », en ligne : <<https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch>> (consulté le 4 février 2026).

⁴²⁷ SECÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, « Registre de l'IA du gouvernement du Canada (produit minimum viable) », *Ouvert.canada.ca* (2026), en ligne : <<https://ouvert.canada.ca/data/fr/dataset/fcbc0200-79ba-4fa4-94a6-00e32facea6b>> (consulté le 4 février 2026).

⁴²⁸ GOUVERNEMENT DES PAYS-BAS, « The Algorithm Register of the Dutch government », *Overheid.nl*, en ligne : <<https://algoritmes.overheid.nl/en>> (consulté le 12 mars 2026).

1.4. Le portrait statistique du système d'accès à l'information

Sommaire

La Commission constate des contraintes limitant grandement l'utilisation et la valorisation des données émanant des redditions de compte en place en matière de demandes d'accès à l'information. Les données existantes ne permettent pas de tirer un portrait global de la situation et ne permettent pas d'émettre de constats chiffrés. Cette situation freine le développement possible d'outils de suivi efficaces et l'identification de pistes d'amélioration en ce domaine.

Dans cette section, la Commission :

- effectue un survol des sources de données existantes;
- souligne les principales contraintes intrinsèques de ces sources.

Considérant la situation préoccupante, la Commission, s'inspirant de solutions en place dans d'autres juridictions, recommande de renforcer la reddition de comptes en matière d'accès à l'information de manière à la rendre :

- plus complète;
- plus uniforme et plus précise;
- centralisée et transparente.

1.4.1. Contexte

À l'ère du numérique et de la valorisation des données, l'administration publique souhaite s'appuyer sur des données fiables afin de mieux mesurer l'efficacité de ses activités et de ses programmes, et de les améliorer en continu. Cette approche permet de faciliter la prise de décision, la détection d'anomalies et l'identification de la cause de certains problèmes, le tout au service d'une meilleure orientation des politiques publiques et des actions de surveillance de l'application des lois, mais aussi d'une plus grande efficacité des organismes.



Pourtant, au Québec, les redditions de compte actuelles en matière de demandes d'accès à l'information⁴²⁹ ne permettent pas une exploitation de données adéquate permettant d'établir un portrait global et fiable du traitement de ce type de demandes. Il est actuellement pratiquement impossible, sans efforts colossaux, d'émettre des constats chiffrés à ce sujet.

En matière de demandes d'accès à l'information, il n'existe pas de source de données centralisée facilement exploitable permettant d'avoir un portrait global de la situation qui pourrait permettre d'orienter les décisions ainsi que les actions de surveillance à ce sujet.

Alors que dans un État moderne, il devrait être relativement aisé d'obtenir des statistiques fiables permettant de répondre à des questions fondamentales sur l'efficacité du traitement opérationnel des demandes d'accès, il est actuellement difficile, voire impossible, d'obtenir des réponses à des questions telles que les suivantes :

- Comment évolue, d'année en année, le nombre de demandes d'accès à l'échelle de tout l'appareil public?
- Quel est le délai de traitement moyen des demandes d'accès? Comment se compare-t-il entre organismes publics? Quelle est son évolution?
- Quelles sont les restrictions à l'accès les plus souvent invoquées par les organismes?
- De quels types de demandeurs proviennent les demandes d'accès (citoyens, entreprises, journalistes, chercheurs, associations ou groupes, autres gouvernements)?
- Quelle est la répartition des demandes d'accès acceptées et refusées pour chaque organisme?
- Quelle proportion des demandes d'accès font-elles l'objet d'un recours en révision?
- Certains organismes présentent-ils une plus grande proportion de dossiers allant jusqu'en révision que d'autres?
- L'adoption de telle ou telle mesure législative ou administrative a-t-elle eu une incidence sur le nombre global de demandes d'accès reçues ou leur traitement?

Cette situation prive la Commission, le gouvernement et la société civile d'un regard global sur l'état du système d'accès à l'information, lequel est un pilier essentiel dans une société démocratique en santé dont le bon fonctionnement devrait faire l'objet d'outils de suivi adéquats. La Commission propose donc des changements législatifs pour réformer la reddition de compte actuelle afin de prévoir une compilation de données plus complète, plus uniforme, plus précise, centralisée et transparente. Une telle compilation de données viserait à soutenir et à orienter l'amélioration continue du système de traitement des demandes d'accès, à identifier les tendances et à améliorer les façons de faire en ce domaine. Le Québec peut s'inspirer de ce qui est mis en place dans plusieurs autres juridictions.

1.4.2. Situation actuelle

En vertu de la Loi sur l'accès, le traitement des demandes d'accès est un processus décentralisé. En effet, chaque organisme assujéti à cette loi est responsable du traitement des demandes d'accès qui lui sont adressées. La Commission est impliquée uniquement lorsque des parties demandent une révision à la

⁴²⁹ Dans le cadre de cette section, ce terme est utilisé pour englober à la fois les demandes d'accès aux documents administratifs (principalement) et les demandes d'accès aux renseignements personnels et de rectification de ceux-ci. Il importe de signaler que la présente section s'intéresse essentiellement aux données portant sur le traitement des demandes d'accès à l'information dans le secteur public.



suite du traitement par l'organisme. Pour avoir un portrait global exploitable de la manière dont l'ensemble de ces traitements se font, il faut donc colliger les données de base auprès d'une multitude d'acteurs éparés.

Malgré un intérêt soutenu pour ce genre de portrait de la part du gouvernement, de la Commission et de la société civile, dont font partie les journalistes et les chercheurs, il n'existe pas encore à ce jour de banque de données centralisée répondant à ce besoin.

Pour l'instant, la Commission identifie quatre sources de données sur l'accès à l'information au Québec. Chacune a toutefois des limites intrinsèques, abordées plus en détail à la section suivante.

- 1) **La reddition de compte annuelle des ministères et de certains organismes.** Les organismes assujettis au *Règlement sur la diffusion et la protection des renseignements personnels*⁴³⁰ doivent diffuser annuellement certaines statistiques en matière d'accès à l'information dans leur rapport annuel de gestion ou d'activités. Cette diffusion s'effectue suivant un gabarit fourni par le Secrétariat du Conseil du trésor⁴³¹, et rend compte des informations suivantes :
 - Le nombre de demandes d'accès à l'information reçues par l'organisme.
 - Le délai consacré à leur traitement.
 - Les dispositions de la Loi sur l'accès justifiant le refus de certaines d'entre elles.
 - Le nombre de demandes acceptées, partiellement acceptées ou refusées.
 - Le nombre de demandes ayant fait l'objet de mesures d'accommodement raisonnable.
 - Le nombre de demandes ayant fait l'objet d'une demande de révision à la Commission.
 - Les activités relatives à l'accès à l'information et à la protection des renseignements personnels réalisées au sein de l'organisme public.
- 2) **La publication des décisions et documents transmis à la suite d'une demande d'accès.** Les organismes assujettis au Règlement sur la diffusion doivent diffuser, sur leur site Internet, « les documents transmis dans le cadre d'une demande d'accès, accompagnés de la décision anonymisée du responsable de l'accès aux documents »⁴³², comme en traite davantage la section 1.3.4.
- 3) **Les outils de suivi internes des organismes.** Bon nombre d'organismes mettent en place des outils de suivi pour organiser le traitement des demandes d'accès qui leur sont soumises conformément aux lois applicables. De tels outils sont souvent des solutions technologiques, plus ou moins complexes, mises en place pour assurer, notamment, le respect des délais applicables au traitement des demandes d'accès⁴³³ ou pour assurer une cohérence et une cohésion dans les décisions rendues par l'organisme. On pense, par exemple, à un tableau de suivi des demandes d'accès ou à un outil de recherche dans les décisions rendues. Il est à noter que ce genre d'outils peut aider à colliger plus facilement l'information abordée au point 1).
- 4) **Les dossiers de révision de la section juridictionnelle de la Commission.** Pour traiter les demandes de révision dans la portion des cas d'accès à l'information qui font l'objet d'un recours, la Commission utilise un système d'information qui permet d'extraire certaines statistiques.

⁴³⁰ Règlement sur la diffusion, art. 2.

⁴³¹ SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Instructions et gabarit pour l'élaboration du rapport annuel de gestion 2025-2026*, 2026, en ligne : <https://www.tresor.gouv.qc.ca/fileadmin/PDF/cadre_gestion/RAG_25-26.docx>.

⁴³² Règlement sur la diffusion, art. 4, par. 8.

⁴³³ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97, p. 7.



1.4.3. Enjeux

Malgré l'existence des sources mentionnées ci-haut, plusieurs contraintes rendent fort complexe leur exploitation afin de pouvoir en retirer les bénéfices attendus. Par ailleurs, même si elles étaient mises en commun, le portrait qui en ressortirait ne serait pas complet.

1.4.3.1. Les sources de données actuelles présentent des limites intrinsèques

La Commission relève diverses contraintes liées principalement à la représentativité, à l'accessibilité et à l'exploitabilité des sources de données actuelles.

1.4.3.1.1. Le Règlement sur la diffusion vise peu d'organismes

Les deux sources de données découlant de l'application du Règlement sur la diffusion ne concernent que les ministères et organismes du gouvernement⁴³⁴, soit uniquement 7 % des organismes publics soumis à la Loi sur l'accès⁴³⁵, un problème abordé plus en détail à la section 1.3.4.3.1. Sans nier l'importance des activités de ces organismes, dont plusieurs sont de grande taille, cette situation a pour effet de restreindre la portée de ces sources de données, lesquelles excluent des pans névralgiques de la société québécoise comme les entités des réseaux de l'éducation et de la santé ainsi que les municipalités. Par conséquent, leur apport à l'établissement d'un portrait global de l'accès à l'information est limité.

1.4.3.1.2. Seule une partie des documents et des décisions des organismes suivant une demande d'accès est diffusée sur leur site

L'obligation de diffuser les documents transmis dans le cadre d'une demande d'accès prévue au Règlement sur la diffusion ne concerne que les demandes d'accès à des documents administratifs des organismes assujettis qui sont acceptées, avec certaines exceptions. Elle ne tient ainsi pas compte :

- des demandes d'accès refusées intégralement, qui ne donnent pas lieu à la transmission de documents;
- des demandes d'accès aux renseignements personnels ou de rectification de ceux-ci, puisque les organismes ne doivent pas diffuser les documents contenant des renseignements personnels.

Cette limite intrinsèque découle directement du but premier de cette obligation, qui est, par souci de transparence, de diffuser les documents auxquels l'accès est octroyé par l'organisme : si ceux-ci sont accessibles à un demandeur, ils doivent l'être pour tous sans démarches administratives supplémentaires. Cela évite, du même coup, la multiplication des demandes d'accès à propos d'un même document. En somme, cette obligation de diffusion ne vise pas la mise en place d'un outil permettant l'examen complet des pratiques des organismes concernés en matière de traitement des demandes d'accès et l'exploitation des données en découlant.

1.4.3.1.3. Les données publiées en lien avec le Règlement sur la diffusion sont décentralisées

Bien que publiques et généralement accessibles moyennant certaines recherches sur les sites Web des ministères et organismes du gouvernement concernés, les deux sources de données découlant de l'application du Règlement sur la diffusion restent décentralisées, ce qui complique leur mise en commun.

⁴³⁴ Règlement sur la diffusion, art. 1.

⁴³⁵ En date du 14 avril 2026, le registre des responsables d'accès de la Commission comptait plus de 2 550 organismes, dont 183 sont visés par l'article 1 du Règlement sur la diffusion.



Chaque organisme est responsable de colliger ses propres données, sans que sa réflexion porte sur la cohérence et la potentielle adéquation de ses données avec celles des autres organismes.

Les décisions et les documents transmis dans le cadre de réponses positives à des demandes d'accès à des documents administratifs sont publiés indépendamment sur le site de chaque organisme assujéti au Règlement sur la diffusion. Il n'existe pas d'outil de compilation et d'exploitation de ces données.

Les statistiques annuelles sur le traitement des demandes d'accès, disponibles dans les rapports annuels d'activités et de gestion, figurent dans des documents indépendants, dispersés sur divers sites Web et présentés en format textuel non « lisible par machine⁴³⁶ », et donc peu adapté à leur extraction et leur incorporation à des statistiques globales. Les rapports annuels concernent plusieurs autres sujets et sont déposés à l'Assemblée nationale à divers moments de l'année, suivant le processus et le calendrier propres à chaque organisme. À la connaissance de la Commission, il n'existe pas de liste exploitable des informations sur le traitement des demandes d'accès contenues dans ces rapports, et nul ne réalise actuellement de suivi systématique de ces statistiques.

1.4.3.1.4. Les données intégrées aux rapports annuels sont agrégées

Les données diffusées annuellement dans les rapports annuels en application du Règlement sur la diffusion sont difficilement exploitables considérant leur caractère agrégé. Elles sont présentées sous forme de sommes concernant des catégories : de délai, de demande, de statut. Par exemple, les organismes rendent compte des délais de traitement en utilisant le tableau suivant, tiré du modèle du Secrétariat du Conseil du trésor⁴³⁷.

Délais de traitement	Demandes d'accès à des documents administratifs	Demandes d'accès à des renseignements personnels	Rectification
0 à 20 jours			
21 à 30 jours			
31 jours et plus (le cas échéant)			
Total			

Ce type d'agrégation masque plusieurs détails importants qu'il pourrait être utile de connaître, comme la fréquence à laquelle a été utilisée chacune des restrictions à l'accès, le nombre de refus invoquant le même motif, le nombre de demandeurs différents ou le délai exact de traitement des demandes.

1.4.3.1.5. Les outils de suivi internes des organismes ne sont pas facilement accessibles

Théoriquement, vu leur finalité, les données contenues dans les outils de suivi internes des organismes pour le traitement des demandes d'accès devraient être granulaires, c'est-à-dire consignées demande par

⁴³⁶ OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « fichier de données lisibles par machine », *Grand dictionnaire terminologique*, en ligne : <<https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8454887/fichier-de-donnees-lisibles-par-machine>> (consulté le 10 avril 2026).

⁴³⁷ SECRÉTARIAT DU CONSEIL DU TRÉSOR, préc., note 431, p. 35-36.



demande et non de manière agrégée, ce qui permettrait une analyse plus riche et plus poussée. Cependant, ces outils de suivi internes ne sont pas publics. L'unique moyen pour les obtenir consiste à s'adresser à chaque organisme concerné individuellement, ce qui représente un travail colossal.

Par ailleurs, il n'existe aucune obligation légale d'utiliser de tels outils. Même s'ils sont très fréquents, il est possible que certains organismes n'y aient pas recours.

1.4.3.1.6. Les données de la Commission visent uniquement les recours

Les données de la Commission, comme il a été expliqué précédemment, visent des cas bien particuliers découlant de l'exercice de sa compétence juridictionnelle. Elles ne concernent que les cas où la décision initiale de l'organisme concerné est contestée formellement suivant le processus prévu à la Loi sur l'accès. Ces données sont donc fragmentaires, puisqu'elles ne portent que sur une partie limitée du processus de traitement des demandes d'accès. Elles sont, en quelque sorte, la pointe de l'iceberg.

1.4.3.1.7. La compilation des données varie d'un organisme à l'autre

Considérant la multitude de sources, toute comparaison ou mise en commun des données souffrirait de leur forte variabilité. En effet, sans modèle formellement prescrit, les bases de calcul et les variables compilées varient d'un organisme à l'autre. Par exemple, dans leurs outils de suivi, certains ne compilent pas le délai de traitement moyen des demandes ou ne font pas de distinction entre les demandes d'accès aux documents administratifs et les demandes liées aux renseignements personnels⁴³⁸. L'année de référence est tantôt civile, tantôt financière, tantôt scolaire. La date considérée pour la comptabilisation des demandes peut aussi varier : il peut s'agir de la date de leur réception, ou encore de la date de transmission de la décision par l'organisme. À ce titre, malgré le gabarit produit par le Secrétariat du Conseil du trésor, ce type d'enjeu est constaté dans les statistiques diffusées dans les rapports annuels de gestion ou d'activités.

Dans tous les cas, cette variabilité affecte la valeur probante des statistiques pouvant être obtenues en exploitant de telles données.

1.4.3.2. La compilation de données est logistiquement exigeante

Plusieurs des contraintes soulevées ci-haut ont été vécues indépendamment par divers acteurs dans les dernières années.

La Commission s'y est notamment heurtée en menant son étude sur les délais d'accès en 2022⁴³⁹. Elle a consacré des efforts opérationnels importants pour obtenir les données internes des 33 organismes de son échantillon. Bien que leur comparaison ait posé un défi substantiel en raison de la variabilité des pratiques, la Commission a pu dégager un portrait éclairant du respect des délais par des organismes de tous horizons et dresser des constats sur l'effet de la pandémie de COVID-19 sur le système d'accès à l'information. Ce portrait reste toutefois un instantané, et l'expérience ne pourrait être refaite qu'au prix d'efforts comparables à ceux consentis pour cette étude.

Des journalistes ont également tenté des expériences semblables. Certains ont constitué des bases de données de demandes d'accès, comme celle du projet du *Globe and Mail*, *Secret Canada*⁴⁴⁰. Elle a été

⁴³⁸ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 97, p. 35.

⁴³⁹ *Id.*, p. 35-36.

⁴⁴⁰ THE GLOBE AND MAIL, « Search FOI summaries », *Secret Canada*, en ligne : <<https://www.secretcanada.com/search-foi-requests>> (consulté le 3 mars 2025).



créée à partir de plus de 400 demandes d'accès aux outils de suivi internes des demandes d'accès de 225 organismes fédéraux et provinciaux, y compris québécois⁴⁴¹. Cet exercice de compilation a été semé d'embûches liées aux limites d'exploitabilité et de comparabilité des outils de suivi, et a exigé un travail manuel colossal⁴⁴². L'analyse du contenu de la base de données a néanmoins permis aux journalistes de révéler plusieurs tendances majeures dans les systèmes d'accès à l'information canadiens, notamment en ce qui a trait aux délais de traitement⁴⁴³. En parallèle, des journalistes de Radio-Canada ont également effectué une compilation des délais de traitement rapportés par les ministères dans leurs rapports annuels 2022-2023 afin d'illustrer la prévalence des décisions en dehors des délais légaux⁴⁴⁴.

En synthèse, à l'heure actuelle, quiconque souhaite broser un portrait du système d'accès à l'information doit multiplier les démarches et les demandes pour avoir accès aux données, et ne peut qu'en obtenir qui soient partielles et indirectement comparables. A fortiori, tout suivi dans le temps impose de recommencer périodiquement ces efforts.

1.4.4. Recommandation

La reddition de compte actuelle en matière d'accès à l'information au Québec apparaît insatisfaisante. À titre de solution, la Commission préconise l'instauration d'une compilation de données améliorée, inspirée de celle prévue dans d'autres juridictions. Certains exemples à cet égard sont abordés dans la section 1.2.1.5.

Cette reddition de compte améliorée devrait être codifiée dans un texte contraignant, réglementaire ou législatif, pour en assurer une compréhension et un respect communs.

Pour qu'elle puisse pleinement jouer son rôle de surveillance en misant sur les données obtenues, et pour garantir une analyse indépendante de ce qu'elles révèlent, la Commission estime qu'elle devrait être chargée d'administrer cette reddition de compte à titre d'autorité de contrôle, à l'instar de plusieurs de ses homologues. Cette nouvelle fonction devrait être accompagnée de ressources attribuées en conséquence.

Les données obtenues pourraient être exploitées par la Commission et permettraient de rapidement fournir des statistiques sur le traitement des demandes d'accès. Un accès public à ces données, présentées organisme par organisme, devrait être prévu.

La réalisation de cette vision aurait divers avantages majeurs :

- **Meilleure vue d'ensemble, meilleurs diagnostics, meilleure utilisation des ressources.** La Commission pourrait beaucoup plus facilement détecter les aspects de la Loi plus problématiques et cibler les organismes aux pratiques potentiellement non conformes. Ce faisant, elle investirait mieux ses ressources en sensibilisation et en surveillance, là où la situation factuelle le justifie. La Commission pourrait aussi, à l'inverse, cibler les organismes dont les données démontreraient des

⁴⁴¹ THE GLOBE AND MAIL, « Methodology », *Secret Canada* (2023), en ligne : <<https://www.secretcanada.com/methodology>> (consulté le 3 mars 2025).

⁴⁴² *Id.*

⁴⁴³ Robyn DOOLITTLE et Tom CARDOSO, « Inside Canada's broken freedom-of-information system: 'An affront to democracy' », *The Globe and Mail* (9 juin 2023), en ligne : <<https://www.theglobeandmail.com/canada/article-canada-freedom-of-information-laws/>> (consulté le 3 mars 2025).

⁴⁴⁴ T. GERBET et D. BOILY, préc., note 209.



expertises ou des pratiques exemplaires et pourrait s'en servir à titre de « modèle à suivre ». L'effet positif serait le même pour le SRIDAIL, qui appuie le ministre responsable de l'Accès à l'information dans sa fonction d'accompagnement des organismes publics. Par ailleurs, les données permettraient de mieux documenter les problèmes récurrents en matière d'accès justifiant des modifications législatives. Le tout pourrait aussi simplifier le repérage des meilleures pratiques à suivre développées au sein d'organismes publics.

- **Amélioration indirecte des processus de traitement des demandes.** Puisqu'ils seraient tenus de transmettre des statistiques complètes et exactes, les organismes seraient incités à améliorer le suivi interne du traitement des demandes d'accès qui leur sont adressées. Cette solution pourrait entre autres mener à une meilleure gestion des délais, un point important abordé dans la section 1.2.3.
- **Examen plus soutenu par la société civile.** La possibilité pour le public de comparer les statistiques de chaque organisme braquerait le projecteur sur leurs activités en accès à l'information, facilitant le travail de certains acteurs de la société civile souhaitant les évaluer, comme les journalistes ou les chercheurs. Elle motiverait assurément les organismes à accroître les ressources consacrées à cette importante fonction légale, comme mentionné dans la section 1.3.1.

Notons que la disponibilité de données globales sur le traitement des demandes d'accès à l'information peut également permettre, comme le montrent certains des exemples abordés dans la section 1.2.1.5, de proposer des tableaux de bord interactifs permettant d'explorer les tendances. Cette possibilité serait cohérente avec des actions similaires posées par le gouvernement du Québec ces dernières années en matière de données ouvertes (p. ex. en santé⁴⁴⁵, en éducation⁴⁴⁶, pour l'action climatique⁴⁴⁷, pour les projets numériques⁴⁴⁸, etc.).

Recommandation 26

Renforcer, par voie législative ou réglementaire, la reddition de comptes en matière d'accès à l'information afin de la rendre :

- plus complète, en s'assurant qu'elle vise un maximum d'organismes publics;
- plus uniforme et plus précise, en s'assurant que les données à compiler par chaque organisme sont granulaires et produites suivant des normes prescrites qui facilitent leur exploitation et en fixant une période de référence commune;
- centralisée et transparente, en prévoyant que les données des organismes soient réunies dans une base de données unique, accessible, pouvant être interrogée par le public et dont la gestion serait confiée à la Commission.

⁴⁴⁵ SANTÉ QUÉBEC, préc., note 392.

⁴⁴⁶ GOUVERNEMENT DU QUÉBEC, préc., note 393.

⁴⁴⁷ GOUVERNEMENT DU QUÉBEC, préc., note 394.

⁴⁴⁸ GOUVERNEMENT DU QUÉBEC, préc., note 395.



1.4.5. Pour aller plus loin

Plusieurs autres juridictions comparables compilent des statistiques détaillées et complètes sur l'accès à l'information, la plupart d'entre eux par le biais d'un cadre législatif. Le Québec devrait s'en inspirer. La Commission a examiné plus en détail l'encadrement en place dans sept de ces juridictions pour en tirer des constats généraux, qu'elle présente dans un premier temps. Elle attire ensuite l'attention plus particulièrement sur l'encadrement prévu dans trois d'entre elles, soit la Colombie-Britannique, l'Écosse et l'Australie.

1.4.5.1. Aperçu général de la compilation de données dans d'autres juridictions

Le tableau de l'annexe 2 présente les principales caractéristiques de l'encadrement mis en place au Canada, au palier fédéral et dans les provinces de l'Ontario et de la Colombie-Britannique, en Écosse, au Royaume-Uni et en Australie, au palier fédéral ainsi que dans l'État de Victoria.

Ce survol de l'encadrement dans ces juridictions permet de tirer les constats suivants :

- Une loi encadre généralement la production de statistiques et peut être complétée par un règlement ou des normes souples.
- Les organismes assujettis aux lois sur l'accès doivent transmettre des données prescrites à un organisme compilateur, tantôt une autorité de contrôle comme la Commission, tantôt une entité du gouvernement central.
- La transmission est souvent annuelle, mais peut être trimestrielle.
- Dans la plupart des cas, les données acheminées sont agrégées, comme ce que prévoit déjà le Règlement sur la diffusion. Exception notable : la Colombie-Britannique compile les données de manière granulaire, soit sous un format demande par demande.
- L'organisme compilateur ne vérifie généralement pas l'exactitude des données, sauf au Royaume-Uni.
- L'organisme compilateur réunit et publie les données sous diverses formes à l'intention du public : des rapports dans la majorité des cas, mais parfois aussi des tableaux de bord ou des données ouvertes.
- La fréquence et la granularité des diffusions publiques réalisées sont le miroir de l'information exigée et reçue.

Lorsque l'on observe les statistiques et les indicateurs compilés pour les juridictions examinées, certains points communs émergent. Au minimum, chaque organisme soumet le nombre de demandes d'accès qu'il a reçues et la répartition des demandes selon la décision rendue, comme l'accès complet ou partiel, le refus ou le transfert à un autre organisme. Dans la majorité des juridictions examinées, l'organisme indique aussi les dispositions invoquées pour refuser l'accès, le nombre de demandes traitées et en traitement, les délais de traitement par catégorie⁴⁴⁹, les frais demandés et le nombre de cas ayant fait l'objet de recours. Divers autres indicateurs peuvent être demandés selon l'État, sans qu'il s'agisse d'une tendance, comme :

- le profil des demandeurs, par exemple citoyen, journaliste ou entreprise;
- le délai de traitement en nombre de jours;
- le motif de non-respect du délai, s'il y a lieu;
- la durée de la prolongation demandée ou autorisée par l'organisme, s'il y a lieu;
- les ressources humaines ou le temps et les coûts engagés pour le traitement des demandes.

⁴⁴⁹ C'est-à-dire des catégories comme « dans les délais », « avec prolongation », « hors délai ».



La richesse de ces données est apparente en ce qu'elle permet la publication de tableaux structurés très détaillés. En effet, les tableaux de compilation publiés dans les différentes juridictions donnent des indications sur une variété d'aspects reliés au traitement des demandes d'accès. Certains d'entre eux comportent de 100 à 215 colonnes différentes, et jusqu'à 897 à l'échelle fédérale canadienne⁴⁵⁰. Cette foule d'informations aisément disponibles contraste avec la situation au Québec.

1.4.5.2. La situation en Colombie-Britannique

Le ministère des Services aux citoyens de la Colombie-Britannique opère un programme centralisé d'accès à l'information, l'Information Access Operations. Les demandes adressées par les citoyens aux ministères et à certains organismes gouvernementaux transitent toutes par ce programme⁴⁵¹. Par conséquent, le ministère des Services aux citoyens peut compiler des statistiques sur le traitement des demandes d'accès par ces organismes publics. Dans son rapport annuel sur l'administration de la loi sur l'accès, le ministère publie ces statistiques⁴⁵².

Depuis 2011, les données brutes du ministère des Services aux citoyens sont aussi diffusées en tant que données ouvertes⁴⁵³. Elles sont disponibles au plus haut niveau de granularité, soit sur une base individuelle par demande, comme l'illustre la capture d'écran suivante⁴⁵⁴.

1	Ministry	Type	Request #	Applicant	Start Date	Due Date	End Date	Status	Disposition	On Hold Days	Processing Days
135242	Health	Personal	HTH-2025-50849	Individual	21-Feb-25	4-Apr-25	28-Mar-25	Closed	Full Disclosure	0	25
135243	Health	Personal	HTH-2025-51199	Individual	12-Mar-25	25-Apr-25	19-Mar-25	Closed	Opened in Error	0	5
135244	Infrastructure	General	INF-2024-42891	Individual	23-Dec-24	6-Feb-25	7-Jan-25	Closed	No Resp. Records Exist/Located	0	8
135245	Infrastructure	General	INF-2025-50151	Individual	27-Jan-25	11-Mar-25	11-Feb-25	Closed	No Resp. Records Exist/Located	0	11
135246	Infrastructure	General	INF-2025-50173	Individual	27-Jan-25	11-Mar-25	13-Feb-25	Closed	Records in another Min/Org	0	13
135247	Infrastructure	General	INF-2025-50186	Business	31-Jan-25	28-Mar-25	12-Mar-25	Closed	No Resp. Records Exist/Located	9	18
135248	Infrastructure	General	INF-2025-50239	Interest Group	31-Dec-24	12-Feb-25	20-Feb-25	Closed	No Resp. Records Exist/Located	0	35
135249	Infrastructure	General	INF-2025-50400	Interest Group	3-Mar-25	14-Apr-25	24-Mar-25	Closed	No Resp. Records Exist/Located	0	15
135250	Infrastructure	Personal	INF-2025-50435	Individual	22-Jan-25	6-Mar-25	13-Feb-25	Closed	Records in another Min/Org	0	16
135251	Infrastructure	General	INF-2025-50442	Interest Group	3-Mar-25	14-Apr-25	25-Mar-25	Closed	Withdrawn	0	16
135252	Infrastructure	General	INF-2025-50499	Individual	6-Mar-25	17-Apr-25	27-Mar-25	Closed	Transferred	0	15
135253	Indigenous Relations	General	IRR-2023-32413	Business	12-Sep-23	13-May-24	7-Mar-25	Closed	Partial Disclosure	23	345
135254	Indigenous Relations	General	IRR-2024-40570	Law Firm	26-Feb-24	30-Aug-24	16-Jan-25	Closed	Partial Disclosure	9	212
135255	Indigenous Relations	General	IRR-2024-41369	Interest Group	24-May-24	20-Aug-24	13-Mar-25	Closed	Partial Disclosure	0	199
135256	Indigenous Relations	General	IRR-2024-42671	Law Firm	20-Nov-24	3-Feb-25	3-Jan-25	Closed	Abandoned	20	9
135257	Indigenous Relations	General	IRR-2025-50121	Business	22-Jan-25	6-Mar-25	14-Feb-25	Closed	No Resp. Records Exist/Located	0	17
135258	Indigenous Relations	General	IRR-2025-50149	Media	22-Jan-25	6-Mar-25	11-Feb-25	Closed	Records in another Min/Org	0	14

⁴⁵⁰ Ces totaux n'impliquent pas que les organismes assujettis doivent transmettre autant d'indicateurs différents. Ils résultent plutôt du fait que plusieurs juridictions croisent les valeurs de différents facteurs pour organiser les données, ce qui entraîne des colonnes précises dont le nombre est élevé. Par exemple : [19 restrictions légales] × [3 types de demandes] = 57 colonnes en Australie; [8 catégories de délai de traitement] × [10 types de décisions rendues] = 80 colonnes au Canada).

⁴⁵¹ MINISTÈRE DES SERVICES AUX CITOYENS DE LA COLOMBIE-BRITANNIQUE, « Request records from government », *Gov.bc.ca* (19 septembre 2024), en ligne : <<https://www2.gov.bc.ca/gov/content/governments/about-the-bc-government/open-government/open-information/freedom-of-information>> (consulté le 4 mars 2025).

⁴⁵² Voir par exemple MINISTÈRE DES RELATIONS AVEC LES CITOYENS DE LA COLOMBIE-BRITANNIQUE, *Report on the administration of Freedom of Information and Protection of Privacy Act*, Colombie-Britannique, 2024, en ligne : <https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/initiatives-plans-strategies/open-government/open-information/annual_report_on_the_administration_of_foippa_fy_2023-24_002.pdf>.

⁴⁵³ OPEN INFORMATION, « Freedom of Information (FOI) Statistics », *British Columbia Data Catalogue*, en ligne : <<https://catalogue.data.gov.bc.ca/dataset/freedom-of-information-foi-statistics>> (consulté le 4 mars 2025).

⁴⁵⁴ Cette capture d'écran est tirée du fichier suivant : OPEN INFORMATION, « BC FOI Statistics », *British Columbia Data Catalogue* (31 juillet 2025), en ligne : <<https://www2.gov.bc.ca/gov/content/data/policy-standards/data-policies/open-data/open-government-licence-bc>> (consulté le 9 avril 2026); ces informations sont soumises à la licence Open Government Licence - British Columbia : GOUVERNEMENT DE LA COLOMBIE-BRITANNIQUE, « Open Government Licence - British Columbia », *Gov.bc.ca* (11 avril 2025), en ligne : <<https://catalogue.data.gov.bc.ca/dataset/freedom-of-information-foi-statistics/resource/2a613175-afa5-4072-8e54-2412a1a8fa1f>> (consulté le 4 mars 2025).

1.4.5.3. La situation en Écosse

La loi sur l'accès à l'information d'Écosse donne au conseil des ministres la fonction d'élaborer un code de pratique en accès à l'information, lequel doit notamment prévoir des dispositions relatives aux statistiques sur le traitement des demandes d'accès⁴⁵⁵. Ce code doit être adopté après consultation du commissaire à l'information écossais. La plus récente version de ce code remonte à 2016⁴⁵⁶. S'il comporte une liste de variables à consigner pour documenter le traitement des demandes d'accès, il n'oblige pas les organismes publics à suivre des règles formelles concernant la compilation.

Bien que ni la loi ni le code prévoient la centralisation des statistiques auprès du commissaire à l'information écossais, celui-ci demande aux organismes de les lui fournir, indiquant qu'ils « devraient déjà compiler ces données, suivant le [code de pratique], et [que] cette information devrait donc déjà être accessible en vertu du droit d'accès aux documents »⁴⁵⁷. Il remet aux organismes une liste des données et des informations qu'il souhaite recevoir et propose un portail numérique permettant de les soumettre sur une base trimestrielle.

Le commissaire à l'information écossais rend disponibles au fur et à mesure qu'il les reçoit les données agrégées pour chaque organisme dans divers tableaux, dont l'un réunit toutes les périodes de référence depuis 2013-2014 pour un portrait évolutif. Depuis juin 2024, il présente l'ensemble des données dans un tableau de bord interactif, qui permet aux utilisateurs d'appliquer différents filtres et d'afficher des statistiques ou des figures personnalisées.

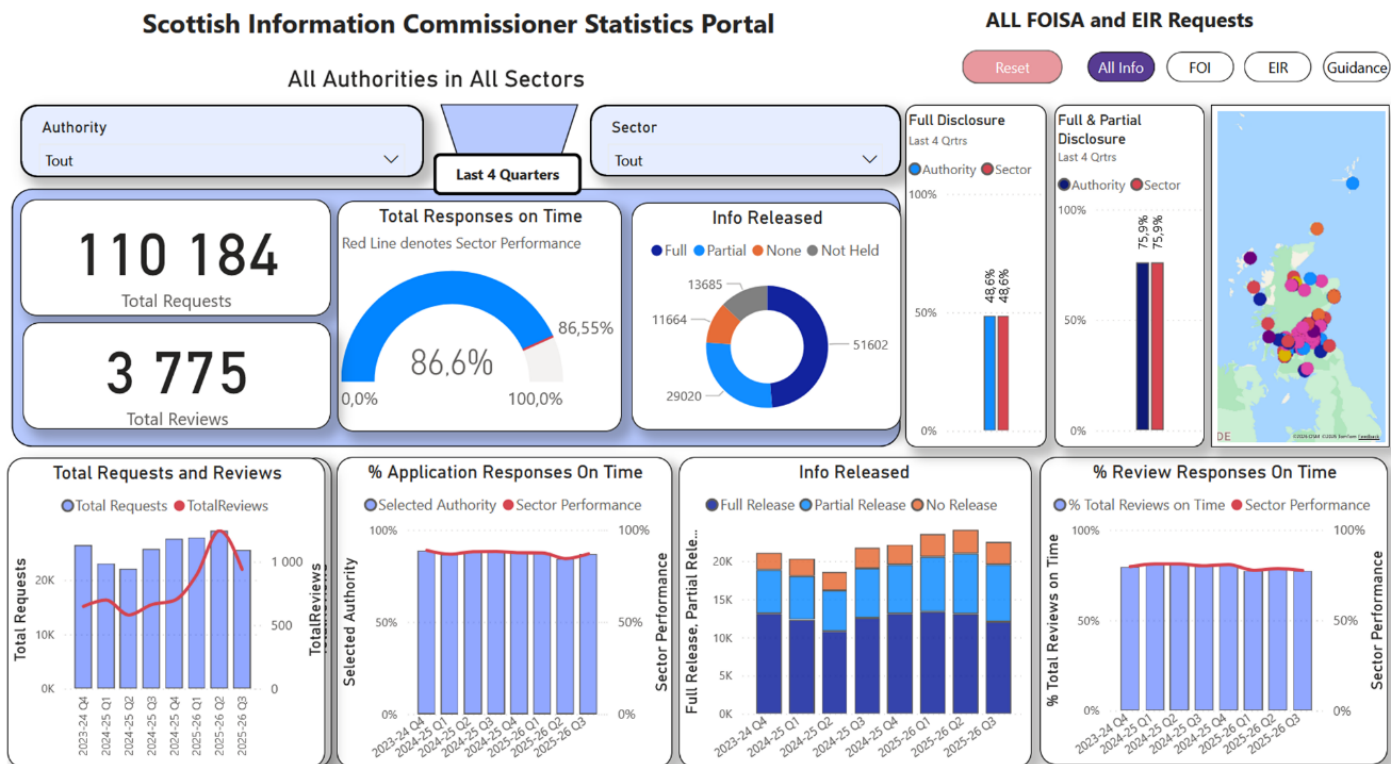
⁴⁵⁵ *Freedom of Information Act 2002 [Écosse]*, 2002, asp 13., art. 60(2)f), en ligne : <https://www.legislation.gov.uk/asp/2002/13/contents>.

⁴⁵⁶ CONSEIL DES MINISTRES DE L'ÉCOSSE, *Scottish Minister's Code of Practice on the Discharge of Functions by Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004*, 2016, en ligne : <https://www.gov.scot/binaries/content/documents/govscot/publications/advice-and-guidance/2016/12/foi-eir-section-60-code-of-practice/documents/foi-section-60-code-practice-pdf/foi-section-60-code-practice-pdf/govscot%3Adocument/FOI%2B-%2Bsection%2B60%2Bcode%2Bof%2Bpractice.pdf>.

⁴⁵⁷ SCOTTISH INFORMATION COMMISSIONER, « FOI and EIRs statistics », en ligne : <https://www.foi.scot/statistics> (consulté le 9 avril 2026); notre traduction.



La capture d'écran suivante donne un aperçu de ce tableau de bord⁴⁵⁸.



1.4.5.4. La situation en Australie au palier fédéral

Le bureau du commissaire australien à l'information a notamment pour fonction de compiler, dans un rapport annuel, des informations et des statistiques concernant l'accès à l'information⁴⁵⁹. De leur côté, les organismes publics ont l'obligation de lui fournir toutes les données nécessaires à la préparation de ce rapport annuel⁴⁶⁰. Ils doivent également se conformer à toute prescription réglementaire liée à la transmission et à la compilation de l'information ainsi qu'aux lignes directrices du bureau du commissaire australien à l'information.

Les organismes publics sont responsables d'envoyer leurs données au bureau du commissaire australien à l'information sur une base trimestrielle, en plus d'un résumé annuel, grâce au portail numérique proposé par l'autorité. Celle-ci fournit un guide pour aider les organismes à se conformer, lequel comprend des précisions sur la comptabilisation des demandes⁴⁶¹.

⁴⁵⁸ *Id.*; Cette capture d'écran contient de l'information du secteur public soumise à la licence Open Government Licence v3.0 : ARCHIVES NATIONALES DU ROYAUME-UNI, « Open Government Licence », en ligne : <https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/> (consulté le 9 avril 2026).

⁴⁵⁹ *Australian Information Commissioner Act 2010*, art. 8(j), 30 et 31, en ligne : <https://www.legislation.gov.au/C2010A00052/latest/text>.

⁴⁶⁰ *Freedom of Information Act 1982 [Australie]*, art. 93, en ligne : <https://www.legislation.gov.au/C2004A02562/latest/text>.

⁴⁶¹ OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, *FOI Guidelines issued by the Australian Information Commissioner under s 93A of the Freedom of Information Act 1982*, 2025, sect. 15, en ligne : https://www.oaic.gov.au/_data/assets/pdf_file/0020/250391/FOI-Guidelines-Compilation-October-2025.PDF.



En plus de publier les statistiques dans son rapport annuel, où il illustre diverses tendances comme le recours à chaque restriction à l'accès comme le montre l'extrait de tableau ci-bas⁴⁶², le bureau du commissaire australien à l'information les rend également disponibles par l'entremise d'un tableau de bord interactif depuis 2024.

Table E.6: Use of exemptions in FOI decisions in 2023–24					
FOI Act reference	Exemption	Personal	Other	Total	% of all exemptions applied
s 33	Documents affecting national security, defence or international relations	248	420	668	4
s 34	Cabinet documents	4	175	179	1
s 37	Documents affecting enforcement of law and protection of public safety	617	215	832	5
s 38	Documents to which secrecy provisions of enactments apply	741	220	961	6
s 42	Documents subject to legal professional privilege	190	350	540	3

Les données brutes, agrégées par organisme, sont en outre publiées annuellement sur le portail de données ouvertes du gouvernement australien⁴⁶³.

⁴⁶² Cet extrait est tiré du document suivant : OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, *Annual report 2023-24*, 2024, p. 141, en ligne : <https://www.oaic.gov.au/__data/assets/pdf_file/0025/243592/OAIC_Annual-Report-2023-24_Digital.pdf>; le contenu de ce rapport est utilisé conformément à la licence CC BY 4.0 : CREATIVE COMMONS, « CC BY 4.0 - Attribution 4.0 International », en ligne : <<https://creativecommons.org/licenses/by/4.0/deed.fr>> (consulté le 9 avril 2026).

⁴⁶³ « Freedom of information statistics », *Data.gov.au*, en ligne : <<https://data.gov.au/data/dataset/freedom-of-information-statistics>> (consulté le 28 octobre 2025).

CHAPITRE 2

2. La protection des renseignements personnels





Introduction

Le Québec a historiquement été un chef de file en Amérique du Nord en matière de protection des renseignements personnels. Ainsi adoptait-il en 1994, avant toute autre juridiction sur le continent, une loi applicable en cette matière au secteur privé. Il a réaffirmé son leadership avec la Loi 25, laquelle a permis de moderniser le cadre législatif québécois pour l'amener au niveau du standard le plus reconnu et le plus avancé du moment, soit celui du *Règlement général sur la protection des données* (le RGPD) de l'Union européenne. Le régime québécois constitue à son tour un modèle pour les autres juridictions canadiennes, qui cherchent à moderniser leurs propres lois sur la protection des renseignements personnels. On ne saurait ainsi reprocher au Québec de manquer d'audace ou d'être à la remorque en matière de vie privée.

Les fondements du modèle de protection des renseignements personnels porté par la législation actuelle, même réformée, sont toutefois restés relativement inchangés. L'architecture des lois québécoises en la matière se fonde toujours sur les principes de protection des renseignements personnels qui ont été développés dans les années 1970 et qui sont désignés par l'acronyme FIP pour *fair information practice principles*⁴⁶⁴. Les principes FIP, au cœur des standards internationaux⁴⁶⁵, ont connu un important succès et ont été érigés en norme quasi universelle⁴⁶⁶. Ces principes sont basés sur les fondements suivants :

- Responsabilité;
- Détermination des fins;
- Limitation de la collecte, de l'utilisation et de la communication des renseignements;
- Consentement;
- Exactitude;
- Sécurité;
- Transparence;
- Droits des personnes concernées (accès et rectification, notamment);
- Recours auprès d'une autorité indépendante.

Les principes FIP se traduisent dans des lois dont les principaux points focaux sont la collecte de renseignements plutôt que leur usage, les individus plutôt que la collectivité, le contrôle individuel plutôt que la réduction des préjudices à la source.

Les lois québécoises sur la protection des renseignements personnels suivent donc un modèle contractuel. Les protections qu'elles mettent en place concernent essentiellement la relation entre une personne et l'organisation qui traite ses renseignements. Elles s'appuient largement sur la rationalité et le libre arbitre de la personne, à qui elles donnent des moyens de contrôle. On doit dûment l'informer du traitement de ses renseignements personnels, solliciter son consentement dans diverses circonstances et

⁴⁶⁴ Ces principes ont été présentés pour la première fois dans un rapport fondateur du gouvernement américain en 1973: US DEPARTMENT OF HEALTH, EDUCATION AND WELFARE, *Records, computers and the rights of citizens: report of the Secretary's Advisory Committee on Automated Personal Data Systems*, Cambridge, Mass, MIT Press, 1973 [ci-après *Records, computers and the rights of citizens*], en ligne : <<https://archive.org/details/recordscomputers00unit/mode/2up>>.

⁴⁶⁵ Ils ont par exemple été intégrés aux Lignes directrices de l'OCDE en matière de vie privée : ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, OECD/LEGAL/0188, 1980, en ligne : <<https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0188>> (consulté le 20 novembre 2025).

⁴⁶⁶ Woodrow HARTZOG, « The Inadequate, Invaluable Fair Information Practices », (2020) 76-4 *Maryland Law Review* 952-983, p. 953-954, en ligne : <<https://www.marylandlawreview.org/s/The-Inadequate-Invaluable-Fair-Information-Practices.pdf>>.

lui permettre de faire valoir des droits en lien avec ses renseignements personnels. Les balises autres que celles associées au contrôle individuel peuvent être qualifiées de procédurales, pour l'essentiel. Ce sont entre autres des obligations de documentation, de fourniture d'avis et de réalisation d'évaluations.

De nouvelles pratiques informationnelles, ayant émergé au tournant du millénaire et s'étant accélérées dans les dix dernières années, remettent toutefois en cause les fondements des lois actuelles. La prémisse contractuelle de ces lois leur permet d'encadrer particulièrement la fourniture de renseignements par la personne concernée dans le cadre d'une relation consciente et volontaire avec une organisation. Leurs limites apparaissent dans un contexte où les renseignements sont bien davantage observés ou inférés que délibérément fournis, où la variété de leurs utilisations s'est accrue et où le nombre de parties impliquées dans leur traitement a explosé.



Cette réalité est principalement due à la progression des technologies et des environnements numériques. Les situations suivantes en sont des exemples⁴⁶⁷ :

- Les objets connectés traversent nos existences. De nos téléphones à nos électroménagers en passant par nos téléviseurs et nos voitures, les capteurs connectés à Internet collectant des données variées en grand volume nous entourent et font le pont entre nos vies physique et numérique⁴⁶⁸.
- Avec l'essor de l'infonuagique, les organisations publiques et privées, tout comme les individus, stockent désormais une grande part de leurs données sur des serveurs externes, amenant les renseignements personnels à transiter parfois d'un bout à l'autre de la planète et à être conservés hors du territoire où résident les personnes qu'ils concernent.
- L'**IA**, que l'on retrouve dans des systèmes variés allant du traitement automatique du langage à la vision par ordinateur, mais aussi à la génération de textes, d'images ou d'autres types de contenus, occupe désormais une place prépondérante dans nos vies personnelles et professionnelles et dans les processus des organisations. Une grande part des systèmes d'**IA** sont « apprenants » et s'appuient largement sur les mégadonnées⁴⁶⁹ : ils sont ainsi nombreux à se nourrir de renseignements personnels, mais aussi à en créer, par inférence ou par génération.

⁴⁶⁷ GROUPE DES POLITIQUES ET DE LA RECHERCHE DU COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Consentement et protection de la vie privée - Document de discussion sur les améliorations possibles au consentement sous le régime de la Loi sur la protection des renseignements personnels et les documents électroniques*, 2016, p. 7, en ligne : 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/2016/consent_201605/.

⁴⁶⁸ COMMISSION DE L'ÉTHIQUE EN SCIENCE ET EN TECHNOLOGIE, *L'internet des objets, la vie privée et la surveillance - Balises éthiques et recommandations*, 2020, p. 5, en ligne : https://www.ethique.gouv.qc.ca/media/s32lokni/cest-internet-des-objets-surveillance_vf.pdf.

⁴⁶⁹ OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « mégadonnées », *Grand dictionnaire terminologique*, en ligne : <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26507313/megadonnees> (consulté le 24 novembre 2025).



De plus en plus, les technologies sont donc construites autour de la création et de l'exploitation de renseignements personnels. Leur intégration dans notre quotidien permet de dégager des savoirs nouveaux, précis et parfois intimes sur les personnes. D'autres développements technologiques déjà amorcés, comme l'IA agentive⁴⁷⁰ ou des neurotechnologies⁴⁷¹, laissent croire à une intensification de ce phénomène. Quant aux capteurs et au calcul quantiques⁴⁷², ils renforceront à la fois la mise en données ainsi que la puissance et la vitesse des calculs, constituant eux aussi un facteur d'accélération.

Le traitement à grande échelle des renseignements personnels fragilise et rend même inopérants plusieurs des principes FIP⁴⁷³ :

Il y a aussi [derrière les principes FIP] un postulat d'exclusivité et d'intentionnalité : qu'un individu a une relation directe et consciente avec un collecteur de données avec qui il souhaite (ou doit) interagir. Les architectes des principes FIP n'avaient pas anticipé la surveillance numérique omniprésente et permanente et la collecte de données rendue possible par les réseaux numériques et les appareils mobiles qui ont émergé dans les années 2000. Pas plus qu'ils n'avaient prévu que nos données seraient collectées par des tiers sans relation directe avec nous.

L'approche maximaliste de la collecte, de l'utilisation et de la communication des renseignements personnels met notamment à mal les principes FIP de détermination des fins et de limitation de la collecte de renseignements personnels, qui se reflètent dans les lois québécoises par le critère de nécessité.

De plus, le contrôle individuel devient de plus en plus difficile à exercer. Les personnes se heurtent à la complexité des pratiques actuelles, alors qu'il devient ardu d'atteindre un « accord des volontés » dans les échanges informationnels actuels⁴⁷⁴, une prémisse pourtant essentielle en droit des contrats.

Tout cela se joue sur fond d'importantes asymétries de pouvoir. Les grandes organisations ont accès à tant d'informations sur tant de personnes qu'elles en développent un capital informationnel considérable, qui confère à certaines le pouvoir de « contrôler ce que nous voyons, ce sur quoi nous cliquons, et dans plusieurs cas ce en quoi nous croyons⁴⁷⁵ ». Le contrôle individuel semble mal adapté à contrer ces

⁴⁷⁰ Une IA agentive est un « [s]ystème d'intelligence artificielle conçu pour agir de manière autonome et proactive, élaboré en vue de poursuivre des objectifs en planifiant des actions de façon itérative, d'utiliser des ressources ou des outils externes et de décomposer des problèmes complexes en sous-tâches afin de produire des sorties adaptées au contexte. » Voir OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « intelligence artificielle agentive », *Grand dictionnaire terminologique*, en ligne : <<https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26578856/intelligence-artificielle-agentive>> (consulté le 16 avril 2026); sur ce thème, voir par exemple INFORMATION COMMISSIONER'S OFFICE, « ICO tech futures: Agentic AI » (8 janvier 2026), en ligne : <<https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/tech-horizons-and-ico-tech-futures/ico-tech-futures-agentic-ai/>> (consulté le 9 janvier 2026).

⁴⁷¹ Voir notamment Régis CHATELLIER, « [Article 1/2] Les neurotechnologies, à la conquête du cerveau », *Laboratoire d'innovation numérique de la CNIL* (1 octobre 2025), en ligne : <<https://linc.cnil.fr/article-12-les-neurotechnologies-la-conquete-du-cerveau>>; Régis CHATELLIER, « [Article 2/2] Des neurodonnées, personnelles, pas comme les autres... », *Laboratoire d'innovation numérique de la CNIL* (1 octobre 2025), en ligne : <<https://linc.cnil.fr/article-22-des-neurodonnees-personnelles-pas-comme-les-autres>>.

⁴⁷² Voir notamment INFORMATION COMMISSIONER'S OFFICE, *ICO tech futures: Quantum technologies*, 2024, en ligne : <<https://ico.org.uk/media/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/ico-tech-futures-quantum-technologies-1-0.pdf>>.

⁴⁷³ Jennifer KING et Caroline MEINHARDT, *Rethinking Privacy in the AI Era. Policy Provocations for a Data-Centric World*, Stanford University Centre for Human-Centered Artificial Intelligence, 2024, p. 33, en ligne : <<https://hai.stanford.edu/sites/default/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf>>, notre traduction.

⁴⁷⁴ Ignacio COFONE, *The Privacy Fallacy: Harm and Power in the Information Economy*, Cambridge (Royaume-Uni); New York (États-Unis), Cambridge University Press, 2023, p. 4.

⁴⁷⁵ Neil M. RICHARDS et Woodrow HARTZOG, « A Relational Turn for Data Protection? », (2020) 6-4 *European Data Protection Law Review*, p. 1-2, DOI : 10.21552/edpl/2020/4/5, notre traduction.



phénomènes qui touchent toute la société et qui illustrent la dimension collective des problèmes de vie privée. Les effets possibles concernent aussi la démocratie et peuvent même l'affecter.

De leur côté, les balises procédurales dans les lois créent des conditions de légitimité des actions posées à l'aide de renseignements personnels plus qu'elles ne les limitent en substance⁴⁷⁶. Pour reprendre les mots du professeur expert en vie privée Ignacio Cofone, elles sous-protègent, mais surencadrent⁴⁷⁷. En effet, elles ne permettent pas toujours d'anticiper correctement les préjudices. Elles imposent un fardeau important en lien avec des pratiques pourtant peu risquées, et laissent en même temps des pratiques risquées avoir cours pour autant qu'elles soient conformes à la procédure. Corrélativement, cette approche exige des organisations qu'elles consacrent des ressources considérables à l'application de procédures, plutôt qu'à une véritable réflexion sur leurs pratiques. On a d'ailleurs pu constater, ces dernières années, à quel point les nouvelles obligations apportées par la Loi 25 sont considérées comme exigeantes par certaines organisations, en particulier les PME.

Dans cette section, la Commission expose la manière dont l'évolution sociotechnique des dernières années met en lumière les limites des fondements actuels des lois québécoises en matière de protection des renseignements personnels. La Loi 25 n'est entièrement en vigueur que depuis quelques années, et tous ses effets ne peuvent encore être pleinement mesurés. La Commission estime cependant que plusieurs des dispositions qu'elle a introduites doivent être renforcées. En effet, tout en soulignant de nombreuses limites du paradigme contractuel et des principes FIP, la Commission ne préconise pas pour autant de faire table rase des lois actuelles. Elles sont efficaces pour encadrer certains types de relations impliquant des renseignements personnels, et elles s'alignent à celles d'États comparables, ce qui favorise leur interopérabilité.

Dans la première partie de ce chapitre, la Commission formule ainsi plusieurs recommandations afin de renforcer et de prolonger l'encadrement établi dans les lois sur la protection des renseignements personnels à la suite de la Loi 25, en abordant successivement :

- le paradigme du contrôle individuel;
- le critère de nécessité;
- les inférences algorithmiques;
- le moissonnage de renseignements personnels;
- le courtage en données;
- l'anonymisation des renseignements personnels;
- l'évaluation des facteurs relatifs à la vie privée;
- les interfaces truquées;
- des enjeux particuliers relatifs à la vie privée des jeunes;
- les dispositions concernant la biométrie.

Dans la deuxième partie de ce chapitre, la Commission invite enfin à une vaste réflexion collective qui permettrait d'approfondir l'encadrement de la protection des renseignements personnels de demain.

⁴⁷⁶ *Id.*, p. 4.

⁴⁷⁷ I. COFONE, préc., note 474, p. 97-101.



2.1. Les éléments justifiant des ajustements aux lois actuelles

2.1.1. Le paradigme du contrôle individuel

Sommaire

Le contrôle des personnes à l'égard des renseignements qui les concernent, appuyé par la transparence et exprimé par le consentement ou l'exercice de droits, constitue l'un des principes maîtres des lois sur la protection des renseignements personnels. La Loi 25 n'a pas remis ce paradigme en question, renforçant plutôt le contrôle individuel de différentes façons. Toutefois, à la lumière des enjeux du monde numérique, la Commission doute que cette approche garantisse un niveau de protection satisfaisant de la vie privée, en particulier à la lumière de l'asymétrie de pouvoir qui existe entre les personnes et les organisations.

Cette section présente ainsi divers facteurs limitant l'efficacité du contrôle individuel, comme :

- l'insuffisance de l'information visant à appuyer la prise de décisions éclairées et les biais affectant ces décisions;
- la vaste étendue des pratiques numériques impliquant des renseignements personnels;
- l'imprévisibilité des inférences pouvant être tirées des renseignements personnels;
- l'absence fréquente d'interaction directe entre les personnes et les organisations;
- la dimension collective de la protection des renseignements personnels.

Elle formule des recommandations qui permettraient :

- d'adapter les règles du consentement à la réalité numérique;
- de clarifier, de simplifier et d'améliorer l'efficacité de l'information fournie aux personnes.

À la fin de ce chapitre, la Commission appelle à une réflexion élargie visant à revoir les fondements des lois sur la protection des renseignements personnels à la lumière des enjeux du numérique.



2.1.1.1. Contexte

Une idée maîtresse des principes FIP⁴⁷⁸, qui se traduit dans les lois québécoises sur la protection des renseignements personnels, veut que les personnes aient le contrôle de leurs renseignements personnels⁴⁷⁹. Trois éléments principaux permettent d'exercer ce contrôle :

- Le consentement.
- La transparence.
- Les droits des personnes concernées, notamment quant à l'accès aux renseignements personnels et à leur rectification.

Ces éléments visent à donner un certain pouvoir aux personnes dans leurs relations avec les organisations, mais ils atteignent de moins en moins cet objectif :

- **Le consentement** est une condition de légalité des pratiques impliquant des renseignements personnels dans de nombreux cas d'espèce et constitue ainsi l'une des clés de voûte actuelles du régime assurant leur protection. **Cependant, comme la Commission l'a déjà exprimé ces dernières années⁴⁸⁰, le consentement s'avère mal adapté à l'économie numérique. Ainsi, il ne peut remplir adéquatement le rôle que lui confient les lois, notamment en raison de l'échelle à laquelle sont traités les renseignements personnels aujourd'hui et du fait que les pratiques concernent des groupes plutôt que des individus.**
- **La transparence** vise à ce que les personnes concernées soient informées de l'utilisation de leurs renseignements personnels afin qu'elles puissent prendre de meilleures décisions et se prévaloir de leurs droits et de leurs recours. Si elle demeure un excellent principe, elle se heurte cependant elle aussi aux réalités actuelles et aux pratiques numériques. Ces pratiques sont d'une grande complexité, car elles impliquent une multitude d'acteurs et des technologies souvent peu comprises par le public. Cette situation complique la fourniture d'informations simples et claires, mais tout de même suffisamment complètes et exhaustives, permettant aux personnes de prendre des décisions éclairées.
- **Les droits conférés par les lois aux personnes concernées** leur permettent entre autres d'accéder à leurs renseignements personnels, de les faire rectifier ou encore de faire cesser leur diffusion. Malgré leur importance, ces droits ne parviennent pas eux non plus à rééquilibrer la relation entre les personnes et les organisations. C'est particulièrement vrai en raison de l'étendue des pratiques numériques : exercer ses droits auprès d'un très grand nombre d'organisations paraît fastidieux, voire irréaliste.

Dans cette section, la Commission explique davantage la manière dont les divers éléments propres au paradigme du contrôle individuel s'intègrent aux lois actuelles, puis en expose plusieurs limites, surtout

⁴⁷⁸ C'est-à-dire les *fair information practice principles* évoqués dans l'introduction du présent chapitre.

⁴⁷⁹ Solon BAROCAS et Helen NISSENBAUM, « Big Data's End Run around Anonymity and Consent », dans Julia LANE, Victoria STODDEN, Stefan BENDER et Helen NISSENBAUM (dir.), *Privacy, Big Data, and the Public Good*, 1^{re} éd., Cambridge University Press, 2014, p. 44-75 à la page 57, DOI : 10.1017/CBO9781107590205.004.

⁴⁸⁰ Voir par exemple COMMISSION D'ACCÈS À L'INFORMATION, *Projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels – Mémoire de la Commission d'accès à l'information présenté à la Commission des institutions dans le cadre des consultations particulières et auditions publiques*, 2020, p. 34 à 39, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_ME_PL-64.pdf>; Voir par exemple COMMISSION D'ACCÈS À L'INFORMATION, *Mieux protéger les renseignements personnels des jeunes à l'ère numérique*, 2022, p. 98 à 100, 103 à 105, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_RAP_RP_Jeunes.pdf>; COMMISSION D'ACCÈS À L'INFORMATION, *L'IA au travail : pour un meilleur encadrement. Mémoire de la Commission d'accès à l'information présenté au ministère du Travail dans le cadre de la consultation sur la transformation des milieux de travail par le numérique*, 2025, p. 5, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_ME_Transfo_Travail.pdf>.



liées aux pratiques numériques. Selon elle, ces limites contribuent à remettre en question la vision voulant que la vie privée corresponde au contrôle des personnes sur leurs renseignements personnels – elle y revient davantage dans la section 2.2 à la fin du présent chapitre. Néanmoins, compte tenu de la nécessité d'améliorer la situation à court terme, la Commission invite à certains changements pour donner plus de force au consentement et à la transparence.

2.1.1.2. Situation actuelle

Cette section expose la place qu'occupent actuellement le consentement, la transparence et les droits des personnes concernées au sein des lois québécoises sur la protection des renseignements personnels.

2.1.1.2.1. Le consentement

Le consentement constitue une condition de légalité applicable aux actions des organisations en matière de traitement de renseignements personnels. En vertu des lois, les organisations doivent généralement s'appuyer sur un consentement pour :

- utiliser des renseignements personnels⁴⁸¹;
- communiquer des renseignements personnels à des tiers⁴⁸²;
- recueillir directement, auprès d'un mineur de moins de 14 ans, un renseignement qui le concerne. Le consentement est alors donné par le titulaire de l'autorité parentale ou le tuteur⁴⁸³, sauf si cette collecte est manifestement au bénéfice du mineur;
- recueillir un renseignement auprès d'un tiers plutôt qu'auprès de la personne concernée, sauf exception, dans le secteur privé⁴⁸⁴.

Pour que le consentement atteigne son objectif, lorsqu'il est requis, les lois prévoient qu'il respecte certains critères garantissant sa validité⁴⁸⁵. Il doit ainsi être manifeste, libre, éclairé et spécifique, mais aussi granulaire, compréhensible, temporaire et distinct⁴⁸⁶.

Dans certaines situations, les organisations peuvent agir sans consentement, par exemple pour l'utilisation à des fins compatibles avec celles pour lesquelles les renseignements personnels ont été recueillis⁴⁸⁷ ou la communication en situation d'urgence mettant en danger la vie, la santé ou la sécurité⁴⁸⁸.

De plus, les lois établissent qu'une personne consent à l'utilisation et à la communication de renseignements personnels lorsqu'elle les fournit après avoir été dûment informée des fins qui justifient leur collecte⁴⁸⁹. Les organisations n'ont donc pas à demander activement le consentement pour ces fins.

Même lorsque le consentement est obtenu, le critère de nécessité, abordé plus en détail à la section 2.1.2, demeure cardinal. Lorsqu'il s'applique, il doit toujours être préalablement satisfait : le consentement

⁴⁸¹ Loi sur l'accès, art. 65.1; Loi sur le privé, art. 12; LRSSS, art. 5.

⁴⁸² Loi sur l'accès, art. 53, 59 et 88; Loi sur le privé, art. 13 et 40; LRSSS, art. 5.

⁴⁸³ Loi sur l'accès, art. 64.1; Loi sur le privé, art. 4.1.

⁴⁸⁴ Loi sur le privé, art. 6.

⁴⁸⁵ Loi sur l'accès, art. 53.1; Loi sur le privé, art. 14; LRSSS, art. 6.

⁴⁸⁶ Ces critères sont présentés en détails dans les lignes directrices de la Commission sur les critères de validité du consentement : COMMISSION D'ACCÈS À L'INFORMATION, *Lignes directrices 2023-1 - Consentement : critères de validité*, 2023, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_Criteres_Validite_Consentement.pdf>.

⁴⁸⁷ Loi sur l'accès, art. 65.1; Loi sur le privé, art. 12; LRSSS, art. 62.

⁴⁸⁸ Loi sur l'accès, art. 59; Loi sur le privé, art. 18; LRSSS, art. 74.

⁴⁸⁹ Loi sur l'accès, art. 65 et 65.0.2; Loi sur le privé, art. 8 et 8.3; LRSSS, art. 14 al. 4.



n'autorise pas les organisations à le contourner. Il agit donc comme critère cumulatif de légalité des actions posées avec des renseignements personnels.

2.1.1.2.2. La transparence

Plusieurs mesures de transparence sont prévues explicitement ou implicitement par les lois actuelles et témoignent de l'importance accordée par le législateur à ce principe.

Lors de la collecte auprès d'une personne concernée, l'organisation doit fournir une série d'informations, certaines par défaut, d'autres sur demande. Par exemple, elle doit toujours informer la personne de la finalité poursuivie, des moyens de la collecte et de ses droits d'accès, de rectification et de retrait de consentement⁴⁹⁰. Le cas échéant, elle doit notamment lui indiquer le nom des tiers ou les catégories de tiers à qui les renseignements personnels seront communiqués⁴⁹¹. Puisque le consentement doit être éclairé lorsqu'il intervient, il y a lieu d'établir une analogie entre les informations qu'une organisation est tenue de fournir lors de la collecte et celles qu'elle devrait fournir au moment de chaque demande de consentement⁴⁹².

Par ailleurs, la collecte de renseignements personnels par un moyen technologique impose la publication d'une politique de confidentialité par l'organisation⁴⁹³. Pour les organismes publics assujettis à la Loi sur l'accès, son contenu est prescrit par règlement⁴⁹⁴ et recoupe les informations que la Loi impose de fournir lors de la collecte.

Lorsqu'elles recueillent des renseignements personnels à l'aide d'une technologie permettant l'identification, la localisation ou le profilage, les organisations doivent informer les personnes qu'elles y ont recours et leur indiquer les moyens offerts pour activer ces fonctions⁴⁹⁵. Par voie de conséquence, ces fonctions doivent être désactivées par défaut⁴⁹⁶ : l'activation demandée aux personnes constitue là encore un moyen de contrôle offert aux personnes concernées.

Enfin, lorsqu'elles rendent une décision fondée exclusivement sur un traitement automatisé de renseignements personnels, les organisations doivent en informer les personnes concernées au plus tard lorsqu'elles leur annoncent la décision⁴⁹⁷. En cas de demande de ces personnes, les organisations doivent leur fournir des informations supplémentaires, notamment celles expliquant les raisons, les principaux facteurs et les paramètres ayant mené à la décision.

⁴⁹⁰ Loi sur l'accès, art. 65; Loi sur le privé, art. 8; LRSSS, art. 14.

⁴⁹¹ Loi sur l'accès, art. 65; Loi sur le privé, art. 8; LRSSS, art. 14.

⁴⁹² COMMISSION D'ACCÈS À L'INFORMATION, préc., note 486, sect. 3.3.

⁴⁹³ Loi sur l'accès, art. 63.4; Loi sur le privé, art. 8.2.

⁴⁹⁴ *Règlement sur les politiques de confidentialité des organismes publics recueillant des renseignements personnels par un moyen technologique*, RLRQ, c. A-2.1, r. 4.1.

⁴⁹⁵ Loi sur l'accès, art. 65.0.1; Loi sur le privé, art. 8.1; LRSSS, art. 15.

⁴⁹⁶ COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, COMMISSION D'ACCÈS À L'INFORMATION, COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE LA COLOMBIE-BRITANNIQUE, et COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ALBERTA, « Conclusions en vertu de la LPRPDE n° 2025-003: Enquête conjointe sur TikTok Pte. Ltd. menée par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta » (23 septembre 2025), par. 153, en ligne : <<https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2025/lprpde-2025-003/>> (consulté le 23 septembre 2025);

COMMISSION D'ACCÈS À L'INFORMATION, préc., note 486, sect. B.4; SECRÉTARIAT À LA RÉFORME DES INSTITUTIONS DÉMOCRATIQUES, À L'ACCÈS À L'INFORMATION ET À LA LAÏCITÉ, *Témoins de connexion*, 2024.

⁴⁹⁷ Loi sur l'accès, art. 65.2; Loi sur le privé, art. 12.1; LRSSS, art. 65.



2.1.1.2.3. Les droits des personnes concernées

Depuis les premières versions des lois sur la protection des renseignements personnels, en 1982 pour la Loi sur l'accès et en 1994 pour la Loi sur le privé, le Québec offre aux personnes concernées un droit d'accéder à leurs renseignements personnels⁴⁹⁸ et un droit de les faire rectifier s'ils sont inexacts, incomplets ou équivoques⁴⁹⁹. Ces droits, d'ailleurs issus du Code civil⁵⁰⁰, permettent aussi l'accès, par un proche, aux renseignements personnels d'une personne décédée si ses intérêts et ses droits sont en cause⁵⁰¹.

La Loi 25 a étendu le droit d'accès aux renseignements personnels, d'une part pour y intégrer un droit à la portabilité⁵⁰², c'est-à-dire à obtenir communication de certains renseignements dans un format technologique structuré et couramment utilisé, et d'autre part pour permettre aux proches d'une personne décédée d'avoir accès à ses renseignements pour des motifs de deuil⁵⁰³.

Les droits d'accès et de rectification ont également des pendant dans le secteur de la santé et des services sociaux, avec des nuances adaptées à son contexte⁵⁰⁴. En effet, les personnes concernées peuvent refuser l'accès à leurs renseignements de santé et de services sociaux selon certaines circonstances en matière de recherche⁵⁰⁵ ou restreindre l'accès à un tel renseignement à un intervenant ou à une catégorie d'intervenants donnée⁵⁰⁶.

En outre, les lois québécoises confèrent aux personnes concernées le droit :

- de demander la révision d'une décision entièrement automatisée par un membre du personnel d'une organisation⁵⁰⁷;
- d'exiger la cessation de la diffusion ou la désindexation d'un renseignement personnel, notamment si elles peuvent démontrer un préjudice grave ou une contravention à la loi ou à une ordonnance judiciaire, dans le secteur privé⁵⁰⁸;
- de s'opposer à l'utilisation d'un renseignement personnel pour des fins de prospection commerciale ou philanthropique, dans le secteur privé⁵⁰⁹;
- de refuser qu'un conjoint ou un proche parent accède à leurs renseignements personnels pour motifs de deuil⁵¹⁰.

La plupart de ces droits ont été ajoutés par la Loi 25.

2.1.1.3. Enjeux

La posture philosophique qui sous-tend le modèle du contrôle individuel repose sur l'idée que les personnes sont pleinement en mesure de prendre, dans leur intérêt fondamental, des décisions éclairées

⁴⁹⁸ Loi sur l'accès, art. 83; Loi sur le privé, art. 27.

⁴⁹⁹ Loi sur l'accès, art. 89; Loi sur le privé, art. 28.

⁵⁰⁰ *Code civil du Québec*, RLRQ, c. CCQ-1991, art. 38 à 40.

⁵⁰¹ Loi sur l'accès, art. 88.1; Loi sur le privé, art. 41.

⁵⁰² Loi sur l'accès, art. 84; Loi sur le privé, art. 27.

⁵⁰³ Loi sur l'accès, art. 88.0.1; Loi sur le privé, art. 40.1.

⁵⁰⁴ LRSSS, art. 17 à 19, 21 à 31, 66.

⁵⁰⁵ *Id.*, art. 8.

⁵⁰⁶ *Id.*, art. 7.

⁵⁰⁷ Loi sur l'accès, art. 65.2; Loi sur le privé, art. 12.1; LRSSS, art. 65.

⁵⁰⁸ Loi sur le privé, art. 28.1.

⁵⁰⁹ *Id.*, art. 22.

⁵¹⁰ Loi sur l'accès, art. 88.0.1; Loi sur le privé, art. 40.1; LRSSS, art. 8.



et rationnelles grâce aux outils de contrôle que leur offrent les lois sur la protection des renseignements personnels, soit le consentement, la transparence et les droits à l'égard des renseignements personnels.

Dans la pratique, en raison de nombreuses limites inhérentes à la cognition humaine et structurelles émergeant dans le contexte des pratiques numériques et abordées ci-après, les personnes ne sont souvent pas en mesure d'agir de manière à protéger efficacement leur vie privée au moyen de ces outils de contrôle.

La Commission note que nombre d'enjeux évoqués ci-bas sont particulièrement saillants lorsque des renseignements personnels sont utilisés à des fins commerciales, dans le secteur privé. Pour autant, ils s'appliquent également au secteur public, où la transformation numérique est bien engagée.

2.1.1.3.1. L'information est souvent insuffisante et les décisions sont sujettes à des raccourcis

La prise de décision éclairée implique que la personne concernée dispose d'informations suffisantes pour poser un jugement sur la situation et évaluer la portée de son accord. Elle doit entre autres comprendre les risques auxquels elle s'expose et les conséquences d'un refus.

Dans l'économie numérique, les enjeux tant de carence que de surabondance informationnelle et les biais décisionnels compromettent le caractère éclairé des décisions. Dans ce contexte, on évoque même parfois un « mythe de la rationalité⁵¹¹ ».

On sait ainsi que les politiques de confidentialité, qui sont la principale source d'information sur les pratiques numériques des organisations, ne sont dans la plupart des cas ni lues⁵¹² ni comprises⁵¹³. C'est d'ailleurs sur la base de ce constat que le législateur a imposé, avec la Loi 25, qu'elles soient rédigées en termes simples et clairs. En parallèle, toutefois, les lois exigent désormais que davantage d'informations soient fournies, dans l'objectif de permettre une compréhension suffisante des tenants et aboutissants des pratiques de traitement des renseignements personnels. **On voit ici se dessiner le paradoxe de la transparence : les lois reconnaissent qu'une certaine quantité d'information est requise pour que les personnes prennent une décision éclairée, mais simplifier et clarifier une politique de confidentialité engendre forcément une perte de précision de l'information⁵¹⁴.**

⁵¹¹ I. COFONE, préc., note 474, p. 29-32.

⁵¹² L'étude classique à ce sujet remonte à 2008 et montrait que déjà à l'époque, un Américain moyen devrait consacrer au bas mot 81 heures par année pour ne serait-ce que parcourir en diagonale les politiques de confidentialité des sites visités pendant cette période : Aleecia M McDONALD et Lorrie Faith CRANOR, « The cost of reading privacy policies », (2008) 4-3 *I/S: A Journal of Law and Policy for the Information Society* 543-568, en ligne : <<https://kb.osu.edu/bitstreams/a9510be5-b51e-526d-aea3-8e9636bc00cd/download>>; on sait que depuis, la longueur et la complexité des politiques n'ont fait que croître : Yousra JAVED et Ayesha SAJID, « A Systematic Review of Privacy Policy Literature », (2025) 57-2 *ACM Computing Surveys* 1-43, p. 11-13, DOI : 10.1145/3698393.

⁵¹³ Par exemple, un sondage mené en 2025 auprès de 1500 Canadiens de 16 ans ou plus montre que 71 % des répondants jugent plutôt (42 %) ou très (29 %) difficile de comprendre ces politiques : PHOENIX SPI, « Recherche sur l'opinion publique concernant les enjeux liés à la protection de la vie privée de 2024-2025 », *Commissariat à la protection de la vie privée du Canada* (31 mars 2025), en ligne : <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/2025/por_ca_2024-25/#fig19> (consulté le 25 novembre 2025).

⁵¹⁴ S. BAROCAS et H. NISSENBAUM, préc., note 479 aux pages 58-59; Daniel J. SOLOVE, « Privacy Self-Management and the Consent Dilemma », (2013) 126-7 *Harvard Law Review* 1880-1903, p. 1885, en ligne : <https://harvardlawreview.org/wp-content/uploads/2013/05/vol126_solove.pdf>.



Par ailleurs, même si l'on arrive à décrire succinctement et clairement les pratiques d'une organisation prise isolément, l'environnement numérique est lui-même profondément complexe. Il implique des technologies et des échanges informationnels qui dépassent le niveau de conscience et les connaissances d'une personne raisonnable et informée. **Ainsi, bien qu'elles recourent constamment aux technologies numériques, les personnes n'en saisissent pas tous les rouages ni les implications.**

Ces technologies sont même généralement conçues dans un objectif de simplicité d'utilisation et présentent des interfaces invisibilisant les traitements de renseignements personnels qu'elles entraînent. Même les spécialistes peinent à s'y retrouver dans cette complexité.

Par surcroît, même parfaitement informées, les personnes concernées peinent à évaluer correctement les conséquences de leur accord en raison de plusieurs facteurs⁵¹⁵. La recherche en sciences sociales montre que les gens prennent souvent leurs décisions en fonction de la façon dont les choix leur sont présentés, en recourant à des raccourcis décisionnels⁵¹⁶. Compte tenu de la complexité inhérente aux choix concernant la vie privée, en effet, ils s'appuient sur des réflexions simplifiées. Par exemple, ils jugent plus graves les risques qu'ils connaissent par rapport à ceux qu'ils ne connaissent pas, et envisagent difficilement les risques futurs associés à l'utilisation et à la communication de leurs renseignements personnels. Il faut dire que l'étendue des pratiques de traitement des renseignements et les possibilités inférentielles en découlant, en plus de la vitesse des innovations technologiques, rendent tout effort d'anticipation hasardeux.

En parallèle, il importe de souligner que les humains ont une conception intrinsèquement interpersonnelle de la vie privée, comme le démontrent des recherches en la matière⁵¹⁷. Autrement dit, les personnes interprètent les échanges informationnels avec les organisations de la même façon qu'elles voient ceux entre personnes physiques, avec des attentes similaires. Par exemple, dans leurs relations avec les organismes ou les entreprises, elles se concentrent sur les renseignements personnels qu'elles fournissent activement, parce que ce sont ces derniers qui ont le plus d'effet sur les relations interpersonnelles. Les personnes portent ainsi beaucoup moins attention aux renseignements qui sont observés ou inférés à leur sujet, lesquels échappent à leur vigilance. Ce sont pourtant ces derniers qui, de plus en plus, sont exploités par les organisations⁵¹⁸.

En somme, la nature éclairée du consentement reste théorique dans la sphère numérique⁵¹⁹.

⁵¹⁵ La Commission revient davantage sur ce sujet dans la section 2.1.8.3.1.

⁵¹⁶ D. J. SOLOVE, préc., note 514, p. 1887; I. COFONE, préc., note 474, p. 29.

⁵¹⁷ Sonia LIVINGSTONE, Mariya STOILOVA et Rishita NANDAGIRI, *Children's data and privacy online – Growing up in a digital age. An evidence review*, London School of Economics and Political Sciences, 2019, p. 23, en ligne : <https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf>; voir aussi COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, sect. 3.2.3.2.

⁵¹⁸ Mariya STOILOVA, Sonia LIVINGSTONE et Rishita NANDAGIRI, *Children's data and privacy online*, The London School of Economics and Political Science, 2021, p. 21-22, en ligne : <<https://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf>>.

⁵¹⁹ Michelle ALBERT-ROCHETTE, Clara LAVIS et Mathilde MEUNIER, « Protection de la vie privée dans le contexte des plateformes en ligne : les limites des fiducies de données et du devoir fiduciaire de loyauté », (2023) 28-1 *Lex Electronica*, p. 32, en ligne : <<https://www.lex-electronica.org/en/articles/vol28/num1/protection-de-la-vie-privee-dans-le-contexte-des-plateformes-en-ligne-les-limites-des-fiducies-de-donnees-et-du-devoir-fiduciaire-de-loyaute/>> (consulté le 13 août 2025).



2.1.1.3.2. Les facteurs temporels affectent le contrôle des personnes

Plusieurs aspects liés à la temporalité font obstacle à l'efficacité du modèle du contrôle individuel.

Au moment de prendre une décision en matière de renseignements personnels, les personnes tendent à se concentrer sur l'immédiateté. Si elles perçoivent un avantage dans l'instant, elles sont portées à ignorer les risques abstraits ou futurs. Or, cette perspective à court terme ne tient pas adéquatement compte du fait que les effets négatifs en matière de vie privée se manifestent généralement dans la durée.

« On peut ignorer une piqûre d'abeille, mais une centaine ou un millier peuvent être mortelles. Le préjudice des violations de la vie privée peut se développer graduellement dans le temps, mais les décisions à propos de la vie privée doivent être prises individuellement, isolément et longtemps d'avance⁵²⁰. »

L'instantanéité qui caractérise le numérique n'est pas propice à la rationalité décisionnelle. La nature dématérialisée et rapide des services numériques cantonne l'acte du consentement à une courte période temporelle⁵²¹. Beaucoup d'informations sont données en même temps, alors que plusieurs incitatifs encouragent la prise d'une décision immédiate. Conséquemment, la réflexion sur la portée du consentement est escamotée.

Il faut aussi souligner que dans la sphère numérique, le consentement est presque toujours demandé par une interface, et non par un humain. Cette façon de faire empêche les personnes de poser des questions pour bien comprendre. À cet égard, même si la Loi 25 a créé un devoir d'assistance, il n'est pas encore clairement établi qu'il soit bien implanté dans les pratiques des organisations ni bien adapté au contexte numérique. Il implique ainsi que les personnes investissent des efforts conséquents : interrompre leur démarche en ligne, téléphoner ou rédiger un courriel, attendre une réponse, voire effectuer un suivi... Si une telle démarche peut être envisageable isolément, son coût temporel devient vite intenable compte tenu de la multiplicité des contextes, en ligne, où des décisions en matière de vie privée sont exigées, comme il en sera question à la section 2.1.1.3.3.

Par ailleurs, la mémoire s'effrite avec le temps et, conséquemment, la nature prolongée des relations unissant désormais les utilisateurs à certaines organisations dans le monde numérique pose des défis. Ainsi, suivant l'architecture des lois québécoises, dont le point focal pour la fourniture d'informations se situe lors de la collecte initiale de renseignements personnels, les organisations campent dès le départ la manière dont les renseignements seront traités ultérieurement.

Prenons l'exemple d'une plateforme de média social portant sa politique de confidentialité à l'attention de la personne concernée lors de son inscription. En supposant que cette personne lise la politique, elle acquerra une compréhension contemporaine de ce qui se joue lorsqu'elle fournit ses renseignements personnels ou que l'organisation en observe ou en infère à son sujet. Mais son utilisation de la plateforme, souvent, se fait sur le long terme.

⁵²⁰ D. J. SOLOVE, préc., note 514, p. 1891, notre traduction.

⁵²¹ Yves POULLET, « Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle », (2021) 1 *Revue des affaires européennes* 87-101, p. 96, en ligne : <<https://researchportal.unamur.be/files/61104360/8792.pdf>>.



Ainsi, la personne peut s'être inscrite sur le média social en 2015 avec une certaine vision, à l'époque, des conséquences de ce choix et des paramètres de la relation en termes de traitement de renseignements personnels. Elle poursuit l'utilisation de la plateforme sans constamment revenir à la politique de confidentialité.

Cette personne se souvient-elle alors, une décennie plus tard, de ce qui peut advenir des photos qu'elle téléverse, des messages qu'elle publie, des mentions « j'aime » qu'elle attribue?

Certes, en cas de mise à jour de la politique de confidentialité, la Loi sur le privé prévoit que les personnes concernées en soient avisées⁵²², ce qui se traduit souvent par un courriel ou une notification éphémère sur la plateforme. Pour les raisons mentionnées dans la section 2.1.1.3.1, il y a lieu de douter que cette information soit lue et assimilée. Par conséquent, des années après avoir mené une réflexion initiale sur ce qu'implique la fréquentation du média social, la personne concernée continue à voir ses renseignements personnels collectés, utilisés et communiqués suivant des modalités dont elle n'est plus activement consciente.

Enfin, les moyens de contrôle offerts aux personnes permettent surtout d'agir *après coup*. On peut par exemple demander la révision d'une décision déjà prise, exiger la cessation d'une diffusion déjà opérée, retirer un consentement déjà donné ou demander la rectification de renseignements personnels dont on a constaté qu'ils sont erronés. Le fait de donner ou de retirer son consentement et l'exercice de ces droits ne sont donc pas des moyens optimaux d'éviter les préjudices.

2.1.1.3.3. L'étendue des pratiques complique la compréhension et l'exercice des droits

L'étendue du traitement des renseignements personnels, plus précisément le nombre d'acteurs impliqués et les relations complexes entre eux, dépasse désormais l'entendement. Cette situation mine elle aussi l'efficacité du modèle du contrôle individuel.

Dans les années 1980 et 1990, lors de l'adoption initiale des lois sur la protection des renseignements personnels au Québec, une personne entretenait un nombre limité de relations contractuelles impliquant des renseignements personnels⁵²³. Elle interagissait ainsi avec sa banque, son assureur, son employeur, son fournisseur de téléphonie, son garagiste, un journal, quelques professionnels, quelques organismes à but non lucratif, sa clinique médicale, quelques ministères et organismes publics... Eût-elle souhaité gérer sa vie privée de façon plus rigoureuse, elle aurait pu, moyennant certains efforts, dresser une liste assez exhaustive des organisations à contacter.

En 2026, le portrait a changé. En sus des relations évoquées ci-dessus, toujours bien d'actualité, il faut considérer une multitude d'interactions conscientes avec des services numériques : plateformes de diffusion de vidéo et de musique, outils d'**IA** et de productivité, jeux, téléphonie, médias sociaux... Mais surtout, ce sont les interactions inconscientes qui se sont multipliées. Même si l'expérience numérique est en partie concentrée sur certaines grandes plateformes, elle comporte aussi une importante part de décentralisation, en particulier dans l'installation d'applications et la simple navigation Web. Tous ces services impliquent le traitement de renseignements personnels. Mais ce n'est pas tout : chaque éditeur a des sous-traitants et des partenaires.

⁵²² Loi sur le privé, art. 8.2.

⁵²³ GROUPE DES POLITIQUES ET DE LA RECHERCHE DU COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 467, p. 7.



Ces tiers ont eux-mêmes leurs propres sous-traitants et partenaires, si bien que c'est un nombre exponentiel d'organisations qui traitent aujourd'hui les renseignements personnels, la plupart du temps à l'insu des personnes concernées.

Qui n'a pas déjà vu une bannière de témoins de connexion évoquant des centaines de publicitaires affiliés?

Les personnes n'ont tout simplement pas les ressources pour exercer un réel contrôle sur leurs renseignements personnels dans un tel environnement. Elles manquent de temps, et les limites inhérentes à la cognition humaine les empêchent de considérer autant d'information. Ces conditions affectent tant le consentement que la transparence et l'exercice de leurs droits.

Chacun est assailli, au quotidien, de demandes en lien avec l'utilisation et la communication de renseignements personnels, dès qu'il pose un geste aussi simple que d'entrer sur un site Web⁵²⁴. L'expérience numérique est en effet transactionnelle par nature. Elle est structurée par un échange d'informations et de services au sein duquel le consentement joue un rôle prépondérant : il est constamment sollicité. Or cette répétition lui fait perdre de son sens.

« Dès le moment où les gens allument un appareil, ils se voient offrir un "contrôle" sur leurs informations par le biais de politiques de confidentialité, de conditions d'utilisation et de bannières de consentement pour chaque site Web ou application visité ou utilisé. Ce déferlement incessant suffit à faire perdre la vigilance et à ce que nous cliquons sur tout ce qu'on nous propose de façon à pouvoir finalement utiliser le service⁵²⁵. »

Le vocable « lassitude du consentement » est utilisé pour décrire cette tendance, qui pousse les personnes à accepter machinalement les pratiques, de façon résignée, sans considérer le contexte ou les informations reçues⁵²⁶.

En outre, la quantité d'informations que devrait absorber une personne pour comprendre vraiment ce qui advient de ses renseignements personnels dans ce contexte est démesurée. Pourtant, la logique des lois voudrait qu'une personne prenne connaissance des informations fournies par chaque organisation avec laquelle elle entre directement en contact, mais aussi par toutes les organisations qui coopèrent avec celle-ci, et ainsi de suite, en cascade.

L'exercice des droits requiert quant à lui des démarches généralement formelles, impliquant des documents à teneur juridique, des échanges écrits et des justificatifs d'identité. Ainsi, les faire valoir auprès d'une multiplicité d'acteurs dont on ne connaît pas forcément l'identité s'avère presque impossible. Des auteurs y voient une bataille perdue d'avance⁵²⁷.

Il est vrai que l'exercice de certains droits est parfois partiellement automatisé dans l'environnement numérique. Par exemple, certaines plateformes de médias sociaux prévoient des fonctionnalités permettant de demander copie de l'ensemble de ses renseignements personnels. Dans le domaine de la

⁵²⁴ W. HARTZOG, préc., note 466, p. 973-977.

⁵²⁵ *Id.*, p. 975, notre traduction.

⁵²⁶ J. KING et C. MEINHARDT, préc., note 473, p. 33; Juliana ABRUSIO, « The (in)efficacy of consent for the processing of personal data », (2024) 6-1 *Humanities and Rights, Global network journal*, p. 181-182, DOI : 10.24861/2675-1038.v6i1.133.

⁵²⁷ I. COFONE, préc., note 474, p. 92-94; Daniel J. SOLOVE, « The Limitations of Privacy Rights », (2023) 98-3 *Notre Dame Law Review* 975-1036, p. 5, en ligne : <<https://scholarship.law.nd.edu/ndlr/vol98/iss3/1/>>.



santé et des services sociaux, des services numériques permettent également un accès sans formalité à des renseignements comme des résultats de tests. Toutefois, ces procédures automatisées n'existent que pour une minorité de services, que la personne est d'ailleurs pleinement consciente d'utiliser.

« Le problème rappelle les étudiants assiégés par des professeurs qui leur donnent collectivement trop de lectures chaque soir. De la perspective de chaque professeur, les lectures sont raisonnables pour une journée. Mais lorsque cinq ou six d'entre eux demandent simultanément le temps d'une soirée en lectures, la charge de travail totale devient beaucoup trop importante. Par conséquent, même si toutes les entreprises fournissaient des informations et des choix adéquats, ce problème de gestion des données persisterait; la personne moyenne n'a tout simplement pas assez de temps ou de ressources pour gérer toutes les entités qui détiennent ses données⁵²⁸. »

2.1.1.3.4. Les effets d'inférence peuvent révéler bien plus que le renseignement initialement visé par le contrôle

Le paradigme de l'inférence, dont il est question de façon détaillée dans la section 2.1.3, entraîne lui aussi des défaillances importantes pour le modèle du contrôle individuel.

En effet, bien que les personnes soient réputées capables d'évaluer les conséquences des décisions impliquant leurs renseignements personnels, elles ne peuvent savoir à l'avance ce que ces renseignements permettront d'inférer, ni à quel moment⁵²⁹. L'analyse « coût-bénéfice » que l'on attend d'elles est donc incomplète : elle doit se faire à la pièce, sans vue d'ensemble⁵³⁰. Ici encore, l'étendue des pratiques et leur dimension temporelle entrent en ligne de compte : il ne s'agit pas d'évaluer la combinaison possible de deux renseignements personnels, mais bien de milliers d'entre eux, et ce, dans un avenir dont les contours demeurent incertains. Par exemple, qui s'attendrait à ce que l'analyse de la musique qu'il écoute permette de deviner ultérieurement ses convictions politiques⁵³¹?

En parallèle, le caractère spécifique du consentement souffre du fait que les organisations elles-mêmes ne savent pas toujours d'emblée ce qu'elles pourraient inférer dans l'avenir sur la base des renseignements obtenus à un moment donné : « la valeur des mégadonnées découle du caractère inattendu des corrélations qu'elles peuvent révéler⁵³² ». Du point de vue des organisations, la transmission d'informations aux personnes concernées en application du principe de transparence devient particulièrement compliquée.

2.1.1.3.5. La diversité des modes d'obtention des renseignements rompt la prémisse d'interaction entre les personnes et les organisations

Le contrôle individuel s'incarne surtout lorsque la personne concernée est en interaction directe et active avec une organisation, par exemple lorsqu'elle s'inscrit à un service, lorsqu'elle discute avec un agent au téléphone, lorsqu'elle remplit un formulaire. Comme discuté dans la section 2.1.3.2, l'obligation

⁵²⁸ D. J. SOLOVE, préc., note 514, p. 1889, notre traduction.

⁵²⁹ Alicia SOLOW-NIEDERMAN, « Information Privacy and the Inference Economy », (2022) 117-2 *Northwestern University Law Review*, p. 378-379, en ligne : <<https://scholarlycommons.law.northwestern.edu/nulr/vol117/iss2/1>> (consulté le 18 novembre 2025).

⁵³⁰ D. J. SOLOVE, préc., note 514, p. 1890.

⁵³¹ Philippe MERCURE, « Étude: Dis-moi ce que tu écoutes, je te dirai pour qui tu votes », *La Presse* (19 novembre 2025), en ligne : <<https://www.lapresse.ca/dialogue/chroniques/2025-11-19/etude/dis-moi-ce-que-tu-ecoutes-je-te-dirai-pour-qui-tu-votes.php>> (consulté le 26 novembre 2025).

⁵³² S. BAROCAS et H. NISSENBAUM, préc., note 479 à la page 60, notre traduction.

d'information reflète cette prémisse interactionnelle. Les lois prescrivent que les informations soient données *au moment de la collecte auprès de la personne concernée*.

Les expressions utilisées dans les lois, comme « auprès de » ou « fournit », paraissent toutefois mal adaptées quand on tient compte de l'importance relative de chaque mode d'obtention de renseignements personnels par les organisations. Dans la sphère numérique, la prédominance de l'observation de renseignements personnels – c'est-à-dire la mise en données des comportements de la personne, et non la fourniture de renseignements – et de l'inférence empêchent ce moment interactionnel de survenir. Il n'y a alors pas d'occasion déterminée pour fournir des informations ni pour solliciter le consentement. Conséquemment, les personnes n'ont pas en tête l'objet même des droits qu'elles pourraient exercer. Il en résulte que des pratiques de traitement des renseignements personnels ont largement cours à leur insu.

Dans son rapport de 2022 sur la protection des renseignements personnels des jeunes dans le monde numérique, la Commission illustre différents modes d'obtention des renseignements personnels par le biais de l'image de l'iceberg⁵³³ :

Renseignements fournis

par les individus eux-mêmes, en général volontairement et consciemment

Niveau de conscience des personnes concernées

Renseignements observés

au sujet des individus au gré de leurs interactions avec des systèmes ou d'autres individus, souvent sans qu'ils en aient connaissance (on parle aussi de « traces » ou d'« empreintes »)

Renseignements inférés

au sujet des individus à partir d'analyses reposant sur des renseignements fournis, observés ou obtenus d'autres sources, qui impliquent souvent des algorithmes et des corrélations entre individus

Exemples

- Âge dans un formulaire
- Égoportrait publié en ligne

- Données de témoins de connexion
- Données de géolocalisation
- Historique de navigation
- Métadonnées

- Profil d'intérêts d'achats
- État émotionnel déduit
- Traits de caractères prédits
- Lieu de travail (à partir de la géolocalisation)

L'exemple du moissonnage des renseignements personnels, abordé plus en détail à la section 2.1.4, illustre bien ces difficultés. On peut également souligner que de nombreux objets connectés recueillent des renseignements au sujet de personnes qui ne sont pas impliquées dans la relation plus « formelle » avec le fabricant⁵³⁴. C'est par exemple le cas des lunettes ou des enceintes connectées, qui recueillent l'image ou la voix des passants, ou encore des voitures connectées dont les capteurs saisissent les

⁵³³ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, p. 8.

⁵³⁴ Alexandre PLOURDE, « Retour vers le futur : l'Internet des objets et la protection de la vie privée », dans SERVICE DE LA QUALITÉ DE LA PROFESSION DU BARREAU DU QUÉBEC (dir.), *Développements récents en droit à la vie privée*, 465, coll. Développements récents, Montréal, Éditions Yvon Blais, 2019, p. 33-66 à la page 56.



renseignements des passagers et des passants, plutôt que seulement ceux du propriétaire – a fortiori lorsque les véhicules sont en location⁵³⁵.

2.1.1.3.6. Les choix peuvent être manipulés

Pour être libre, le consentement ne doit pas être influencé par une contrainte ou une pression induite. Pourtant, dans l'environnement numérique, en particulier commercial, plusieurs mécanismes, déployés à dessein ou encore sans intention trompeuse, orientent les choix des utilisateurs vers ceux qui profitent le plus aux organisations.

Ainsi, les interfaces ne sont pas neutres. Elles visent généralement à augmenter le taux de consentement. Pensons à :

- la mise en valeur visuelle de l'option la moins protectrice de la vie privée, par exemple l'activation d'une fonctionnalité invasive;
- l'utilisation d'un langage volontairement complexe et déroutant;
- l'emploi de mots et d'images faisant appel aux émotions.

D'autres stratégies peuvent être mises en œuvre pour décourager ou complexifier l'exercice des droits. Pour n'en donner qu'un exemple, plusieurs plateformes rendent l'option de supprimer un compte difficile à trouver et forcent les utilisateurs à passer par plusieurs étapes de confirmation de leur intention avant de finalement traiter la requête.

La Commission revient sur les interfaces truquées dans la section 2.1.8.

2.1.1.3.7. Les refus peuvent engendrer des coûts sociaux ou financiers importants

Le modèle du contrôle se heurte également à des facteurs sociaux et économiques qui diminuent encore davantage la possibilité d'un choix réellement libre et éclairé dans plusieurs situations. Ils engendrent une acceptation résignée et peu significative des pratiques. Refuser de consentir ou d'utiliser un service peut ainsi entraîner un coût important, qu'il soit perçu ou effectif.

Même dans un contexte d'interaction plus traditionnel (de personne à personne), lorsque les choix à faire impliquent des traitements complexes de renseignements personnels, les personnes peuvent percevoir des coûts liés à un refus potentiel de leur part. L'exemple suivant l'illustre.

Un nombre croissant de médecins et de professionnels de la santé et des services sociaux ont désormais recours à des systèmes d'**IA** permettant la transcription des interactions avec le patient, parfois appelés « scribes d'**IA** », pour faciliter la tenue de dossiers. Ces systèmes impliquent généralement l'enregistrement audio d'une rencontre, puis des opérations de reconnaissance vocale et de traitement automatique du langage, parfois opéré sur les serveurs d'un fournisseur tiers, afin de générer un résumé des faits saillants pouvant être intégré à un dossier médical électronique, par exemple⁵³⁶. Des renseignements de santé et de services sociaux sensibles sont donc utilisés et communiqués. À cet effet, Santé Québec et le Collège

⁵³⁵ Voir par exemple UNION DES CONSOMMATEURS, *Rapport final du projet de recherche - Voitures connectées : les consommateurs risquent-ils de perdre le contrôle?*, 2025, p. 42-43, en ligne : <https://uniondesconsommateurs.ca/wp-content/uploads/2025/12/20251204_RAPPORT_Voiture-connectee_FR_VFF.pdf>.

⁵³⁶ Lyes BACHATENE et Nathalie JOBIN, *Logiciels de transcription vocale basés sur l'IA en santé et en services sociaux : considérations pour leur déploiement à grande échelle (état des connaissances)*, Institut national d'excellence en santé et en services sociaux, 2026, p. 5, en ligne : <https://www.inesss.qc.ca/fileadmin/doc/INESSS/Rapports/Innov_non_pharma/Transcripteurs_IA_EC_INESSS.pdf>.



des médecins ont diffusé des orientations quant à l'utilisation de ces outils, qui préconisent l'obtention d'un consentement explicite auprès du patient⁵³⁷. Les professionnels sont encouragés à bien expliquer les raisons du recours aux scribes et leur implication en matière de traitement des renseignements de santé et de services sociaux. Celle-ci reste relativement complexes à appréhender.

Même s'il reçoit dûment toute l'information prévue par les lois, un patient déjà préoccupé par un problème relevant du domaine de la santé et des services sociaux, pouvant avoir attendu une longue période avant d'obtenir un rendez-vous, peut ne pas se trouver dans les meilleures conditions pour évaluer la possibilité de ne pas consentir. Il peut ainsi *percevoir* des risques associés à un éventuel refus, par exemple celui de se voir refuser les soins ou de déplaire au professionnel concerné.

Le coût du refus peut d'abord être social. Le consentement au traitement de renseignements personnels est souvent une condition d'utilisation des produits et services numériques ou d'accès à toutes leurs fonctionnalités. Le refus revient donc essentiellement à s'abstenir d'y avoir recours. La Commission soulignait en 2022⁵³⁸ que ce choix avait une forte incidence sur la socialisation des mineurs. Sensibles aux pairs et soucieux de se développer avec eux, ils font face à une forte pression pour fréquenter les espaces numériques sous peine d'exclusion.

Force est de constater que la même dynamique est à l'œuvre, peu importe l'âge. Ainsi, quelques plateformes permettant de réaliser des activités aussi courantes et essentielles que socialiser, effectuer des paiements ou s'informer concentrent les utilisateurs sur un nombre restreint d'espaces numériques, qui en deviennent incontournables. Chacun est alors plus ou moins obligé de s'y trouver, sous peine, par exemple, de ne plus être au courant de ce qui se passe dans sa communauté, de ne plus pouvoir aussi facilement participer à des activités ou de ne plus pouvoir échanger efficacement avec ses pairs.

Les outils numériques sont devenus de facto une condition d'une vie sociale et citoyenne satisfaisante⁵³⁹. Dans ce contexte, il serait difficile de plaider aujourd'hui que le recours au numérique – et aux traitements de renseignements personnels qu'il implique – est un véritable choix⁵⁴⁰.

⁵³⁷ Voir par exemple SANTÉ QUÉBEC, *Foire aux questions Scribes IA*, 2025, p. 6 et suiv., en ligne : <<https://cms.cmq.org/files/documents/Informations-cliniques/ia/sante-quebec-qr-scribes-ia.pdf>>; COLLÈGE DES MÉDECINS DU QUÉBEC, « Scribe et intelligence artificielle - Certification nécessaire et rappel quant au consentement » (14 janvier 2026), en ligne : <<https://www.cmq.org/en/pratiquer-la-medecine/informations-clinique/intelligence-artificielle/scribe-ia>> (consulté le 11 avril 2026).

⁵³⁸ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, p. 100.

⁵³⁹ Daniel J. SOLOVE, « The Myth of the Privacy Paradox », (2021) 89-1 *George Washington Law Review*, p. 37, DOI : 10.2139/ssrn.3536265; Fabien LECHEVALIER, « Les vulnérabilités inhérentes à l'approche individualiste des données de santé dans l'ère big data », (2020) 25-2 *Lex Electronica*, p. 54, en ligne : <<https://www.canlii.org/fr/doctrine/doc/2020CanLIIDocs3355>>.

⁵⁴⁰ I. COFONE, préc., note 474, p. 55-56; dans un arrêt de la Cour suprême de 2017, les juges majoritaires l'énoncent ainsi : « Le choix de « ne pas être en ligne » ne saurait constituer un choix véritable à l'ère d'Internet. » *Douez c. Facebook, Inc.*, 2017 CSC 33, par. 56, en ligne : <<https://decisions.scc-csc.ca/scc-csc/scc-csc/fr/item/16700/index.do>>.



« [...] [F]ace aux géants du numérique, le consentement des personnes sera souvent résigné sous peine de se voir refuser l'accès aux services ou de perdre certains avantages. La forme binaire du consentement (oui ou non) pourrait se résumer à opposer l'individu à la société ou la société à l'individu. Si les personnes n'acceptent pas le traitement de leurs données personnelles, elles se coupent alors de différents services qui s'avèrent aujourd'hui être une nécessité sociale – trouver un emploi, communiquer avec des ami·es ou des membres de la famille, accéder aux nouvelles ou participer à la vie politique⁵⁴¹. »

En plus d'être social, le coût du refus peut être financier. La gratuité de nombreux services en ligne n'est possible que parce que l'information génère de l'argent via la publicité ciblée, qui repose sur du profilage⁵⁴². Il en résulte une collecte, une utilisation et une communication en continu et à large échelle de renseignements personnels appuyant ce profilage et en étant issus. Ce modèle fait en sorte que la gratuité des services numériques n'est souvent réellement possible qu'à condition de céder ses renseignements personnels. Ainsi, les options gratuites impliquent généralement une collecte, une utilisation et une communication beaucoup plus importantes de renseignements personnels⁵⁴³. Les choix en la matière sont nécessairement affectés par cette dimension financière.

Cette transformation des renseignements personnels en monnaie d'échange est un phénomène observé de longue date, mais il est encore plus transparent aujourd'hui avec l'émergence du modèle « payer ou consentir ». L'expression désigne les cas où l'accès à un service numérique est bloqué à moins qu'une personne consente au traitement de ses renseignements personnels à des fins de publicité ciblée ou ne verse un montant d'argent. Autrement dit, il faut payer pour être à l'abri de ces pratiques.

Notre système économique voudrait que la concurrence permette d'atténuer ces effets. Les utilisateurs pourraient sélectionner d'autres plateformes ou services en fonction de leurs pratiques en matière de protection des renseignements personnels. **Cependant, l'environnement numérique est caractérisé par une forte concentration d'activités entre les mains de peu d'acteurs adoptant des pratiques similaires. On peut y voir un oligopole, voire un monopole dans certains secteurs.**

Dans ce contexte, les gens n'ont pas le choix ou le pouvoir d'aller voir ailleurs⁵⁴⁴ :

Une faiblesse fondamentale du cadre des principes FIP tient au fait qu'il suppose que les individus ont un niveau de contrôle et de pouvoir égal à celui des entreprises et des institutions qui recueillent et traitent leurs données. Cependant, ce n'est pas le cas. Souvent, les individus ne peuvent pas simplement choisir un autre produit ou service caractérisé par des pratiques de collecte de données plus respectueuses de la vie privée. Les pratiques monopolistiques du secteur de la technologie, l'enfermement propriétaire et un incitatif généralisé des entreprises à recueillir le plus de renseignements possibles affaiblissent la valeur compétitive de la vie privée, sauf dans de rares cas.

Conséquemment, les personnes continuent de consentir à des pratiques qui, pourtant, nuisent à leur vie privée. L'observation n'a pas échappé à ceux qui y ont vu un « paradoxe de la vie privée⁵⁴⁵ », puisque ce comportement ne concorde pas avec l'attachement que les personnes disent avoir à la protection de leur

⁵⁴¹ M. ALBERT-ROCHETTE, C. LAVIS et M. MEUNIER, préc., note 519, p. 30-31, références omises.

⁵⁴² Alexandre PLOURDE, *Le prix de la gratuité – Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne?*, Option consommateurs, 2015, p. 7, en ligne : <<https://ised-isde.canada.ca/site/recherche-dans-le-repertoire/fr/node/14642>>.

⁵⁴³ I. COFONE, préc., note 474, p. 56; J. KING et C. MEINHARDT, préc., note 473, p. 24.

⁵⁴⁴ J. KING et C. MEINHARDT, préc., note 473, p. 24, notre traduction.

⁵⁴⁵ I. COFONE, préc., note 474, p. 33; D. J. SOLOVE, préc., note 539, p. 6-11.



vie privée. Mais ce paradoxe n'est qu'apparent⁵⁴⁶ : il ne tient pas compte du contexte de résignation⁵⁴⁷. Ainsi, nombre de personnes ont intériorisé l'idée selon laquelle la cession de renseignements personnels, et donc l'acceptation d'une perte de vie privée, constitue une condition *sine qua non* à l'utilisation de services numériques dont il est devenu réellement difficile de se passer. Conséquemment, l'accord exprimé dans ce contexte risque d'être factice.

2.1.1.3.8. Le contrôle individuel peut servir de caution morale quant aux risques

L'omniprésence de la notion de consentement entretient l'idée que chacun exprime son accord avec ce qu'il advient de ses renseignements personnels, ce qui peut ensuite servir à justifier presque n'importe quelle action.

En effet, l'aura de simplicité intuitive et de force légitimatrice du consentement fait en sorte qu'il est demandé comme caution morale, même lorsqu'il n'est pas requis par les lois. Une telle pratique masque toutefois le fait que le respect du critère de nécessité demeure essentiel⁵⁴⁸. Conséquemment, on simplifie à outrance les enjeux entourant le traitement des renseignements personnels. Par exemple, il est courant de présenter une politique de confidentialité à un utilisateur et de lui demander s'il « l'accepte » globalement, ce qui mène à un « consentement » de façade.

« Le consentement est devenu un outil mécanique, une sorte de blanc-seing qui autorise le gestionnaire des données à "abuser" des renseignements. Ainsi, on peut relever un détournement fonctionnel puisque de la fonction initiale de protection qui est dévolue au consentement, on en est arrivé à lui faire assumer une fonction de permission⁵⁴⁹. »

En cas de problèmes subséquents, l'organisation peut rappeler à l'individu ce « consentement » qu'il a exprimé. On lui attribue ainsi une bonne part de la responsabilité des préjudices de vie privée qu'il peut subir⁵⁵⁰. Chacun dans la société a internalisé cette culpabilité, mais elle cache la responsabilité des organisations, qui sont celles qui ont le véritable contrôle sur leurs pratiques⁵⁵¹. En somme, le consentement renverse le fardeau de la protection.

2.1.1.3.9. La protection des renseignements personnels revêt une dimension collective

Vu la prémisse contractuelle des lois actuelles, la protection s'articule principalement dans le cadre de la relation entre chaque organisation et chaque personne, prises isolément⁵⁵². **Pourtant, les pratiques des organisations sont généralement applicables à toutes les personnes avec lesquelles elles interagissent, alors que les moyens de contrôle, eux, sont décorrélés et individualisés. Il en résulte une asymétrie de pouvoir.**

⁵⁴⁶ D. J. SOLOVE, préc., note 539, p. 22-33.

⁵⁴⁷ I. COFONE, préc., note 474, p. 32-38; D. J. SOLOVE, préc., note 539, p. 44-49; Meiling FONG et Zeynep ARSEL, « Pour protéger la vie privée en ligne, il faut d'abord s'attaquer à la "résignation numérique" », *The Conversation* (23 août 2023), DOI : 10.64628/AAP.wsfqp9nyk.

⁵⁴⁸ Voir la section 2.1.2.

⁵⁴⁹ Ledy Rivas ZANNOU, « Profilage en ligne et protection des renseignements personnels - Pour en finir avec le mythe du consentement », (2023) 101-1 *Revue du Barreau canadien*, p. 137-138, en ligne : <<https://www.canlii.org/fr/doctrines/doc/2023CanLIIDocs1147>>, références omises.

⁵⁵⁰ I. COFONE, préc., note 474, p. 95-96.

⁵⁵¹ Daniel J. SOLOVE et Woodrow HARTZOG, « Kafka in the Age of AI and the Futility of Privacy as Control », (2024) 104-4 *Boston University Law Review* 1021-1042, p. 1035-1036, en ligne : <<https://www.bu.edu/bulawreview/files/2024/06/SOLOVE-HARTZOG.pdf>>.

⁵⁵² F. LECHEVALIER, préc., note 539, p. 53.



Il faut ainsi constater que la protection des renseignements personnels doit maintenant être envisagée sous un angle collectif, puisqu'elle comprend une forte dimension sociale. S'il n'est pas possible de traiter de ces sujets ici de manière exhaustive, la Commission en dresse néanmoins les grandes lignes.

Considérons trois situations survenues ces dernières années :

1. Comme mentionné dans la section 2.1.3.2.1.3, l'application de questionnaires ayant nourri la firme Cambridge Analytica recueillait aussi des renseignements sur les amis de ses utilisateurs, complètement à leur insu et sans leur consentement.
2. En 2018, Joseph James DeAngelo est arrêté en Californie, en lien avec des meurtres survenus plus de 40 ans plus tôt dans cet État. Surnommé le « Golden State Killer », il est identifié par les policiers grâce à l'ADN d'un de ses cousins au troisième degré, c'est-à-dire qu'il partage avec lui un arrière-arrière-grand-parent⁵⁵³. Ce cousin a passé un test génétique récréatif, puis son ADN s'est retrouvé dans la banque GEDMatch, qui peut être utilisée à des fins de généalogie génétique d'enquête. Une étude parue la même année conclut que si le profil de 1 % d'une population d'intérêt se trouve dans une banque génétique, alors la police a environ 90 % de probabilité de trouver au moins un cousin au troisième degré de toute personne à partir d'un échantillon de son ADN⁵⁵⁴.
3. En 2025, un média révèle que les trajets de course d'un garde du corps de l'ancien premier ministre canadien Justin Trudeau, diffusés sur une application de partage de performances sportives, permettent de déduire certains lieux qu'il fréquente au quotidien ou lors de ses visites à l'étranger⁵⁵⁵. Le journal indique que ce risque, appelé « fitleaking », s'est matérialisé à bien d'autres reprises dans les dix dernières années⁵⁵⁶.

Ces situations montrent que ce à quoi chacun consent a aussi des répercussions sur autrui. Cet effet se manifeste de deux manières.

D'une part, la divulgation de nos renseignements personnels implique parfois de révéler ceux d'autres personnes⁵⁵⁷. Certains renseignements concernent aussi simultanément plusieurs individus⁵⁵⁸. C'est le cas, par exemple, des photographies de groupe. Une personne peut mettre en ligne une photo qui lui plaît, mais qui s'avère embarrassante pour d'autres personnes qui y figurent.

⁵⁵³ Jocelyn KAISER, « We will find you: DNA search used to nab Golden State Killer can home in on about 60% of white Americans », *Science* (11 octobre 2018), en ligne : <<https://www.science.org/content/article/we-will-find-you-dna-search-used-to-nab-golden-state-killer-can-home-about-60-white>> (consulté le 2 décembre 2025).

⁵⁵⁴ Yaniv ERLICH, Tal SHOR, Itsik PE'ER et Shai CARMI, « Identity inference of genomic data using long-range familial searches », (2018) 362-6415 *Science* 690-694, DOI : 10.1126/science.aau4832.

⁵⁵⁵ Jean-Hugues ROY, « Application sportive Strava | Trudeau exposé à une « faille de sécurité majeure » », *La Presse* (19 mars 2025), en ligne : <<https://www.lapresse.ca/actualites/application-sportive-strava/trudeau-expose-a-une-faille-de-securite-majeure/2025-03-19/c-est-un-risque-evident.php>> (consulté le 19 mars 2025).

⁵⁵⁶ Jean-Hugues ROY, « De nombreux précédents au « fitleaking » », *La Presse* (19 mars 2025), en ligne : <<https://www.lapresse.ca/actualites/application-sportive-strava/trudeau-expose-a-une-faille-de-securite-majeure/2025-03-19/de-nombreux-precedents-au-fitleaking.php>> (consulté le 19 mars 2025).

⁵⁵⁷ Ignacio COFONE, « The 23andMe data breach reveals the vulnerabilities of our interconnected data », *The Conversation* (22 octobre 2023), en ligne : <<http://theconversation.com/the-23andme-data-breach-reveals-the-vulnerabilities-of-our-interconnected-data-193615>> (consulté le 24 octobre 2023), notre traduction.

⁵⁵⁸ D. J. SOLOVE, préc., note 527, p. 14-15.



Cette nature partagée des renseignements personnels entre différentes personnes affecte sérieusement la valeur du consentement comme moyen de contrôle individuel⁵⁵⁹.

D'autre part, l'essentiel du phénomène des inférences algorithmiques décrit à la section 2.1.3 repose justement sur l'idée que les caractéristiques sont partagées entre individus, et corrélées entre elles. **C'est l'effet de réseau : l'agrégation de plusieurs points de données révèle plus que la somme de ces données en dévoilant des liens entre elles et en permettant des prédictions.**

Par exemple, si des milliers d'utilisateurs d'un service numérique qui déclarent être de genre masculin interagissent avec des contenus liés à la musculation, il devient trivial pour l'entreprise offrant le service de déduire qu'il est probable qu'un nouvel utilisateur de genre masculin soit intéressé par la musculation. Autrement dit, plus des renseignements personnels sont disponibles, notamment parce que des personnes les ont fournis ou ont consenti à ce qu'ils soient observés à leur sujet, moins le refus ultérieur d'autres personnes de consentir a d'effet. En effet, il est possible d'établir des patrons probabilistes et statistiques de relations entre les renseignements⁵⁶⁰. Il peut en découler une certaine tyrannie de la minorité, où les choix d'un faible nombre de personnes entraînent des conséquences pour la masse⁵⁶¹. Même si les personnes retiennent des informations qu'elles ne veulent pas divulguer, la possibilité demeure qu'elles soient inférées par des organisations, passant alors outre leur volonté.

« Il est possible que vous ne le sachiez pas, mais un algorithme d'IA utilisé pour trier les candidats a décidé que vous êtes trop risqué. [...] Il est sans importance que vous pratiquiez une bonne hygiène de vie privée numérique, soit en gardant la plupart de vos renseignements personnels pour vous, en évitant de partager vos opinions en ligne et en refusant que les applications et les sites Web vous suivent. Sur la base des détails limités qu'elle a sur vous, l'IA prédit comment vous vous comporterez au travail, en se fondant sur des patrons appris à partir d'innombrables autres personnes comme vous⁵⁶². »

La possibilité d'inférer de nouvelles informations sur des individus, mais également l'appréciation globale des comportements ainsi que des caractéristiques et du vécu humains découlant de ces patrons statistiques, confère aux organisations un pouvoir informationnel inégalé, que certains ont appelé « le point de vue divin »⁵⁶³. **Elles peuvent alors catégoriser, influencer, surveiller, voire contraindre. Les risques deviennent systémiques et dépassent forcément la sphère individuelle, que l'on a traditionnellement associée à la vie privée.**

Ces considérations ont amené de nombreux experts à se pencher davantage, ces dernières années, sur ce qui a été nommé « la vie privée de groupe »⁵⁶⁴. Le mot « groupe » peut désigner des communautés dont les membres font consciemment partie et auxquels ils s'identifient : pensons à des groupes

⁵⁵⁹ F. LECHEVALIER, préc., note 539, p. 53-55; I. COFONE, préc., note 474, p. 50; M. ALBERT-ROCHETTE, C. LAVIS et M. MEUNIER, préc., note 519, p. 33.

⁵⁶⁰ S. BAROCAS et H. NISSENBAUM, préc., note 479 aux pages 62-63.

⁵⁶¹ *Id.* à la page 61.

⁵⁶² Maximilian KASY, « Opinion | How A.I. Can Use Your Personal Data to Hurt Your Neighbor », *The New York Times* (2 novembre 2025), en ligne : <<https://www.nytimes.com/2025/11/02/opinion/ai-privacy.html>> (consulté le 13 novembre 2025), notre traduction.

⁵⁶³ Linnet TAYLOR, Luciano FLORIDI et Bart VAN DER SLOOT, « Introduction: A New Perspective on Privacy », dans Linnet TAYLOR, Luciano FLORIDI et Bart VAN DER SLOOT, *Group privacy: new challenges of data technologies*, coll. Philosophical studies series, Volume 126, Cham, Springer, 2017, p. 1-12 aux pages 3-4.

⁵⁶⁴ L. TAYLOR, L. FLORIDI et B. VAN DER SLOOT, préc., note 563.



sociodémographiques classiques, comme « les Québécois » ou « les adolescents », ou à des groupes d'intérêts comme un parti politique ou un club d'échecs. Mais ces experts se sont surtout concentrés sur les groupes « passifs », dont « l'existence [...] dépend de l'externe; c'est le regard des autres qui [leur] donne naissance⁵⁶⁵ ». Ces derniers émergent artificiellement, du fait que leurs membres partagent certaines caractéristiques observées ou inférées par des organisations, et peuvent faire l'objet de décisions, d'influence, ou de discrimination⁵⁶⁶ sans que ces membres en aient conscience⁵⁶⁷. Le fait que les personnes membres soient individuellement identifiables revêt peu d'importance : c'est leur appartenance au groupe qui les affecte⁵⁶⁸. Les groupes de ce genre sont potentiellement infinis⁵⁶⁹ :

[L]es personnes ayant consulté une fiche-produit sur un site transactionnel en ligne; les élèves qu'un algorithme a étiquetés [...] comme potentiels décrocheurs; les candidats à un poste considérés à haut potentiel en raison de leurs résultats à un test psychométrique; etc.

Dès lors, les experts appellent à penser la protection de la vie privée d'une façon plus collective, en se concentrant autant sur les effets globaux du pouvoir informationnel que sur ses effets individuels, que vise à juguler le modèle du contrôle. Par exemple, à l'égard des groupes, on propose de ne plus envisager « leur vie privée », en parlant des membres, mais bien « sa vie privée », en parlant du groupe⁵⁷⁰. Cela ramène à la dimension sociale de la vie privée : en plus de sa valeur intrinsèque, elle revêt une fonction instrumentale pour la réalisation d'autres droits fondamentaux, voire collectifs⁵⁷¹. On peut penser à la préservation de la liberté d'association, de l'autonomie morale de chacun ou de la liberté de parole et de pensée, à la protection contre la discrimination, ou encore à des valeurs comme le pluralisme et la démocratie⁵⁷². Il y a donc lieu de la protéger dans cette dimension, comme on le fait pour le droit à un environnement sain.

En synthèse, les risques de vie privée ne sont plus adéquatement envisagés en tant que succession de cas isolés. Les coûts et bénéfices des pratiques informationnelles sont mieux compris lorsqu'on les envisage « cumulativement et de manière holistique⁵⁷³ ». Le modèle du contrôle individuel a pour grande faiblesse de circonscrire à la sphère de l'individualité des décisions qui ont pourtant différentes composantes et d'importants effets sociaux, avec pour conséquence de renforcer les asymétries de pouvoir.

⁵⁶⁵ Simon DU PERRON, « La vie privée des groupes : nouveau cadre théorique pour une protection contre le profilage algorithmique », (2020) 25-2 *Lex Electronica* 36, p. 39, en ligne : <<https://www.canlii.org/fr/doctrine/doc/2020CanLIIDocs3354>>.

⁵⁶⁶ Jocelyn MACLURE et Sylvain AUCLAIR, *Penser le droit à la vie privée au regard des droits individuels et collectifs*, 2022, p. 29, en ligne : <https://www.fp.ulaval.ca/sites/fp.ulaval.ca/files/fp/professeurs/Rapport_de_recherche_2022.pdf>.

⁵⁶⁷ L. TAYLOR, L. FLORIDI et B. VAN DER SLOOT, préc., note 563 aux pages 7-8.

⁵⁶⁸ Pierre-Luc DÉZIEL, « Les limites du droit à la vie privée à l'ère de l'intelligence artificielle : groupes algorithmiques, contrôle individuel et cycle de traitement de l'information », (2018) 30-3 *Les Cahiers de propriété intellectuelle* 827-847, p. 839, en ligne : <<https://www.lespci.ca/articles/v30/n3/les-limites-du-droit-a-la-vie-privée-a-l-ère-de-l'intelligence-artificielle-groupes-algorithmiques-contrôle-individuel-et-cycle-de-traitement-de-l'information/>>.

⁵⁶⁹ Martin CARBONNEAU, *L'évaluation des risques et des préjudices portés à la vie privée en contexte de transformation numérique - Considérations éthiques autour de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi 25)*, mémoire de maîtrise, Université du Québec à Rimouski, 2022, p. 149, en ligne : <<https://semaphore.uqar.ca/id/eprint/2129/>>.

⁵⁷⁰ L. TAYLOR, L. FLORIDI et B. VAN DER SLOOT, préc., note 563 à la page 11; S. DU PERRON, préc., note 565, p. 40-42.

⁵⁷¹ S. DU PERRON, préc., note 565, p. 44; J. MACLURE et S. AUCLAIR, préc., note 566, p. 35-36.

⁵⁷² Alessandro MANTELERO, « Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection », (2016) 32-2 *Computer Law & Security Review* 238-255, p. 243, DOI : 10.1016/j.clsr.2016.01.014.

⁵⁷³ D. J. SOLOVE, préc., note 514, p. 1881, notre traduction.

2.1.1.4. Recommandations

À l'instar de nombreux auteurs⁵⁷⁴, la Commission estime qu'il n'est plus opportun que les lois sur la protection des renseignements personnels misent autant sur le contrôle individuel, du moins dans le monde numérique. Le contrôle à exercer devrait plutôt être celui, social et normatif, des pratiques et de l'environnement numériques⁵⁷⁵.

Cependant, dans l'attente d'une réflexion élargie et tournée vers l'avenir comme celle à laquelle invite la Commission à la fin du présent chapitre, dans la section 2.2, certaines modifications aux lois actuelles peuvent déjà améliorer le contrôle individuel. La Commission les recommande en considérant que les principes FIP continuent pour l'heure de structurer la protection des renseignements personnels dans le monde numérique.

2.1.1.4.1. Permettre l'expression unifiée du consentement pour certains types de communications numériques

La multiplication des bannières et des fenêtres d'autorisation au fil de la navigation engendre une lassitude de consentement et peut décourager les personnes de refuser : qu'elles soient en accord ou en désaccord avec les traitements de renseignements personnels concernés, elles doivent ainsi sans cesse réitérer leurs choix. Pour la Commission, leur permettre d'exprimer une seule fois leurs choix constituerait une solution intéressante.

Diverses propositions techniques ont émergé au fil des ans pour atteindre cet objectif. L'idée est d'enregistrer un signal de consentement, aussi appelé indication de consentement automatisée, dans un navigateur ou un magasin d'applications, et de le transmettre aux organisations afin qu'elles se conforment à la volonté exprimée par l'utilisateur. La Commission présente certaines de ces initiatives plus en détail dans la section 2.1.1.5.1 et y fait état de diverses lois imposant désormais d'y recourir.

Les signaux de consentement présentent certaines limites. Entre autres :

- Ils semblent jusqu'ici incompatibles avec l'idée de granularité du consentement, car ils renferment une valeur binaire d'acceptation ou de refus.
- Ils ne peuvent concerner qu'un type de consentement, à savoir celui à la communication de renseignements personnels à des tiers ou au dépôt de témoins de connexion tiers, ce qui ne reflète pas nécessairement les besoins de toutes les relations numériques fondées sur les renseignements personnels⁵⁷⁶.
- Généralement, un éditeur de site ou d'application qui accepte un tel signal peut malgré tout afficher une bannière ou une fenêtre d'autorisation présentant des choix, mais en ajoutant simplement une mention selon laquelle la préférence déjà consignée de l'utilisateur, si aucune action n'est posée, sera respectée.

Même si les signaux de consentement ne peuvent régler tous les enjeux du suivi en ligne, ils constituent tout de même un moyen d'améliorer l'exercice du consentement par les personnes concernées. La Commission recommande ainsi au législateur de s'inspirer de la proposition étudiée par l'Union

⁵⁷⁴ S. BAROCAS et H. NISSENBAUM, préc., note 479 aux pages 56-58; D. J. SOLOVE et W. HARTZOG, préc., note 551, p. 1039-1042; J. KING et C. MEINHARDT, préc., note 473, p. 25; I. COFONE, préc., note 474, p. 44.

⁵⁷⁵ D. J. SOLOVE, préc., note 527, p. 5-6.

⁵⁷⁶ D. J. SOLOVE, préc., note 514, p. 1902.



européenne⁵⁷⁷ pour légiférer sur cette question et, ainsi, que les organisations soient tenues de respecter les indications de consentement automatisées. Corollairement, les entreprises offrant des navigateurs ou des magasins d'application devraient être tenues de consigner et de relayer ces indications, dont la valeur par défaut devrait être le refus de consentir, puisque cette valeur assure le plus haut niveau de confidentialité. Les organisations devraient pouvoir être sanctionnées si elles n'ajustent pas leurs pratiques de manière à respecter l'indication automatisée.

Recommandation 27

Intégrer aux lois sur la protection des renseignements personnels un mécanisme permettant aux personnes concernées de formuler des indications de consentement automatisées, tout en prévoyant :

- une liste de protocoles permettant d'émettre de telles indications, comprise dans un règlement;
- le refus de consentir comme paramétrage par défaut de telles indications, si elles ne sont pas manuellement configurées par les personnes concernées;
- l'impossibilité que les éditeurs puissent redemander à la personne concernée de consentir si des indications ont déjà été données.

2.1.1.4.2. Rendre les avis aux personnes plus concrets et faire en sorte qu'ils soient affichés au moment opportun

Malgré les défis de transparence évoqués dans la section 2.1.1.3.1, la Commission note que certaines mesures peuvent tout de même être envisagées pour améliorer l'information transmise aux personnes concernées.

Premièrement, l'information peut être encore clarifiée en la rendant plus synthétique et digeste, ou encore plus évidente. Diverses possibilités à cet égard sont présentées dans la section 2.1.1.5.2, impliquant généralement de résumer les faits saillants des politiques de confidentialité par des images ou des indicateurs.

Deuxièmement, on peut agir pour que les informations soient fournies au moment opportun aux personnes concernées. C'est l'approche « juste à temps », préconisée par diverses autorités de protection des renseignements personnels. Le Commissariat à la protection de la vie privée du Canada (le CPVPC), entre autres, explique dans ses lignes directrices sur le consentement⁵⁷⁸ que, compte tenu du sentiment d'urgence et de l'instantanéité des décisions en ligne, il est utile que les informations pertinentes à un choix soient présentées immédiatement avant ce choix, plutôt que longtemps à l'avance ou dans un document distinct. Selon l'autorité, la fourniture d'informations « juste à temps » peut, par exemple, se traduire par :

⁵⁷⁷ Voir la section 2.1.1.5.1.

⁵⁷⁸ COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Lignes directrices pour l'obtention d'un consentement valable » (13 août 2021), sect. 4, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gl_omc_201805/> (consulté le 17 novembre 2022).



- l’affichage d’une bulle d’information à proximité d’un champ de formulaire demandant l’âge d’une personne afin d’expliquer la raison pour laquelle ce renseignement est recueilli;
- le rappel des informations liées à la géolocalisation au moment où l’utilisateur est appelé à activer cette fonction pour la première fois plutôt que lors de l’inscription au service⁵⁷⁹.

La Commission est favorable à cette approche, qui permet d’éviter un long délai entre la réception de l’information par la personne concernée et le moment où elle en a besoin pour prendre une décision éclairée.

Recommandation 28

Obliger les organisations à résumer d’une façon simple et claire les faits saillants de leurs politiques de confidentialité, par exemple sous forme graphique, selon des modalités qui seraient déterminées par règlement.

Recommandation 29

Modifier les lois sur la protection des renseignements personnels afin que les organisations doivent fournir « juste à temps » les informations pertinentes à la prise de décision en matière de traitement de renseignements personnels, c’est-à-dire de manière contemporaine au choix.

2.1.1.5. Pour aller plus loin

La Commission présente ci-après des informations complémentaires relatives à ses recommandations, en ce qui a trait à l’expression unifiée du consentement et à la clarification de l’information fournie aux personnes.

2.1.1.5.1. L’expression unifiée du consentement numérique

Le signal Do Not Track⁵⁸⁰, apparu au début des années 2010 dans le cadre des travaux du World Wide Web Consortium (W3C), a constitué une première tentative d’opérationnaliser un mécanisme d’expression unifiée du consentement numérique. L’objectif était de créer une norme technique simple permettant aux internautes de consigner, à même leur navigateur, leur refus d’être suivis lors de leur navigation. Malgré une adoption initiale par plusieurs navigateurs, le signal Do Not Track a souffert du fait de ne pas être

⁵⁷⁹ *Id.*

⁵⁸⁰ W3C WORKING GROUP, « Tracking Preference Expression (DNT) », *World Wide Web Consortium* (17 janvier 2019), en ligne : <<https://www.w3.org/TR/tracking-dnt/>> (consulté le 1 décembre 2025).



légalement obligatoire. L'adhésion au signal était entièrement volontaire pour les entreprises, et peu d'acteurs de l'industrie publicitaire ont accepté de s'y conformer⁵⁸¹.

De façon plus contemporaine, un mécanisme analogue, le Global Privacy Control, gagne du terrain depuis quelques années et paraît prometteur⁵⁸². Il s'agit d'une initiative lancée en 2020 par une coalition regroupant à la fois des chercheurs universitaires, des médias, des organisations de défense des droits et des entreprises technologiques. Le Global Privacy Control se présente comme un paramètre intégré au navigateur ou à une extension. Lorsqu'il est activé, un signal est envoyé automatiquement aux sites visités (via un en-tête HTTP ou un script JavaScript) pour exprimer la volonté de l'utilisateur de refuser la vente ou la transmission de ses renseignements personnels.

Plusieurs navigateurs intègrent déjà le Global Privacy Control. En effet, des dizaines de millions d'internautes l'auraient déjà adopté, aux dires de ses développeurs⁵⁸³. Surtout, plusieurs lois adoptées ou actuellement à l'étude visent à obliger les éditeurs de sites à respecter un signal unifié de consentement comme le Global Privacy Control, dont plus d'une dizaine d'États américains comme la Californie⁵⁸⁴, le Colorado⁵⁸⁵ ou le Texas⁵⁸⁶.

Dans l'univers des appareils mobiles, certains ont avancé des mécanismes du même genre. Ainsi, Apple a introduit, en 2021, la fonctionnalité App Tracking Transparency⁵⁸⁷, qui impose aux applications d'obtenir un consentement explicite avant de pouvoir accéder à l'identifiant publicitaire unique de l'utilisateur, servant au ciblage publicitaire entre applications. Le signal de consentement est centralisé dans le système d'exploitation iOS, ce qui permet aux utilisateurs de refuser globalement le suivi d'un simple geste.

Comme les États américains précités, l'Union européenne s'intéresse elle aussi aux mécanismes d'expression unifiée du consentement, mais les envisage d'une manière plus large. Dans son projet de loi omnibus sur le numérique, elle songe à introduire au RGPD une obligation technologiquement neutre de respecter les « indications automatisées et lisibles par machine quant aux choix individuels⁵⁸⁸ ». La

⁵⁸¹ Sebastian ZIMMECK, Oliver WANG, Kuba ALICKI, Jocelyn WANG et Sophie ENG, « Usability and Enforceability of Global Privacy Control », (2023) 2023-2 *Proceedings on Privacy Enhancing Technologies Symposium*, p. 267, DOI : 10.56553/popets-2023-0052.

⁵⁸² « Take Control Of Your Privacy », en ligne : <<https://globalprivacycontrol.org/>> (consulté le 9 juillet 2025).

⁵⁸³ Aram ZUCKER-SCHARFF et Sebastian ZIMMECK, *How to Implement Global Privacy Control (GPC) for Publishers*, s. d., en ligne : <<https://globalprivacycontrol.org/Implementing%20GPC%20for%20Publishers.pdf>>.

⁵⁸⁴ *California Consumer Privacy Act of 2018*, code civil de la Californie, division 3, partie 4, titre 1.81.5, art. 1798.185 (a)(19) [ci-après CCPA], en ligne :

<https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5>.

⁵⁸⁵ *Colorado Privacy Act*, C.R.S. 6-1-1301, art. 1313, en ligne : <https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf>.

⁵⁸⁶ *Texas Data Privacy and Security Act*, Texas Business & Commerce Code, titre 11, section C [articles 541.001 à 541.205], art. 541.055(e) et (f), en ligne : <<https://capitol.texas.gov/tlodocs/88R/billtext/html/HB00004F.htm>>.

⁵⁸⁷ APPLE, « App Tracking Transparency », *Apple Developer Documentation*, en ligne : <<https://developer.apple.com/documentation/apptrackingtransparency>> (consulté le 19 août 2025);

« NSUserTrackingUsageDescription », *Apple Developer Documentation*, en ligne : <<https://developer.apple.com/documentation/bundleresources/information-property-list/nsusertrackingusagedescription>> (consulté le 19 août 2025).

⁵⁸⁸ Voir l'article 3 proposant l'ajout de l'article 88 *ter* au RGPD : COMMISSION EUROPÉENNE, *Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL modifiant les règlements (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 et (UE) 2023/2854 ainsi que les directives 2002/58/CE, (UE) 2022/2555 et (UE) 2022/2557 en ce qui concerne la simplification du cadre législatif numérique, et abrogeant les règlements (UE) 2018/1807, (UE) 2019/1150 et (UE) 2022/868 ainsi que la directive (UE) 2019/1024 (règlement omnibus numérique)*, COM(2025) 837 final (2025), en ligne : <<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52025PC0837>> (consulté le 2 décembre 2025); voir aussi la section 1 des notes explicatives, lorsqu'il est question des « indications automatisées et lisibles par machine quant aux choix individuels », de même que le considérant 46 de l'omnibus lui-même.



Commission européenne, dans ses notes explicatives, indique que l'objectif de cette terminologie est de permettre le recours à des signaux intégrés aux navigateurs ou aux systèmes d'exploitation mobiles, mais aussi à tout autre moyen technique susceptible d'être développé et permettant d'atteindre le même objectif. À cet égard, elle fait explicitement référence à la possibilité que des agents d'**IA** puissent « aider les utilisateurs à faire des choix en matière de consentement⁵⁸⁹ ». Fait à noter : la Commission européenne exclurait les entreprises œuvrant dans le domaine du journalisme de l'obligation de respecter ces signaux de consentement, du fait de l'« importance des flux de revenus en ligne pour le journalisme indépendant en tant que pilier indispensable d'une société démocratique⁵⁹⁰ ».

2.1.1.5.2. La clarification de l'information fournie aux personnes

Plusieurs options ont été proposées pour rendre plus digestes ou évidentes les informations fournies aux personnes en amont du traitement de leurs renseignements personnels.

Comme la Commission le mentionnait déjà en 2011⁵⁹¹, des pictogrammes peuvent être utilisés pour évoquer certaines pratiques typiques. L'initiative suisse Privacy Icons peut être inspirante à cet égard⁵⁹².

Une autre avenue consiste à recourir à des cotes permettant d'illustrer, en un coup d'œil, le niveau général de protection des renseignements personnels d'un produit ou d'un service, ou d'en évaluer certains aspects. C'est l'idée derrière le « Cyberscore » français, qui concerne la cybersécurité des sites Web et qui s'inspire du « Nutriscore » alimentaire, lequel devrait être établi par un auditeur externe⁵⁹³. Quoique la loi l'ayant introduit ait été adoptée, les règlements afférents au Cyberscore n'ont toujours pas été publiés à ce jour. Des chercheurs ont aussi proposé une méthodologie analogue permettant d'afficher, de façon superposée à un site Web, une cote lettrée découlant de l'analyse des politiques de confidentialité par **IA**⁵⁹⁴.

Pour aider à visualiser l'étendue de la toile d'acteurs impliqués dans la communication de renseignements en ligne, certains outils permettent aussi d'illustrer, par des graphes, les relations qui les unissent de façon à démontrer l'étendue de ces communications⁵⁹⁵.

En ce qui concerne le caractère évident des informations, certains ont exploré l'idée d'exiger que les avis aux personnes fassent davantage appel à leurs réponses émotionnelles pour leur permettre de prendre conscience des risques liés au traitement des renseignements personnels. Qualifiés de « viscéraux », ces avis stimuleraient un autre circuit cérébral que celui de l'analyse et de la réflexion.

⁵⁸⁹ *Id.*, notes explicatives.

⁵⁹⁰ *Id.*, notes explicatives.

⁵⁹¹ Rapport quinquennal 2011, p. 24-25.

⁵⁹² PRIVACY ICONS, « Icons as privacy notices for everyone » (2023), en ligne : <<https://privacy-icons.ch/en/>> (consulté le 23 avril 2024).

⁵⁹³ Loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public [France], en ligne : <<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045294275>>; « Cyberscore : la notation de la sécurité de vos données en ligne », *Cyberscore*.

⁵⁹⁴ Kimberly GARCIA, Aurelia TAMO-LARRIEUX, Yannic MEIER, Simon MAYER, Christoph LUTZ, Clement GUITTON, Leonardo STERN, Raffael ROT, Simeon PILZ et Stephan MULDER, « Visual Privacy: The Impact of Privacy Labels on Privacy Behaviors Online », 2025, doi : 10.31235/osf.io/5kthu_v1.

⁵⁹⁵ Alessandro ACQUISTI, Idris ADJERID, Rebecca BALEBAKO, Laura BRANDIMARTE, Lorrie Faith CRANOR, Saranga KOMANDURI, Pedro Giovanni LEON, Norman SADEH, Florian SCHAUB, Manya SLEEPER, Yang WANG et Shomir WILSON, « Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online », (2017) 50-3 *ACM Computing Surveys* 1-41, p. 16, doi : 10.1145/3054926.



« Les avis viscéraux diffèrent des avis traditionnels en ce qu'ils ne s'appuient pas nécessairement sur la description des pratiques par le biais des mots ou des symboles. À la place, ils misent sur l'expérience même du consommateur grâce à un produit ou à un service pour l'avertir ou l'informer⁵⁹⁶. »

Pour comparer simplement, il s'agit de la même stratégie que celle imposant d'afficher, sur les paquets de cigarettes, des images de lésions causées par le tabagisme. Dans le domaine de la vie privée, des avis viscéraux pourraient par exemple se traduire par⁵⁹⁷ :

- l'ajout d'éléments de design anthropomorphiques, comme des yeux qui suivent la souris sur un site, pour faire prendre conscience du suivi opéré;
- l'affichage de véritables renseignements personnels concernant l'utilisateur, comme son adresse IP, la ville où il se trouve, son navigateur et quelques centres d'intérêt, pour l'aider à réaliser qu'ils peuvent être recueillis.

⁵⁹⁶ Ryan CALO, « Against Notice Skepticism In Privacy (And Elsewhere) », (2012) 87-3 *Notre Dame Law Review* 1027-1072, p. 1033, en ligne : <<https://scholarship.law.nd.edu/ndlr/vol87/iss3/3/>>, notre traduction.

⁵⁹⁷ Victoria GROOM et Ryan CALO, *Reversing The Privacy Paradox: An Experimental Study*, *Telecommunications Policy Research Conference 2011*, 25 septembre 2011, en ligne : <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1993125>.



2.1.2. Le critère de nécessité

Sommaire

Le critère de nécessité enchâssé dans les lois sur la protection des renseignements personnels constitue une balise importante pour mettre en balance l'intérêt des organisations de traiter ces renseignements et le droit à la vie privée des personnes. En imposant des limites à la collecte, à l'utilisation, à la communication et à la conservation de renseignements personnels, cette balise doit permettre d'éviter que les organisations adoptent des pratiques préjudiciables pour la vie privée.

Dans la pratique, la Commission constate cependant que :

- le test permettant d'évaluer la nécessité est mal compris par les organisations et qu'il est appliqué de manière variable;
- la réflexion en matière de nécessité reste trop axée sur la phase de collecte des renseignements;
- certains obstacles compliquent ses activités de surveillance et de promotion du respect du critère de nécessité;
- cette balise se heurte à des obstacles nouveaux liés aux mégadonnées et à l'IA.

Afin d'améliorer la compréhension et l'opérationnalisation du critère de nécessité, la Commission recommande :

- d'explicitier le test de nécessité dans les lois, de même que l'étendue des situations où il s'applique;
- de faciliter l'opérationnalisation du critère de nécessité par des balises plus claires.

2.1.2.1. Contexte

Le droit à la vie privée est reconnu par la Charte⁵⁹⁸. L'atteinte à un tel droit peut être justifiée dans une société libre et démocratique si, d'une part, elle poursuit un objectif important, légitime et réel, et, d'autre part, elle est proportionnelle à cet objectif. Ces éléments sont au cœur du critère de nécessité énoncé dans les lois sur la protection des renseignements personnels, au Québec comme au Canada et dans d'autres juridictions. Les organisations peuvent ainsi recueillir, utiliser, communiquer et conserver des renseignements personnels, pourvu que ces traitements soient nécessaires.

Le critère de nécessité permet de mettre en balance les intérêts des personnes concernées et ceux des organisations, et sert donc de rempart contre les pratiques préjudiciables. Il permet d'incarner juridiquement le principe FIP de détermination des fins et celui de limitation de la collecte, de l'utilisation et de la communication.

⁵⁹⁸ Charte, art. 5.



Le critère de nécessité s'applique indépendamment du consentement des personnes concernées. Ainsi, face aux lacunes du paradigme du contrôle individuel mentionnées à la section 2.1.1, il se trouve à jouer un rôle névralgique en matière de protection des renseignements personnels. **En théorie, une application rigoureuse de cette balise devrait permettre d'éviter l'émergence de pratiques nuisibles ou disproportionnées dans l'atteinte causée à la vie privée des personnes. Toutefois, dans la pratique, l'évaluation des éléments devant être présents pour établir la nécessité pose des défis d'application.** Le respect du critère de nécessité se heurte aussi aux caractéristiques propres à l'**IA**.

Même si cette balise demeure incontournable, la Commission estime qu'elle doit être améliorée, principalement dans l'objectif d'y apporter une plus grande clarté. Après avoir présenté le cadre légal actuel, elle expose divers enjeux et présente des solutions qui pourraient aider à clarifier l'application du critère de nécessité.

2.1.2.2. Situation actuelle

Le principe de nécessité doit être considéré par les organisations tout au long du cycle de vie des renseignements personnels.

2.1.2.2.1. Le cadre légal

Étant donné que les lois actuelles mettent l'accent sur la phase de la collecte⁵⁹⁹, c'est principalement à cette étape que se manifeste explicitement l'obligation d'évaluer la nécessité. Un organisme public ne peut recueillir que les renseignements personnels *nécessaires* à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont il a la gestion, ou encore à celles d'un organisme public avec lequel il collabore⁶⁰⁰. Il en va de même pour un organisme du secteur de la santé et des services sociaux⁶⁰¹. Dans le secteur privé, une entreprise doit uniquement recueillir les renseignements *nécessaires* aux fins déterminées avant la collecte⁶⁰². Ces fins doivent répondre à un intérêt sérieux et légitime⁶⁰³. En cas de doute sur la nécessité d'un renseignement personnel, une organisation devrait s'abstenir de le recueillir.

Le terme « nécessaire » figure également dans d'autres dispositions, notamment en matière :

- de communication de renseignements personnels sans le consentement des personnes concernées ou d'accès, à l'intérieur d'une organisation, à un renseignement personnel⁶⁰⁴;
- d'utilisation sans le consentement des personnes concernées⁶⁰⁵.

2.1.2.2.2. L'interprétation du critère de nécessité

Historiquement, la notion de nécessité a été interprétée de diverses façons. Au cours des deux premières décennies de son existence, la Commission a ainsi fait valoir une interprétation⁶⁰⁶ :

⁵⁹⁹ Voir la section 2.1.3.

⁶⁰⁰ Loi sur l'accès, art. 64.

⁶⁰¹ LRSSS, art. 13.

⁶⁰² Loi sur le privé, art. 4 et 5.

⁶⁰³ *Id.*, art. 4.

⁶⁰⁴ Loi sur l'accès, art. 59, 60, 60.1, 62, 63.8, 67, 67.1, 67.2, 67.2.1, 67.2.3, 68; Loi sur le privé, art. 3.5, 18, 18.1, 18.3, 18.4, 20, 21, 21.0.2, 31; LRSSS, art. 22, 27, 30, 38, 39, 44, 50, 55, 64, 69, 72, 74, 75, 76, 77, 80, 108.

⁶⁰⁵ Loi sur l'accès, art. 65.1; Loi sur le privé, art. 12; LRSSS, art. 62.

⁶⁰⁶ *Laval (Société de transport de la Ville de) c. X*, [2003] C.A.I. 667, par. 22 (C.Q.), en ligne : <<https://canlii.ca/t/1btq1>>.



- « stricte et littérale »⁶⁰⁷, où l'adjectif « nécessaire » était associé à ce qui était « indispensable », « essentiel » ou « primordial », et non simplement « utile », « commode » ou « avantageux »;
- « relative et contextuelle »⁶⁰⁸, où le mot « nécessaire » était compris sur la base de sa définition courante de ce « qui n'est pas superflu ou sans pertinence »⁶⁰⁹.

En 2003, la Cour du Québec, dans le jugement *Société de transport de la Ville de Laval*, a écarté chacune de ces deux interprétations⁶¹⁰.

Il paraît donc improductif de se lier par une définition fixe de la nécessité et de se contraindre à une application technique de ce critère, sans considération pour les faits particuliers de chaque affaire, pour le type et la nature du renseignement litigieux et pour les finalités poursuivies par l'organisme. En conséquence, l'interprétation retenue devra permettre de formuler un critère plus dynamique, plus juste et mieux à même d'évaluer au mérite chaque situation.

La Cour a plutôt déterminé que la nécessité doit s'évaluer par un test semblable à celui développé par la Cour suprême du Canada dans l'arrêt *Oakes*⁶¹¹, ancré dans le droit constitutionnel.

Depuis ce jugement de la Cour du Québec, la Commission comme les organisations appliquent ce test en deux étapes :

- La fin poursuivie a un caractère important, légitime et réel.
- L'atteinte à la vie privée est proportionnelle à cette fin, ce qui signifie que :
 - la collecte, l'utilisation ou la communication des renseignements est rationnellement liée à la fin poursuivie;
 - l'atteinte au droit à la vie privée est minimisée;
 - la collecte, l'utilisation ou la communication du renseignement est nettement plus utile à l'organisation que préjudiciable à la personne concernée.

2.1.2.3. Enjeux

Plusieurs enjeux se posent aujourd'hui quant au critère de nécessité :

- Il est mal appliqué par les organisations, ce qui entraîne des pratiques non conformes.
- La réflexion en matière de nécessité est trop axée sur la phase de collecte des renseignements personnels.

⁶⁰⁷ Lukasz GRANOSIK, « Le critère de nécessité : son évolution, son importance, son impact et son application », dans SERVICE DE LA FORMATION CONTINUE DU BARREAU DU QUÉBEC (dir.), *Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé*, coll. Développements récents, n°392, Cowansville, Éditions Yvon Blais, 2014, p. 83-110 à la page 94, en ligne : <<https://app.caij.qc.ca/fr/doctrine/document/on/onafraat/-en>>; Pierre-Luc DÉZIEL, « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », dans SERVICE DE LA QUALITÉ DE LA PROFESSION DU BARREAU DU QUÉBEC (dir.), *Développements récents en droit à la vie privée*, coll. Développements récents, n°465, Montréal, Éditions Yvon Blais, 2019, p. 3-31 à la page 9, en ligne : <<https://app.caij.qc.ca/fr/doctrine/document/developpements-recents-vol-465-369051329-est-ce-bien-necessaire-le-principe-de-limitation-de-la-collecte-face-aux-defis-de-lintelligence-artificielle-et-des-donnees-massives>>.

⁶⁰⁸ L. GRANOSIK, préc., note 607 à la page 94.

⁶⁰⁹ P.-L. DÉZIEL, préc., note 607 à la page 12.

⁶¹⁰ *Laval (Société de transport de la Ville de) c. X*, préc., note 606, par. 30.

⁶¹¹ *R. c. Oakes*, [1986] 1 RCS 103 (Cour suprême du Canada), en ligne : <<https://scc-csc.lexum.com/scc-csc/scc-csc/fr/item/117/index.do>>.



- Certains obstacles compliquent la surveillance et la promotion de son respect par la Commission.
- Il se heurte à de nouveaux obstacles liés à l'IA et aux mégadonnées.

2.1.2.3.1. La mauvaise application du critère de nécessité engendre des pratiques non conformes

Le test de nécessité est un puissant outil de mise en balance des droits des uns et des autres dans les sociétés démocratiques. Cependant, le test de l'arrêt *Oakes* dont il découle a d'abord et avant tout été conçu pour être appliqué par les législateurs et les tribunaux, étant donné les connaissances en droit qu'il requiert.

Au fil des années, la Commission a pu constater dans un grand nombre de dossiers que la réflexion des organisations sur la nécessité, lorsqu'elle a bel et bien été menée, tend à être superficielle, de façon peu compatible avec l'importance du droit à la vie privée en cause.

Les assujettis faisant l'objet d'une intervention en surveillance se limitent souvent à affirmer à la Commission qu'ils « ont besoin » du renseignement personnel concerné, et donc qu'il leur est « nécessaire ». D'autres se justifient en évoquant des usages courants dans leur secteur d'activités. Ces arguments ne cadrent pas avec le degré d'exigence du test de nécessité évoqué dans la section 2.1.2.2.2.

Une partie du problème s'explique par le fait que la loi ne codifie pas ce test mis de l'avant par la Cour du Québec en 2003. Or, les lois sur la protection des renseignements personnels sont d'application très large et, malgré les efforts de vulgarisation de la Commission, aucun progrès substantiel n'est constaté dans l'application de ce critère au fil des ans.

Au demeurant, même si le test de nécessité était mieux compris et appliqué, sa nature contextuelle peut mener à des conclusions différentes dans des situations similaires. La Commission observe fréquemment des évaluations variables de ce test concernant des pratiques pourtant apparentées. Or, une mauvaise application du critère de nécessité engendre des pratiques non conformes aux exigences à la Loi, qui peuvent perdurer.

« Bien que nous considérions les limites prévues dans ces lois comme importantes, le fait qu'elles doivent être interprétées de manière contextuelle les rend difficiles à appliquer, sauf dans les cas les plus flagrants. Étant donné qu'il existe peu de limites strictes, c'est l'entreprise qui collecte les données qui décide si la pratique est raisonnable ou non. Un tribunal ou un organisme qui veille à l'application de la loi peut contester cette décision après coup et la juger déraisonnable, mais ce n'est qu'après que la collecte, l'utilisation et parfois la divulgation des données aient déjà eu lieu. À ce stade, le mal que tentait d'éviter la loi est fait⁶¹². »

En sus de ce qui précède, des obstacles importants minent l'autoévaluation de la nécessité par les organisations et affaiblissent globalement l'efficacité de cette balise.

Premièrement, le critère de nécessité s'évalue par rapport à une fin donnée. Or le spectre des finalités permises ou non peut être variable et vaste. Dans le secteur public, les fins poursuivies sont pour la plupart fixées dans des lois constitutives ou liées à l'application d'exigences légales, et c'est en regard de celles-ci, déjà légitimées par leur codification législative, que le test de nécessité doit s'effectuer.

⁶¹² UNION DES CONSOMMATEURS, préc., note 535, p. 102.



Cependant, dans le secteur privé, ce sont les entreprises qui déterminent elles-mêmes leurs finalités⁶¹³. La seule balise est que ces fins doivent répondre à un intérêt sérieux et légitime. Les entreprises jouissent ainsi d'une grande latitude dans la détermination de leurs fins⁶¹⁴. Pourtant, celles-ci constituent la clé de voûte de l'analyse subséquente de nécessité.

Deuxièmement, l'autoévaluation de la nécessité fait en sorte que la mise en balance d'intérêts revient à l'une des parties en cause. **Les organisations se trouvent à évaluer la proportionnalité de leurs propres pratiques, actuelles ou projetées, par rapport au droit à la vie privée des personnes concernées.** Il est alors peu surprenant que certaines d'entre elles sous-évaluent les préjudices potentiels pour ces personnes ou n'envisagent pas toujours toutes les perspectives. C'est encore plus vrai dans le secteur privé, où l'objectif premier n'est pas toujours l'intérêt public.

Par ailleurs, l'évaluation des risques est d'autant plus difficile que les contours exacts de la notion de vie privée ne sont pas clairement définis et que les préjudices possibles sont méconnus, diffus, généralement intangibles ou abstraits, et surtout cumulatifs. Ils sont généralement de faible ampleur lorsque pris isolément, mais deviennent majeurs lorsqu'on les considère dans leur ensemble, au niveau de la société en général.

Troisièmement, le critère de nécessité peut ne pas être satisfait. En toute logique, le test permettant de l'évaluer doit donc pouvoir mener les organisations, dans certaines circonstances, à conclure qu'elles ne peuvent adopter une pratique donnée parce qu'elle n'est pas nécessaire. En particulier dans le secteur privé, toutefois, elles doivent mener leur réflexion dans une atmosphère de course à la valorisation des renseignements personnels, associée à l'économie de la donnée. Pour atteindre des standards de compétitivité et d'efficience, les entreprises privées peuvent être incitées à collecter et à utiliser de plus en plus de renseignements personnels. Dès lors, la possibilité qu'elles concluent qu'une pratique n'est pas nécessaire est fortement réduite, puisque leur santé économique peut dépendre de leur adhésion à ce principe de valorisation. Bien que les incitatifs à l'œuvre soient différents, cette situation existe aussi dans le secteur public, dans une certaine mesure.

Dans le contexte actuel, l'autoévaluation du critère de nécessité par les organisations peut donc rendre cette balise illusoire. La plupart n'ont pas d'intérêt intrinsèque à s'abstenir d'agir pour des considérations liées à la vie privée d'autrui.

⁶¹³ Loi sur le privé, art. 5.

⁶¹⁴ Roger CLARKE, « Privacy impact assessment: Its origins and development », (2009) 25-2 *Computer Law & Security Review* 123-135, sect. 2, en ligne : <<https://www.rogerclarke.com/DV/PIAHist-08.html>> (consulté le 22 octobre 2024).



« [I]l paraît plutôt improbable qu'une organisation considère [des risques immatériels, sociétaux ou associés à la protection de la vie privée des groupes] dans ses processus d'évaluation. Devant ces préjudices hautement hypothétiques ou difficilement mesurables, elle trouverait encore ici très peu de leviers d'intervention, si ce n'est celui de ne pas mettre en œuvre de projets impliquant des renseignements personnels. De plus, en étant coincée dans un système économique misant massivement sur le recours aux données, l'organisation n'aurait sans doute pas beaucoup d'intérêt à les considérer, puisque ce faisant elle irait à l'encontre de ses intérêts stratégiques concrets et immédiats pour des considérations immatérielles et hypothétiques sur lesquelles elle aura peu de moyens d'intervenir si ce n'est, comme je l'ai mentionné, en s'abstenant d'agir tout simplement. Il paraît peu probable que les organisations optent pour une telle avenue considérant les diverses injonctions qu'elles subissent à se transformer numériquement⁶¹⁵. »

En somme, alors que le critère de nécessité devrait permettre d'éviter des pratiques disproportionnées, il perd de sa force du fait qu'il est mal compris et mal appliqué, et qu'il existe des facteurs systémiques faisant pencher la balance en faveur du traitement des renseignements personnels.

2.1.2.3.2. La réflexion en matière de nécessité est trop axée sur la collecte

Comme indiqué précédemment, le critère de nécessité est surtout mis en application lors de la phase de collecte des renseignements personnels.

Puisqu'il n'existe pas de renseignement mieux protégé que celui qui n'est pas recueilli, il est évidemment essentiel que la nécessité soit évaluée dès le départ. Cependant, cette balise devrait être considérée chaque fois qu'une pratique pouvant porter atteinte à la vie privée est envisagée pour une *fin* donnée, ce qui englobe donc la collecte, l'utilisation, la communication et la conservation⁶¹⁶. C'est d'ailleurs ce que veulent les principes FIP de limitation de la collecte, de l'utilisation et de la communication.

La codification actuelle de la nécessité ne reflète pas suffisamment cet état de fait. En effet, elle n'est pas explicitement mentionnée pour toutes les communications et les utilisations de renseignements personnels.

2.1.2.3.3. Certains obstacles compliquent la surveillance et la promotion du respect du critère de nécessité par la Commission

Vu le rôle névralgique de la nécessité dans le régime québécois de protection des renseignements personnels, une proportion importante des plaintes que la Commission reçoit année après année concerne l'application de ce critère.

L'intervention de la Commission survient généralement après la mise en place d'une pratique donnée. Elle est donc souvent curative.

Par ailleurs, la surveillance de certaines pratiques problématiques récurrentes pose certaines difficultés. En effet, la Commission est souvent appelée à se pencher sur des pratiques similaires lorsqu'il s'agit de nécessité. Elle devrait, en principe, pouvoir en tirer des conclusions claires lui permettant de fournir des

⁶¹⁵ M. CARBONNEAU, préc., note 569, p. 124-125.

⁶¹⁶ L. GRANOSIK, préc., note 607 à la page 85.



orientations par le biais de guides, ou même de lignes directrices, comme le prévoit la Loi⁶¹⁷. **Cependant, en raison de la nature contextuelle du test de nécessité, une analyse doit être menée pour chaque cas d'espèce⁶¹⁸.** Il lui est donc parfois difficile de généraliser ses constats précédents pour tracer des lignes claires à respecter par les assujettis en général.

Deux exemples permettent d'illustrer les limites de l'approche actuelle : la collecte de renseignements personnels avant la location d'un logement et la vidéosurveillance.

2.1.2.3.3.1. La collecte de renseignements avant la location d'un logement

Avant de conclure un bail avec un aspirant locataire, les locateurs recueillent des renseignements personnels à son sujet. En principe, ces informations doivent permettre d'établir l'identité du locataire, sa capacité de payer et son bon comportement. La Commission recommande de limiter les renseignements personnels collectés pour atteindre ces fins, en préconisant par exemple de demander⁶¹⁹ :

- à voir une pièce d'identité avec photo plutôt que d'en produire une photocopie ou d'en demander une photo par voie électronique;
- à obtenir des attestations concernant les bonnes habitudes de paiement, ou encore à consulter un dossier de crédit, avec consentement;
- à obtenir des références d'anciens locateurs.

En pratique, bon nombre de locateurs demandent une variété importante de renseignements d'une manière qui n'est pas proportionnelle à leurs finalités. Dans certains cas examinés par la Commission, certains recueillaient, auprès des aspirants locataires :

- des feuillets fiscaux de type T4;
- plusieurs bulletins de paie complets;
- la marque et le modèle du véhicule ou son numéro de plaque d'immatriculation;
- le salaire, le poste occupé, l'ancienneté, le statut d'emploi;
- le numéro de compte bancaire ou de folio;
- des photocopies de cartes de crédit;
- des avis de cotisation.

Malgré la diffusion d'outils d'informations pour le public et des décisions rendues par la Commission depuis 1995⁶²⁰, la Commission continue de recevoir, année après année, un nombre important de plaintes et de questions en matière de location de logement. L'exemple le plus typique de renseignement recueilli systématiquement est le numéro d'assurance sociale. La justification avancée est l'identification unique de personnes qui pourraient avoir des homonymes lors de la consultation du dossier de crédit.

⁶¹⁷ Loi sur l'accès, art. 123, par. 9.

⁶¹⁸ Rappelons que la Cour du Québec, dans l'affaire Laval, a rejeté l'idée selon laquelle la nécessité pouvait s'apprécier d'une manière plus « fixe » et technique. *Laval (Société de transport de la Ville de) c. X*, préc., note 606.

⁶¹⁹ COMMISSION D'ACCÈS À L'INFORMATION, « Signature d'un bail », en ligne : <<https://www.cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-d-interet/signature-bail>> (consulté le 14 avril 2026).

⁶²⁰ Voir par exemple *Regroupement des comités logement et associations de locataires du Québec et Corporation des propriétaires immobiliers du Québec*, [1995] C.A.I. 370 et 371; COMMISSION D'ACCÈS À L'INFORMATION, *Julien c. Domaine Laudance*, dossier C.A.I. PV 01 02 95, 2003; *Perreault c. Blondin*, [2006] C.A.I. 162; COMMISSION D'ACCÈS À L'INFORMATION, *X. et Y. et Gestion P. Laflèche*, dossier C.A.I. 09 18 86, 2013; COMMISSION D'ACCÈS À L'INFORMATION, *X. c. Habitations populaires du Québec*, dossier C.A.I. 10 04 75 et 10 06 09, 2013; COMMISSION D'ACCÈS À L'INFORMATION, *Services d'enquêtes Oligny et Thibodeau*, dossier 1008641-S, 2018, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/decisions-en-surveillance/1008641-S_decision-cai-services-enquetes-oligny-et-thibodeau-2018-02-20.pdf>.



Dans plusieurs décisions rendues jusqu'en 2018, la Commission avait établi que le numéro d'assurance sociale n'était pas nécessaire. Or, dans un jugement de 2018, la Cour du Québec a déterminé que la Commission avait appliqué ses conclusions antérieures sans mener une analyse contextuelle du cas à l'étude⁶²¹. Cette décision constitue un rappel des limites, pour la Commission, à la possibilité de généraliser ses décisions de surveillance en ce qui a trait au critère de nécessité, que ce soit pour des dossiers subséquents ou en matière de promotion.

Plusieurs formulaires de location, dont ceux proposés par des associations de locataires, prévoient ainsi toujours un champ pour le numéro d'assurance sociale. Étant donné que se loger est un besoin primaire et que le contexte actuel d'accès au logement est défavorable, les aspirants locataires n'osent souvent pas refuser de fournir les renseignements demandés, bien qu'ils puissent leur paraître excessifs. Malgré la protection prévue à la Loi⁶²², ils craignent de rater une occasion de location. La Commission constate régulièrement que les locataires n'ont pas considéré ses décisions antérieures et ses documents de promotion dans leur évaluation de la nécessité de demander ces renseignements.

En somme, bien que la Commission tente de donner des orientations unifiées pour les situations comparables afin de clarifier les obligations des entreprises, la jurisprudence actuelle établit que l'évaluation de nécessité doit se faire au cas par cas.

2.1.2.3.3.2. La vidéosurveillance

L'utilisation des caméras de surveillance est courante et même en progression, que ce soit dans la sphère publique ou la sphère privée. Chaque année, la Commission reçoit plusieurs plaintes quant à l'installation ou l'utilisation de systèmes de vidéosurveillance, employés dans différents contextes, comme dans les aires communes et privées d'immeubles à logements ou de copropriétés, des cabines de camions, des toilettes et vestiaires, des services de garde, etc. Certaines organisations se permettent également de filmer et d'enregistrer des rencontres avec leurs employés.

Bien que la Commission ait rendu plusieurs décisions balisant cette pratique au fil du temps⁶²³, plusieurs problèmes liés à l'application du critère de nécessité perdurent. Par exemple :

- La finalité justifiant l'installation et l'utilisation des caméras n'est pas toujours adéquate.
- Des paramètres comme l'angle de prise de vue et la durée de conservation des bandes vidéo peuvent affecter la proportionnalité de la pratique.

L'augmentation des plaintes quant à l'utilisation de caméras de surveillance soulève des inquiétudes sur l'ampleur de la problématique et le respect accordé à la vie privée.

⁶²¹ *Gestion immobilière GESCORP inc. c. Rioux*, 2018 CQ 5695, en ligne : <<https://canlii.ca/t/htj5m>>.

⁶²² Loi sur le privé, art. 9.

⁶²³ Voir par exemple COMMISSION D'ACCÈS À L'INFORMATION, *Garderie Excelsiori Daycare Inc.*, dossier 111756-S, 2015, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/decisions-en-surveillance/111756-S_decision-cai-garderie-excelsiori-daycare-inc-2015-02-09.pdf>; COMMISSION D'ACCÈS À L'INFORMATION, *Akelius Montréal Ltd.*, dossier 1015303-S, 2021, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/decisions-en-surveillance/1015303-S_decision-cai-akelius-montreal-ltd-2021-07-06.pdf>; COMMISSION D'ACCÈS À L'INFORMATION, *Association des copropriétaires du Lowney I*, dossier 1016882-S, 2021, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/decisions-en-surveillance/1016882-S_decision-cai-association-coproprietaires-lowney1-2021-05-05.pdf>; COMMISSION D'ACCÈS À L'INFORMATION, *Société 13859380 Canada Inc. (Crane Supply)*, dossier 1031833-S, 2025, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/decisions-en-surveillance/1031833-S_decision-cai-13859380-canada-inc-2025-05-20.pdf>.



2.1.2.3.4. Les mégadonnées et l'IA amènent des obstacles nouveaux pour l'évaluation du critère de nécessité

Le paradigme des mégadonnées et l'IA, des phénomènes abordés davantage dans la section 2.1.3, causent une remise en question de la détermination d'une fin précise en amont du traitement des renseignements personnels. Or, c'est de cette fin que dépend tout le test de nécessité⁶²⁴.

Ainsi, la collecte de données devient de plus en plus maximaliste⁶²⁵. Effectivement, en matière d'IA ou d'exploration de mégadonnées, la valeur des données réside davantage dans ce qu'elles permettent de découvrir une fois combinées et explorées⁶²⁶ que dans le fait de répondre à une fin connue d'avance.

Cela implique une rupture avec la séquence prévue par les principes FIP et les lois, qui veut que la fin soit déterminée *d'abord* et contribue *ensuite* à limiter la collecte, l'utilisation et la communication de renseignements personnels⁶²⁷.

Dans plusieurs cas, des organisations cherchent même à recueillir des renseignements personnels dans le seul objectif de créer des ensembles de données qui pourront par la suite être explorés et analysés pour diverses fins. L'accumulation de données devient la fin en soi. Cette tendance est notamment présente dans des activités comme le moissonnage ou le courtage en données, abordées respectivement dans les sections 2.1.4 et 2.1.5.

En recherche également, l'exploration de données a plus que jamais la cote, et les fins précises ne sont pas nécessairement déterminées aisément en amont⁶²⁸. La LRSSS le reconnaît d'ailleurs implicitement en permettant aux personnes de consentir à « des thématiques de recherche, des catégories d'activités de recherche ou des catégories de chercheurs⁶²⁹ ».

Bon nombre de systèmes d'IA peuvent quant à eux être créés pour accomplir plusieurs fins, ou être conçus sans a priori sur leurs objectifs. C'est le cas des systèmes d'IA génératifs, par exemple, dont on peut faire pratiquement n'importe quel usage. Dans ce contexte, bien qu'il soit possible pour une organisation utilisant un tel système d'évaluer la nécessité de recueillir ou d'utiliser des renseignements personnels par son entremise, il est beaucoup plus ardu d'évaluer celle de recueillir et d'utiliser des renseignements personnels pour *concevoir* le système alors que ses fins ne sont pas déterminées.

Face à cet enjeu, certaines autorités de protection des renseignements personnels suggèrent, à défaut de pouvoir cibler une finalité précise en amont, d'identifier à tout le moins très clairement le type de système développé et ses capacités envisagées⁶³⁰. Même si elle peut constituer une voie de passage dans le

⁶²⁴ P.-L. DÉZIEL, préc., note 568, p. 844-845.

⁶²⁵ P.-L. DÉZIEL, préc., note 607 à la page 3.

⁶²⁶ *Id.* aux pages 21-22.

⁶²⁷ J. MACLURE et S. AUCLAIR, préc., note 566, p. 39.

⁶²⁸ COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, « IA : Définir une finalité » (8 avril 2024), sect. « Comment définir la finalité du développement d'un système d'IA à des fins de recherche scientifique ? », en ligne : <<https://www.cnil.fr/fr/definir-une-finalite-0>> (consulté le 17 novembre 2025).

⁶²⁹ LRSSS, art. 6.

⁶³⁰ Par exemple, « développement d'un grand modèle de langage [...] capable de répondre à des questions, de générer du texte en fonction de contexte (courriels, lettres, rapports, y compris du code informatique), effectuer des traductions, résumés et corrections de texte, faire de la classification de texte, de l'analyse de sentiments, etc. ». Voir COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 628, sect. « Comment définir la finalité du traitement pour le développement de systèmes d'IA à usage général ? »



régime actuel, la liste des fonctionnalités de ces systèmes peut être longue et complique considérablement l'évaluation de la nécessité, rendant la balise difficilement applicable.

Conséquemment, il y a un potentiel d'incompatibilité entre ces nouvelles approches du traitement des renseignements personnels et le critère de nécessité. Plusieurs parties prenantes avaient d'ailleurs exposé ce problème à la Commission lors de sa consultation sur l'IA en 2020⁶³¹. Certains proposaient de remplacer la nécessité par une balise de raisonnabilité. Notons toutefois que cette dernière existe dans l'encadrement fédéral applicable au secteur privé⁶³², et qu'au fil des ans, les tribunaux l'ont ramenée elle aussi au test inspiré par l'arrêt *Oakes*⁶³³.

2.1.2.4. Recommandations

En ce qui concerne les enjeux plus fondamentaux soulevés par l'IA et les mégadonnées, ils font partie de ceux qui amènent la Commission à appeler, dans la section 2.2, à une réflexion élargie sur le futur de la protection des renseignements personnels, permettant de compléter le régime fondé sur les principes FIP par de nouvelles balises.

Pour le reste, de l'avis de la Commission, certaines mesures permettraient d'améliorer la compréhension et l'opérationnalisation du critère de nécessité. D'une part, elle propose à la section 2.1.7 des modifications relatives à l'évaluation des facteurs relatifs à la vie privée, un outil réflexif dont l'essence même est d'amener les organisations à analyser en profondeur le critère de nécessité dans le cadre d'un projet. D'autre part, elle recommande ci-après des modifications législatives lui paraissant essentielles pour une meilleure application du critère de nécessité.

2.1.2.4.1. Expliciter dans les lois le test de nécessité et l'étendue de son application

La Commission considère qu'il y a lieu de préciser dans les lois que le critère de nécessité s'applique, peu importe l'étape du cycle de vie du renseignement personnel. Ainsi, les assujettis auraient des balises claires à respecter, et toutes les utilisations et les communications de renseignements seraient soumises sans ambiguïté à une démonstration de nécessité. S'agissant d'une balise fondamentale, la clarté législative est de mise.

Dans le même esprit, la Commission juge qu'il serait avantageux de codifier les critères établis dans le test de nécessité afin de sceller l'interprétation du mot « nécessaire » et d'en clarifier l'application. Il importe aussi qu'il soit précisé qu'une fin interdite par une loi ne peut être considérée comme légitime au sens de ce test.

⁶³¹ COMMISSION D'ACCÈS À L'INFORMATION, *Intelligence artificielle et protection des renseignements personnels - Retour sur la consultation sur les principes en intelligence artificielle*, 2021, p. 6, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_DOC_Reflex_IA_RP.pdf>.

⁶³² *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c.-. 5, art. 5(3) [ci-après LPRPDÉ], en ligne : <<https://laws-lois.justice.gc.ca/fra/lois/p-8.6/>>.

⁶³³ *Eastmond c. Canadien Pacifique Ltée*, 2004 CF 852, par. 82, en ligne : <<https://canlii.ca/t/1hwq9>>; *Turner c. Telus Communications Inc.*, 2005 CF 1601, par. 48, en ligne : <<https://canlii.ca/t/1mw29>>.



Recommandation 30

Expliciter dans les lois que le critère de nécessité doit être évalué et respecté, non seulement pour la fin initiale pour laquelle la collecte est envisagée, mais également pour toute autre opération impliquant des renseignements personnels à travers leur cycle de vie.

Recommandation 31

Codifier expressément le test de nécessité dans les lois sur la protection des renseignements personnels.

2.1.2.4.2. Faciliter l'opérationnalisation de la nécessité par des balises plus claires

Selon la Commission, il apparaît pertinent de faciliter l'opérationnalisation du critère de nécessité.

Premièrement, il y aurait lieu d'énoncer des règles claires et observables qui permettraient aux assujettis de juger plus objectivement des renseignements qui peuvent ou non être nécessaires dans certaines situations courantes plutôt que de devoir analyser la nécessité à la pièce. Dans l'attente de prescriptions plus substantielles sur une variété de fins et de pratiques, que la Commission évoque dans la section 2.2.3.1, des balises devraient déjà être prévues pour des pratiques ayant des répercussions évidentes dans le quotidien des citoyens. Un intérêt évident existe ainsi à encadrer les renseignements personnels qu'il est possible ou non de recueillir, d'utiliser ou de communiquer, notamment dans le cadre de la collecte de renseignements personnels avant la location d'un logement et de la vidéosurveillance⁶³⁴.

Certes, la Commission peut émettre des lignes directrices pour faciliter l'application des lois. Cependant, elles ne peuvent avoir de force contraignante. Dans ce contexte, c'est par voie législative, ou à défaut réglementaire, qu'il conviendrait d'énoncer les règles plus claires, évoquées ci-haut.

De l'avis de la Commission, des textes explicites permettant de connaître ce qui est permis ou non dans ces contextes seraient véritablement gagnants pour toutes les parties :

- Ils assureraient à toutes les personnes se trouvant dans une situation analogue une protection équivalente.
- Ils apporteraient davantage de clarté aux organisations et, dans le secteur privé, simplifieraient des réflexions parfois difficiles dans un contexte de pressions concurrentielles.
- Ils faciliteraient la surveillance des pratiques par la Commission, dès lors qu'elle pourrait les comparer à un standard objectif qui permet d'établir, à sa face même, la nécessité ou la non-nécessité.

⁶³⁴ Soulignons que certains recours à la vidéosurveillance au Québec font déjà l'objet d'un encadrement plus précis, dans l'esprit présenté ici, en ce qui a trait à l'installation par les usagers ou leurs représentants de mécanismes de surveillance dans les centres d'hébergement et de soins longue durée ou dans les centres de réadaptation. Cet encadrement ne concerne toutefois pas l'usage de la vidéosurveillance par les organisations, mais par les individus. Voir GOUVERNEMENT DU QUÉBEC, « Décret 474-2026 du 25 mars 2026 concernant le Règlement concernant les modalités d'utilisation de mécanismes de surveillance par certains usagers », dans *Gazette officielle du Québec*, 158^e année, n° 14, Québec, Éditeur officiel du Québec, 2026, p. 1752-1754, en ligne : <https://www.publicationsduquebec.gouv.qc.ca/fileadmin/gazette/pdf_encrypte/lois_reglements/2026F/87738.pdf>.

Dans la section 2.1.2.5, la Commission offre un aperçu de différents encadrements prévus dans d'autres États, qui pourraient inspirer le législateur.

Recommandation 32

Encadrer, par voie législative ou réglementaire, les renseignements pouvant être considérés nécessaires ou non dans le cadre de pratiques courantes et ayant des répercussions importantes dans la vie des citoyens, comme la collecte de renseignements personnels avant la location d'un logement ou la vidéosurveillance.

2.1.2.5. Pour aller plus loin

La Commission donne ci-après quelques exemples d'encadrements prévus dans d'autres États relativement au traitement de renseignements personnels pour la prélocation et la vidéosurveillance.

La France a prévu, dans son cadre législatif relatif à la location de logement, qu'un décret encadre les renseignements pouvant être exigés d'un aspirant locataire ou de toute personne agissant à titre de caution⁶³⁵. Le décret adopté en vertu de cette loi⁶³⁶ prévoit notamment que le locateur peut exiger une pièce d'identité valide avec photo et recueillir :

- une seule pièce justificative du domicile actuel;
- un ou plusieurs documents attestant des activités professionnelles, parmi une liste fermée;
- un ou plusieurs documents attestant des ressources financières, parmi une liste fermée.

Selon la Commission, la collecte permise en France reste fort étendue, mais elle adhère au principe de création de listes fermées de renseignements légalement exigibles.

Quant à la vidéosurveillance, de nombreux pays se sont dotés de législations spécifiques. Par exemple :

- La Belgique a adopté une loi sur la vidéosurveillance, qui ne s'applique toutefois pas aux caméras sur des lieux de travail⁶³⁷. Elle fixe les lieux et des types d'appareils acceptables. Elle prescrit également les finalités permissibles et des conditions pour l'installation, comme l'affichage d'un avis, le recours à des pictogrammes, la tenue d'un registre et la durée de conservation des bandes. Des sanctions sont prévues en cas de contravention.
- En France, une loi encadre le déploiement de caméras par les pouvoirs publics ou sur la voie publique par des acteurs privés⁶³⁸. Elle précise elle aussi des fins permissibles et oblige l'obtention d'une autorisation pour installer les caméras. Entre autres, elle interdit la visualisation de l'intérieur des

⁶³⁵ Loi n° 89-462 du 6 juillet 1989 tendant à améliorer les rapports locatifs et portant modification de la loi n° 86-1290 du 23 décembre 1986 [France], art. 22-2, en ligne : <<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000509310/2025-11-13>>.

⁶³⁶ Décret n° 2015-1437 du 5 novembre 2015 fixant la liste des pièces justificatives pouvant être demandées au candidat à la location et à sa caution [France], en ligne : <<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000031444493/2026-04-01>>, annexe 1.

⁶³⁷ Loi réglant l'installation et l'utilisation de caméras de surveillance [Belgique], 2007-03-21/39, en ligne : <https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2007032139&table_name=loi>.

⁶³⁸ Code de la sécurité intérieure [France], tit. V (Vidéoprotection), en ligne : <https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000025505402/2026-04-01>.



immeubles d'habitation. La loi renvoie explicitement au cadre de protection des renseignements personnels, en plus de prévoir elle aussi des sanctions.

- Dans sa loi concernant plus généralement les technologies utilisées par les autorités, les libertés civiles et la collecte de preuves, le Royaume-Uni prévoit la création d'un code de pratique pour la vidéosurveillance, qui contient notamment des prescriptions sur les finalités permissibles, les modalités et les types de caméras appropriés⁶³⁹. Un commissaire à la vidéosurveillance est institué pour veiller à l'application de ces règles.

⁶³⁹ *Protection of Freedoms Act 2012 [Royaume-Uni]*, 2012 c. 9, en ligne : <<https://www.legislation.gov.uk/ukpga/2012/9>>.



2.1.3. Les inférences algorithmiques

Sommaire

La société contemporaine est marquée par un élan vers la production de données, notamment par le truchement de l'utilisation d'objets connectés et la fréquentation des environnements numériques. Cette ère de mise en données favorise l'exploration et l'exploitation des mégadonnées par l'IA.

Cet immense potentiel technologique peut être mis à profit pour générer de nouveaux renseignements sur les personnes à partir d'autres renseignements les concernant. Le processus d'inférence algorithmique représente un nouveau mode de collecte de renseignements personnels, qui fait en sorte qu'il n'est plus nécessaire de toujours les recueillir directement auprès des personnes concernées. L'inférence algorithmique nécessite ainsi un cadre législatif adapté.

Dans cette section, la Commission aborde les enjeux suivants :

- Les lois ne sont pas assez explicites quant au statut de renseignements personnels de certaines inférences.
- Le critère de l'identification qui sous-tend la notion de renseignement personnel n'est plus adapté pour tenir compte des réalités contemporaines.
- Les lois ne prévoient pas de cadre pour la création et l'inférence de renseignements personnels.

Elle formule des recommandations afin :

- de préciser les cas dans lesquels les inférences constituent des renseignements personnels;
- d'adapter la notion de renseignement personnel;
- d'encadrer l'inférence de renseignements personnels.

2.1.3.1. Contexte

Les régimes de protection des renseignements personnels ont été élaborés pour encadrer les relations d'un à un entre les personnes et les organisations. Ils conviennent bien, par exemple, aux cas où une personne cherche des biens ou des services en magasin ou en clinique : on peut lui indiquer sans problème quels sont les renseignements nécessaires aux fins visées, qui sont souvent aisément compréhensibles.

Toutefois, ces régimes peinent à encadrer les phénomènes nouveaux qui accompagnent la montée en importance des technologies numériques et connectées, ainsi que de l'IA. Au quotidien, les personnes sont en contact avec de nombreux capteurs et objets connectés, qui enregistrent et se communiquent un volume incommensurable de données. **Après leur collecte, ces données peuvent être analysées par des organisations dans l'objectif, notamment, de produire de nouveaux renseignements sur les individus et les groupes.** En effet, de grands ensembles de renseignements peuvent être exploités pour construire des modèles d'IA capables de déduire les caractéristiques de groupes entiers, sur la base



d'autres renseignements moins signifiants. Tout un écosystème d'acteurs qui génèrent, échangent et utilisent les renseignements à des fins diverses s'est développé autour de ce filon⁶⁴⁰.

Ainsi, les personnes sont à la source d'une importante quantité de renseignements générés par les organisations, souvent en toute opacité. Même si elles étaient au courant des pratiques, elles auraient peine à s'y retrouver tant les parties prenantes peuvent être nombreuses et tant les pratiques d'analyse de données sont complexes.

Dans la présente section, la Commission aborde le phénomène de la mise en données et de l'exploration des mégadonnées, soubassements d'une économie de la donnée. Elle s'intéresse ensuite au phénomène des inférences algorithmiques et aux enjeux qu'elles posent pour la protection de la vie privée. Enfin, elle formule des recommandations pour en tenir compte dans le cadre législatif actuel.

2.1.3.2. Situation actuelle

Les inférences algorithmiques émergent dans le contexte du traitement des mégadonnées, comme présenté ci-après⁶⁴¹. Un aperçu du cadre légal qui s'applique en matière de protection des renseignements personnels est donné par la suite.

2.1.3.2.1. Les approches pour obtenir et traiter des données numériques

2.1.3.2.1.1. La mise en données

Une journée dans la vie d'Arthur

À l'aurore, Arthur étend son bras afin d'éteindre son réveille-matin. Celui-ci, connecté, enregistre l'heure de son réveil, plus hâtif qu'à l'habitude. Se sentant en forme, il sort courir. Il enregistre sa séance sur son application sportive, qui suit fidèlement sa géolocalisation⁶⁴². En rentrant, affamé, il concocte son déjeuner à l'aide de ses nouveaux électroménagers, qui enregistrent diverses données⁶⁴³. En route vers le travail, il commande un café via l'application mobile d'une chaîne populaire, qui consigne et analyse soigneusement ses habitudes. Arthur ignore d'ailleurs que ses transactions par carte de crédit, comme celle qu'il vient de faire, sont soigneusement analysées par des tiers⁶⁴⁴. En attendant son breuvage, il pose quelques questions à un assistant virtuel, qui enregistre chaque discussion et qui réutilise les données collectées⁶⁴⁵.

⁶⁴⁰ Pensons par exemple aux courtiers en données, que la Commission aborde plus en détail à la section 2.1.5.

⁶⁴¹ Pour développer son propos, la Commission s'appuie notamment sur les travaux de Jocelyn MACLURE et Sylvain AUCLAIR, *Droit à la vie privée : analyse conceptuelle et réflexion éthique sur sa source, sa portée et son redéploiement à l'ère des technologies axées sur les données*, 2021, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/financement-pour-les-projets-de-recherche-et-d-application-des-connaissances/projets-menes-a-bien-dans-le-cadre-du-programme-des-contributions/2020-2021/p_2020-21_08/>.

⁶⁴² Antoine PAQUETTE, « Application sportive: Des coureuses traquées sur Strava », *La Presse* (6 avril 2026), en ligne : <<https://www.lapresse.ca/actualites/2026-04-06/application-sportive/des-coureuses-traquees-sur-strava.php>> (consulté le 11 avril 2026).

⁶⁴³ Daniel WROCLARSKI, « Smart Appliances Promise Convenience and Innovation. But Is Your Privacy Worth the Price? », *Consumer Reports* (24 juillet 2023), en ligne : <<https://www.consumerreports.org/electronics/privacy/smart-appliances-and-privacy-a1186358482/>> (consulté le 16 avril 2026).

⁶⁴⁴ U.S. PIRG EDUCATION FUND, « How Mastercard sells its 'gold mine' of transaction data » (20 septembre 2023), en ligne : <<https://pirg.org/edfund/resources/how-mastercard-sells-data/>> (consulté le 27 novembre 2025).

⁶⁴⁵ Geoffrey A. FOWLER, « Meta AI is a creepier version of ChatGPT. Here's how to protect your privacy », *The Washington Post* (5 mai 2025), en ligne : <<https://www.washingtonpost.com/technology/2025/05/05/meta-ai-privacy/>> (consulté le 27 novembre 2025).



Arthur consulte sa montre connectée, qui connaît bien plus que son fuseau horaire⁶⁴⁶. Café en main, il traverse un parc et croise le faisceau d'une caméra de surveillance dernier cri, laquelle envoie ses données biométriques vers ses serveurs⁶⁴⁷. En entrant au bureau, il ouvre rapidement son ordinateur de travail, qui se met dès lors à suivre son utilisation⁶⁴⁸. Les requêtes qu'il fait à l'IA générative dans le cadre de son travail sont enregistrées par son fournisseur. Sa journée terminée, il fait une balade en voiture, sans savoir que ses habitudes de conduite sont enregistrées et que sa prime d'assurance augmentera bientôt⁶⁴⁹. De retour chez lui, il écoute un programme télévisé. Le téléviseur observe en retour ses habitudes d'utilisation⁶⁵⁰. Pendant une pause publicitaire, il ouvre son réseau social favori, avare de ses données d'utilisation⁶⁵¹. Se sentant fatigué, Arthur s'installe confortablement dans son nouveau lit connecté, qui analyse les données de son sommeil afin de lui formuler des recommandations le lendemain.

Avec l'évolution technologique et la multiplication des appareils connectés, la société actuelle est traversée par la mise en données, soit « la captation de données reliées à une activité en vue de leur exploitation⁶⁵² ». Cette réalité s'accompagne d'une conviction selon laquelle « plus, c'est mieux » : avoir accès à davantage de données permettrait de mieux comprendre le monde sous tous ses aspects. Conséquemment, une dynamique de maximisation des données recueillies et produites ainsi que de leur analyse s'est développée. Les renseignements personnels ne font pas exception.

Le phénomène de la mise en données est déjà bien connu⁶⁵³. Paradoxalement, les personnes tendent toutefois à ignorer l'ampleur de la collecte de renseignements, alors même qu'elles naviguent dans un environnement marqué par l'omniprésence des appareils connectés.

⁶⁴⁶ Cailbhe DOHERTY, Maximus BALDWIN, Rory LAMBE, Marco ALTINI et Brian CAULFIELD, « Privacy in consumer wearable technologies: a living systematic analysis of data policies across leading manufacturers », (2025) 8-1 *npj Digital Medicine* 363, DOI : 10.1038/s41746-025-01757-1.

⁶⁴⁷ Omar AMIZAN, Irfan MEHMOOD et Kamran MAHROOF, « Businesses are harvesting our biometric data. The public needs assurances on security », *The Conversation* (9 juillet 2024), DOI : 10.64628/AB.v7k73qrvx.

⁶⁴⁸ Jon MARTINDALE, « 7 ways Windows 11 collects your data - and how to opt out », *PC World* (11 juillet 2024), en ligne : <<https://www.pcworld.com/article/2379675/ways-windows-11-collects-your-data-and-what-you-can-do-about-it.html>> (consulté le 27 novembre 2025).

⁶⁴⁹ UNION DES CONSOMMATEURS, préc., note 535, p. 21-22.

⁶⁵⁰ Jeff CHESTER et Kathryn C MONTGOMERY, *How TV Watches Us: Commercial Surveillance in the Streaming Era*, Center for Digital Democracy, 2024, en ligne : <<https://democraticmedia.org/assets/cdd-ctv-report-oct24-1.1.pdf>> (consulté le 9 octobre 2024).

⁶⁵¹ Anne CORCOS et Levana HODARA, « How social media are collecting more of users' data: a behavioral model of platform retention strategies », (2023) 3-7 *SN Business & Economics* 117, DOI : 10.1007/s43546-023-00501-9.

⁶⁵² OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « mise en données », *Grand dictionnaire terminologique*, en ligne : <<https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26523020/mise-en-donnees>> (consulté le 24 novembre 2025).

⁶⁵³ Florence MILLERAND, Alexandre COUTANT, Guillaume LATZKO-TOTH et Mélanie MILLETTE (dir.), *Les publics de données: penser la datafication de la société*, Montréal, Les Presses de l'Université de Montréal, 2025, en ligne : <https://pum.umontreal.ca/catalogue/les_publics_de_donnees/fichiers/bd9833a0-55dc-4ee6-ab48-35719fe2fdd5/9782760652255_publics_des_donnees.pdf>; HORIZONS DE POLITIQUES CANADA, *Création de sens : Avenirs*, 2023, en ligne : <<https://horizons.service.canada.ca/fr/2023/05/31/creation-de-sens-avenirs/pdf/creation-avenirs-changements.pdf>>; Wolfie CHRISTL et Sarah SPIEKERMANN, *Networks of control: a report on corporate surveillance, digital tracking, big data & privacy*, Vienne, facultas, 2016 [ci-après *Networks of control*], en ligne : <https://crackedlabs.org/dl/Christl_Spiekermann_Networks_Of_Control.pdf>.



Sous le paradigme de la mise en données, toutes les sphères de la vie d'une personne sont susceptibles d'être scrutées, quantifiées et analysées.

Il peut s'agir de son comportement, de ses caractéristiques, de son état de santé, de ses relations sociales, de ses déplacements ou de ses intérêts. **Ultimement, presque toutes les organisations avec lesquelles la personne fait affaire au quotidien peuvent amasser et analyser des données, ou encore utiliser elles-mêmes des produits et des services d'autres organisations partageant cette pratique.**

La mise en données passe autant par les objets connectés que par les environnements physique et numérique. Il est estimé qu'en 2023, 16,6 milliards d'objets connectés étaient en circulation dans le monde⁶⁵⁴. Seulement pour la catégorie des appareils à l'intention des consommateurs, comme les téléphones intelligents, ce nombre devrait grimper à 17 milliards d'ici 2033⁶⁵⁵. Les lieux sont aussi de plus en plus investis de capteurs en tout genre. Par exemple, le concept de ville intelligente⁶⁵⁶, où des municipalités intègrent des capteurs à plusieurs infrastructures⁶⁵⁷ dans l'objectif d'atteindre une meilleure gestion et d'offrir une meilleure qualité de vie aux citoyens, est en vogue. Enfin, en plus des données que les personnes choisissent volontairement de divulguer sur le Web, elles laissent dans leur sillage de nombreuses métadonnées, comme des adresses IP, des informations sur les appareils utilisés ou des historiques de navigation. Ces métadonnées se prêtent bien à l'analyse et au croisement, par exemple à des fins de publicité ciblée.

2.1.3.2.1.2. Les mégadonnées

En 2022, on estimait qu'en 2027, les objets connectés généreraient 1 100 pétaoctets de données, soit l'équivalent de 165 millions d'heures de vidéo en 4K⁶⁵⁸. Le phénomène de la mise en données contribue ainsi directement à celui des mégadonnées, désignant des données en grandes quantités, structurées ou non, de sources et de formats variés, dont le traitement et l'analyse nécessitent le recours à des technologies avancées⁶⁵⁹.

Parmi ses nombreuses applications, l'exploration des mégadonnées peut servir à déduire des connaissances sur des personnes, qu'il s'agisse de groupes ou d'individus. On parle alors d'inférences algorithmiques⁶⁶⁰. Comme illustré par les exemples de la section 2.1.3.2.1.3, ces inférences servent

⁶⁵⁴ FORTUNE BUSINESS INSIGHTS, « Internet of Things (IoT) Market Size, Share & Industry Analysis, By Component (Platform and Solution & Services), By Deployment (On-premise and Cloud), By Enterprise Type (SMEs and Large), By Industry (BFSI, Retail, Government, Healthcare, Manufacturing, Agriculture, Sustainable Energy, Transportation, IT & Telecom, and Others), and Regional Forecast, 2024-2032 » (juin 2025), en ligne : <<https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307>> (consulté le 27 juin 2025).

⁶⁵⁵ Lionel Sujay VAILSHERY, « Number of IoT connections worldwide 2022-2034 », *Statista* (2025), en ligne : <<https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/>> (consulté le 27 juin 2025).

⁶⁵⁶ OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Ville intelligente », *Grand dictionnaire terminologique*, en ligne : <<https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26544297/ville-intelligente>> (consulté le 24 novembre 2025).

⁶⁵⁷ Martin LESSARD, « Les luminaires urbains connectés : entre économie d'énergie et surveillance », *Radio-Canada* (11 octobre 2016), en ligne : <<https://ici.radio-canada.ca/nouvelle/808033/triplex-ville-intelligente-mobilier-connecte>> (consulté le 24 novembre 2025).

⁶⁵⁸ JUNIPER RESEARCH, « Roaming IoT Connections to Generate 1,100 Petabytes Globally by 2027 » (août 2022), en ligne : <<https://www.juniperresearch.com/press/roaming-iot-connections-to-generate-1-100-petabytes-globally-by-2027/>> (consulté le 20 novembre 2025).

⁶⁵⁹ OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, préc., note 469.

⁶⁶⁰ Privacy International a fait paraître il y a quelques années un répertoire d'articles qui montrent quelles inférences peuvent être tirées de certaines données. Voir PRIVACY INTERNATIONAL, *Examples of Data Points Used In profiling*, 2017, en ligne : <https://privacyinternational.org/sites/default/files/2018-04/data%20points%20used%20in%20tracking_0.pdf>.



grandement au profilage⁶⁶¹ des personnes, car elles permettent de dégager davantage de savoir sur elles, qu'il s'agisse de caractéristiques physiques ou mentales, d'opinions, de goûts ou encore de prédictions concernant leur comportement. Comme tous les autres renseignements personnels, ceux qui sont inférés permettent aux organisations d'exercer un certain pouvoir sur les personnes, qu'il s'agisse par exemple de prendre des décisions les concernant sur la base d'un score de risque ou de leur proposer des publicités leur correspondant davantage.

Dans l'ensemble, les mégadonnées et leur exploration, quels que soient les outils et les méthodes employés, doivent être comprises comme les fondements d'un nouveau paradigme épistémique⁶⁶² et, partant, comme un cadre nouveau pour la prise de décision, la justification des actions et l'orientation des pratiques⁶⁶³. Cette nouvelle acquisition du savoir ne s'appuie pas, comme le raisonnement humain, sur la détermination des causes⁶⁶⁴, mais bien sur la détection de corrélations que l'œil humain, parfois, ne saurait distinguer. Dans ce changement épistémique, le savoir provient plus de procédés algorithmiques opaques que de la perception de l'observateur⁶⁶⁵. **Fait crucial, les renseignements personnels issus de l'exploration des mégadonnées ne sont pas recueillis ou observés auprès des personnes concernées, mais ils sont créés par une organisation. Ces dernières n'ont plus à se tourner vers les personnes pour en savoir plus sur elles : les renseignements eux-mêmes sont la source d'autres renseignements sur les personnes concernées et celles ayant des profils similaires.**

Ce nouveau paradigme de production de renseignements provoque l'émergence de nouveaux modèles d'affaires. La chute du coût d'extraction des données et l'augmentation simultanée des bénéfices liés à leur analyse, couplées au fait qu'il devient plus difficile d'anticiper le potentiel présent ou futur de chacune des données, mettent au jour une économie de la donnée fondée sur la collecte massive et l'inférence⁶⁶⁶. Au sein de cette économie, les organisations qui disposent d'un accès immédiat aux mégadonnées et qui ont les moyens de mobiliser les pleins pouvoirs de l'apprentissage machine⁶⁶⁷ tiennent le haut du pavé. Certains parlent en ce sens d'un pouvoir prédictif détenu par ces organisations qui, fortes des modèles algorithmiques qu'elles ont développés, peuvent déduire des renseignements personnels d'individus à partir de quelques autres renseignements les concernant⁶⁶⁸.

2.1.3.2.1.3. Les inférences algorithmiques

Les inférences algorithmiques et les modèles élaborés pour les générer sont de puissants outils permettant de déduire des renseignements personnels. Elles entraînent avec elles certains risques pour la protection de la vie privée. Les personnes peuvent être profilées efficacement sur la base d'inférences

⁶⁶¹ La Commission utilise ce terme selon la définition qu'en donnent les lois québécoises sur la protection des renseignements personnels; voir la section 2.1.3.2.2.2.

⁶⁶² L'épistème désigne un système général de connaissance. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « épistème », *Grand dictionnaire terminologique*, en ligne : <<https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/17078718/episteme>> (consulté le 10 avril 2026).

⁶⁶³ S. BAROCAS et H. NISSENBAUM, préc., note 479 à la page 46.

⁶⁶⁴ A. SOLOW-NIEDERMAN, préc., note 529, p. 381.

⁶⁶⁵ Lanah Kammourieh et al. « Group Privacy in the Age of Big Data », in Linnet TAYLOR, Luciano FLORIDI et Bart VAN DER SLOOT (dir.), *Group Privacy: New Challenges of Data Technologies*, Cham, Springer International Publishing, 2017 [ci-après Group Privacy], p. 43, DOI : 10.1007/978-3-319-46608-8.

⁶⁶⁶ A. SOLOW-NIEDERMAN, préc., note 529, p. 363.

⁶⁶⁷ OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « apprentissage automatique », *Grand dictionnaire terminologique*, en ligne : <<https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8395061/apprentissage-automatique>> (consulté le 10 avril 2026).

⁶⁶⁸ Rainer MÜLHOFF et Hannah RUSCHEMEIER, « Predictive analytics and the collective dimensions of data protection », (2024) 16-1 *Law, Innovation and Technology* 261-292, DOI : 10.1080/17579961.2024.2313794.



algorithmiques : des renseignements personnels peuvent être inférés par des systèmes automatisés, développés par l'analyse de pairs qui partagent les mêmes traits qu'elles.

Grâce à ce savoir précis, les organisations peuvent prendre des décisions sur les personnes, voire les discriminer, ou les cibler avec des contenus hautement personnalisés dans le but de les influencer.

Plusieurs situations impliquant des inférences algorithmiques ont été médiatisées en raison de préjudices importants. Bien que les deux cas présentés ci-dessous se soient produits il y a plusieurs années déjà, ils sont particulièrement illustratifs de la puissance des inférences algorithmiques et des préjudices qu'elles peuvent occasionner.

TARGET SAIT RECONNAÎTRE LA GROSSESSE

L'exemple le plus emblématique d'inférence algorithmique à des fins de profilage est probablement celui relevé par le *New York Times* en 2012⁶⁶⁹ au sujet de la manière dont la chaîne de magasins à grande surface Target s'y est prise pour apprendre la grossesse d'une de ses clientes avant même son propre père.

Target désirait cibler les ménages qui attendent un enfant puisque ce moment correspond à une période où de nouvelles habitudes de consommation sont formées. Des analystes ont évalué le comportement de consommation des clients de la chaîne afin d'y repérer les indices révélant une grossesse. Ils bénéficiaient d'une manne de renseignements, car Target, à l'instar de nombreux commerces, attribuait un identifiant unique à ses clients afin de conserver un registre de leurs achats et d'accumuler un maximum d'informations sur eux, y compris auprès d'organisations tierces. Pour différencier les comportements des ménages attendant un enfant de celui des autres, les analystes pouvaient compter sur l'existence d'un registre d'achats en vue de fêtes prénatales mis en place par la compagnie. Quelque 25 produits fréquemment achetés par les ménages en attente d'un enfant ont pu être reliés plus particulièrement à la grossesse.

Suivant cette découverte, Target a pu élaborer un algorithme prédictif lui permettant d'attribuer à l'ensemble de ses clients un score de probabilité de grossesse. Ainsi, la chaîne a pu profiter du consentement d'une partie de sa clientèle à la divulgation des renseignements personnels les concernant afin de déduire les mêmes renseignements pour l'ensemble de ses clients. Grâce à ce nouveau savoir, Target a pu envoyer des offres promotionnelles et des feuillets spécialement conçus pour les femmes enceintes, notamment au domicile d'une famille dont le père ignorait la grossesse de sa fille.

CAMBRIDGE ANALYTICA PROPULSE LA MANIPULATION ÉLECTORALE

Le recours aux inférences a aussi eu de très grandes répercussions dans l'affaire Cambridge Analytica⁶⁷⁰. En effet, la firme a été embauchée par des politiciens dans le cadre de campagnes électorales de grande

⁶⁶⁹ Charles DUHIGG, « How Companies Learn Your Secrets », *The New York Times* (16 février 2012), en ligne : <<https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>> (consulté le 25 novembre 2025).

⁶⁷⁰ Matthew ROSENBERG et Gabriel J. X. DANCE, « 'You Are the Product': Targeted by Cambridge Analytica on Facebook », *The New York Times* (8 avril 2018), en ligne : <<https://www.nytimes.com/2018/04/08/us/facebook-users-data-harvested-cambridge-analytica.html>> (consulté le 1 décembre 2025); Matthew ROSENBERG, Nicholas CONFESSORE et Carole CADWALLADR, « How Trump Consultants Exploited the Facebook Data of Millions », *The New York Times* (17 mars 2018), en ligne : <<https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>> (consulté le 26 novembre 2025); Carole CADWALLADR, « 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower », *The Guardian* (18 mars 2018), en ligne : <<https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook->



envergure, à des fins de marketing politique, afin d'y mener des opérations de ciblage psychologique. Par exemple, les personnes avec un haut score de névrosisme pouvaient être exposées à des images d'immigrants franchissant en masse les frontières nationales afin de les inciter à voter pour les candidats anti-immigration, ou encore les électeurs jugés influençables pouvaient être incités à ne pas prendre part au vote.

Ces campagnes basées sur la connaissance de traits psychologiques de millions d'électeurs n'étaient possibles que par le recours à des modèles algorithmiques inférentiels. Afin de développer ces outils, la firme a engagé une compagnie menée par un chercheur, qui avait auparavant travaillé à inférer des traits psychologiques à partir des mentions « j'aime » sur Facebook, pour qu'elle développe une application de questionnaires concernant les traits de personnalités proposés aux utilisateurs de Facebook. L'application aspirait également les renseignements figurant dans leurs profils et ceux de leurs amis sur le réseau social. L'analyse de ces données a servi à construire des modèles capables d'inférer certains traits de personnalité sur la base d'informations en apparence anodines. La firme avait alors un grand pouvoir d'influence sur les personnes ciblées, qui ignoraient à quel point elle en savait sur elles.

2.1.3.2.2. Le cadre légal

Les inférences sur les personnes et la création de renseignements personnels concernent plusieurs aspects des lois sur la protection des renseignements personnels, dont il sera question au cours des sections suivantes.

2.1.3.2.2.1. La définition des renseignements personnels

Deux critères cumulatifs prévus par les lois servent de seuil pour qu'un renseignement soit considéré comme personnel. Il doit :

- concerner une personne physique;
- permettre de l'identifier directement ou indirectement⁶⁷¹, soit seul ou en combinaison avec d'autres.

La Commission a déjà déterminé qu'identifier quelqu'un « peut consister à le reconnaître par rapport à quelqu'un d'autre, par rapport aux différentes classes ou catégories d'individus. Bref, il s'agit de reconnaître sa nature⁶⁷². » En dernière instance, il s'agit de remonter à l'identité concrète de la personne.

Depuis l'entrée en vigueur complète de la Loi 25, les lois sur la protection des renseignements personnels reconnaissent aussi explicitement qu'il existe des renseignements inférés⁶⁷³. En l'espèce, cette notion est introduite dans le contexte du droit à la portabilité, où elle sert à distinguer les renseignements personnels dont une personne ne peut demander copie dans un format technologique structuré et couramment utilisé. Les personnes peuvent faire une telle demande uniquement pour les renseignements personnels recueillis auprès d'elles.

nix-bannon-trump> (consulté le 26 novembre 2025); Carole CADWALLADR et Emma GRAHAM-HARRISON, « Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach », *The Guardian* (17 mars 2018), en ligne : <<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>> (consulté le 26 novembre 2025).

⁶⁷¹ *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*, préc., note 26, art. 54; Loi sur le privé, art. 2.

⁶⁷² *Segal c. Centre de services sociaux de Québec*, [1988] C.A.I. 315 (Commission d'accès à l'information).

⁶⁷³ Loi sur l'accès, art. 84, par. 3; Loi sur le privé, art. 27, par. 3; LRSSS, art. 66, par. 2.



Ainsi, aux yeux de la loi, il existe d'une part des renseignements collectés auprès des personnes ou de tiers, et de l'autre des renseignements créés ou inférés à partir d'autres renseignements personnels.

2.1.3.2.2. La collecte de renseignements personnels et les obligations associées

De nombreuses obligations qui incombent aux organisations doivent être remplies avant la collecte de renseignements personnels. Principalement, elles doivent :

- s'assurer de respecter le critère de nécessité, d'une manière décrite plus avant dans la section 2.1.2.2.1;
- fournir des informations définies aux personnes concernées au moment de la collecte auprès d'elles⁶⁷⁴, de même que dans une politique de confidentialité si elles recueillent des renseignements personnels par moyen technologique⁶⁷⁵, et des informations particulières si elles ont recours à des technologies permettant l'identification, la localisation ou le profilage⁶⁷⁶ :
 - Le terme profilage évoque, dans les lois, la collecte et l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyses diverses⁶⁷⁷;
- obtenir le consentement, dans certains cas abordés plus avant dans la section 2.1.1.2.1 :
 - Lorsqu'elles effectuent, dans le secteur privé, la collecte auprès d'un tiers.
 - Lorsqu'elles recueillent des renseignements personnels directement auprès d'un mineur de moins de 14 ans et que cette collecte n'est pas manifestement à son bénéfice. Le consentement du parent ou du tuteur est alors requis.

2.1.3.3. Enjeux

Au vu des préjudices que peuvent causer les inférences, il est essentiel qu'elles soient correctement encadrées par les lois sur la protection des renseignements personnels. De l'avis de la Commission, ces lois ne sont actuellement pas suffisamment explicites sur le fait qu'elles couvrent les inférences, et les obligations qu'elles prévoient n'y sont pas toutes adaptées.

2.1.3.3.1. Les inférences algorithmiques mettent au défi la notion de renseignement personnel

Les lois et les protections qu'elles mettent en place s'appliquent uniquement aux renseignements correspondant à la définition des renseignements personnels. Il importe alors qu'il soit clair pour tous que les inférences peuvent constituer de tels renseignements.

Le statut des inférences a fait couler beaucoup d'encre au cours des dernières années, et de nombreux doutes ont été soulevés sur des éléments distincts⁶⁷⁸. Au Québec, à l'occasion des consultations sur l'IA menées par la Commission en 2020, avant l'adoption de la Loi 25, les experts de l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (l'Obvia) faisaient valoir des craintes similaires : bien qu'il soit naturel de supposer qu'une inférence concernant une personne est un

⁶⁷⁴ Loi sur l'accès, art. 65; Loi sur le privé, art. 8; LRSSS, art. 14.

⁶⁷⁵ Loi sur l'accès, art. 63.4; Loi sur le privé, art. 8.2.

⁶⁷⁶ Loi sur l'accès, art. 65.0.1; Loi sur le privé, art. 8.1; LRSSS, art. 15.

⁶⁷⁷ Loi sur l'accès, art. 65.0.1; Loi sur le privé, art. 8.1; LRSSS, art. 15.

⁶⁷⁸ Des chercheurs montrent notamment comment le statut des inférences est remis en cause dans la jurisprudence concernant la loi européenne sur la protection des renseignements personnels, le RGPD, dont s'inspirent les lois québécoises en la matière : Sandra WACHTER et Brent MITTELSTADT, « A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI », (2019) 2019-2 *Columbia Business Law Review*, p. 1, doi : 10.7916/d8-g10s-ka92.

renseignement personnel, « la nature plus hypothétique que factuelle d'une prédiction, d'une inférence ou d'une évaluation fragilise l'idée qu'il s'agisse bel et bien d'un "renseignement"⁶⁷⁹ ». Similairement, dans son mémoire sur le projet de loi devenu la Loi 25, la Commission mentionnait que, selon certaines parties, les renseignements inférés ne sont pas des renseignements personnels puisqu'ils sont le « produit » d'une organisation⁶⁸⁰.

Les lois reconnaissent désormais l'existence de renseignements personnels inférés à partir d'autres renseignements personnels. Cependant, cette possibilité n'est mentionnée que de manière incidente, dans une disposition précise sur la portabilité des renseignements personnels. Ainsi, aucune disposition propre n'est consacrée aux inférences, et elles ne sont pas associées directement à la définition des renseignements personnels.

Il est clair pour la Commission que toutes les inférences sont des renseignements personnels si elles concernent une personne et permettent de l'identifier, et ce, malgré leur caractère probabiliste et le fait qu'elles soient générées par des organisations⁶⁸¹. Toutefois, considérant les préjudices susceptibles d'être occasionnés par la production des inférences et les actions entreprises grâce à elles par des organisations, la Commission est d'avis qu'un lien plus clair devrait être tracé entre les notions d'inférence et de renseignement personnel. Cette clarté a d'ailleurs été réclamée par des répondants à ses consultations sur les principes de l'IA en 2020⁶⁸², notamment par les spécialistes de l'Obvia⁶⁸³. À la suite de ses propres consultations sur l'IA, le CPVPC⁶⁸⁴ et le spécialiste Ignacio Cofone⁶⁸⁵ sont par ailleurs arrivés aux mêmes conclusions concernant le cadre fédéral de protection des renseignements personnels.

Toutefois, l'inférence peut ne pas remplir le critère de l'identification dont dépend l'application des lois sur la protection des renseignements personnels, ce qui menace la protection des individus. Le recours aux inférences algorithmiques et à l'exploration des mégadonnées permet aux organisations de déduire des renseignements sur les personnes concernées, et ainsi d'éventuellement fonder des décisions ou produire un effet sur elles, sans que leur identité soit connue. Dans bien des cas, l'identité importe peu, car l'exploration des données elle-même permet d'obtenir davantage de renseignements sur la personne⁶⁸⁶ :

L'exploration des données rompt l'intuition élémentaire qui veut que l'identité soit la plus grande source de préjudice parce qu'elle substitue aux renseignements identificatoires les

⁶⁷⁹ Pierre-Luc DÉZIEL, Karim BENYKHLEF et Eve GAUMOND, *Repenser la protection des renseignements personnels à la lumière des défis soulevés par l'IA*, Observatoire international des impacts sociétaux de l'IA et du numérique, 2020, p. 7, en ligne : <<http://collections.banq.qc.ca/ark:/52327/bs4067010>>.

⁶⁸⁰ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, p. 10.

⁶⁸¹ Elle l'a énoncé à plusieurs reprises dans des communications, des mémoires, et dans ses décisions. Voir COMMISSION D'ACCÈS À L'INFORMATION, « Qu'est-ce qu'un renseignement personnel? », en ligne : <<https://www.cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/renseignement-personnel-definition>> (consulté le 5 décembre 2025); COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, p. 10; COMMISSION D'ACCÈS À L'INFORMATION, *Enquête concernant le Centre de services scolaire du Val-des-Cerfs (anciennement Commission scolaire du Val-des-Cerfs)*, dossier 1020040-S, 2022, par. 28, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/decisions-en-surveillance/1020040-S_decision-cai-centre-services-scolaire-val-cerfs-2022-11-09.pdf>.

⁶⁸² COMMISSION D'ACCÈS À L'INFORMATION, préc., note 631, p. 5.

⁶⁸³ P.-L. DÉZIEL, K. BENYKHLEF et E. GAUMOND, préc., note 679, p. 7.

⁶⁸⁴ COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Un cadre réglementaire pour l'IA : recommandations pour la réforme de la LPRPDE » (12 novembre 2020), en ligne : <https://priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-ai/reg-fw_202011/#fn8> (consulté le 12 novembre 2020).

⁶⁸⁵ Ignacio COFONE, « Propositions stratégiques aux fins de la réforme de la LPRPDE élaborées en réponse au rapport sur l'intelligence artificielle », *Commissariat à la protection de la vie privée du Canada* (12 novembre 2020), en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-ai/pol-ai_202011/>.

⁶⁸⁶ S. BAROCAS et H. NISSENBAUM, préc., note 479 à la page 55.



inférences comme manière de parvenir à des faits additionnels. Plutôt que d'apparier des informations correspondant au même nom (ou autre renseignement personnel) provenant de différents ensembles de données, l'exploration des données produit des corrélations qui permettent aux entreprises de déduire des caractéristiques des individus.

Il est donc possible que certaines inférences concernant des personnes ne soient pas couvertes par la définition actuelle des renseignements personnels. Partant, elles pourraient être utilisées sans que s'appliquent les mesures actuellement prévues par les cadres de protection des renseignements personnels.

Le modèle de la publicité ciblée peut servir d'exemple. Essentiellement, ce modèle commercial, fondé sur le profilage, tire son efficacité de la production d'inférences sur les personnes, sans qu'il soit nécessaire de se concentrer sur leur identité. Certains acteurs de cette industrie prétendent qu'ils peuvent tracer les personnes, les profiler et les cibler avec des publicités correspondant à leurs caractéristiques observées ou inférées, et ce, sans avoir à se soumettre aux régimes de protection des renseignements personnels. Ils s'intéressent aux caractéristiques des personnes plutôt qu'à leur identité, mais l'objectif demeure de les influencer. Si tous conviennent que les renseignements ainsi collectés et utilisés concernent des personnes, certains peuvent avancer qu'elles ne peuvent pas toujours être identifiées⁶⁸⁷.

Fondamentalement, cette pratique illustre la question du seuil à partir duquel des renseignements doivent être considérés comme identificatoires. Il est possible que plusieurs renseignements concernant une personne ne puissent, même combinés, l'identifier. Or, plus on accumule des renseignements, plus cette somme de renseignements est à risque de devenir des renseignements personnels, dans la mesure où il devient plus probable que la personne puisse être identifiée, directement ou indirectement.

Ainsi, il peut être ardu pour les organisations de tracer une démarcation nette entre les renseignements personnels et ceux qui ne le sont pas⁶⁸⁸. Cela complique la détermination du moment où les mesures de protection adéquates doivent être mises en place⁶⁸⁹. Il devient réciproquement difficile pour les personnes de déterminer les renseignements qu'elles doivent éviter de divulguer pour protéger les aspects plus intimes de leur existence. Les exemples de Target et de Cambridge Analytica, évoqués dans la section 2.1.3.2.1.3, montrent bien comment des inférences particulièrement révélatrices peuvent être tirées de données que les personnes n'estiment pas importantes à première vue. Partant, il est difficile pour les personnes d'exercer leur contrôle sur les renseignements personnels⁶⁹⁰.

La Commission considère ainsi que les pratiques d'inférence sur les personnes et de profilage sont susceptibles de mener rapidement à la création de renseignements personnels. **Cependant, elle considère que la possibilité désormais concrète d'exercer un pouvoir sur les personnes sans connaître leur identité rend le critère de l'identification potentiellement trop restrictif.** Ce critère remonte aux origines des lois sur la protection des renseignements personnels. Aux États-Unis, la protection de la vie privée envisagée par Warren et Brandeis à la fin du XIX^e siècle venait en réaction à

⁶⁸⁷ COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Position de principe sur la publicité comportementale en ligne » (13 août 2021), en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/bg_ba_1206/> (consulté le 26 novembre 2025).

⁶⁸⁸ Anna JOHNSTON, *Individuation: Re-imagining Data Privacy Laws to Protect Against Digital Harms*, vol 6 n° 24, coll. Brussels Privacy Hub Working Papers, Brussels Privacy Hub, 2020, p. 7, en ligne : <<https://brusselsprivacyhub.eu/publications/BPH-Working-Paper-VOL6-N24.pdf>>.

⁶⁸⁹ Kate CRAWFORD et Jason SCHULTZ, « Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms », (2014) 55 *Boston College Law Review* 93-128, p. 99, en ligne : <<https://gretchen.law.nyu.edu/cgi/viewcontent.cgi?article=2027&context=fac-articles>>.

⁶⁹⁰ Voir la section 2.1.1.3.4.



l'arrivée de la photographie et de la presse à grand tirage⁶⁹¹. Les préjudices anticipés à l'époque concernaient tous l'identité de la personne, qui pouvait se trouver dans l'embarras ou être mise à risque de préjudices physiques, psychologiques ou économiques si ses renseignements venaient à être connus des mauvaises personnes. Ces préjudices demeurent importants aujourd'hui, mais des pratiques contemporaines telles que le ciblage ou la discrimination sur la base de certaines caractéristiques ou certains comportements pourraient s'avérer préjudiciables, même sans l'identification des personnes concernées⁶⁹².

2.1.3.3.2. Le cadre législatif n'assimile pas l'inférence et la création de renseignements personnels à une collecte

Les règles actuelles en matière de collecte n'établissent pas explicitement que la création ou l'inférence de renseignements sur la base d'autres renseignements constituent une collecte au sens de la loi. La rédaction actuelle des lois peut plutôt laisser croire qu'il existe des renseignements créés ou inférés d'une part, et les renseignements recueillis auprès de la personne concernée ou de tiers d'autre part. Dès lors, certains pourraient croire que la création ou l'inférence ne sont pas sujettes aux dispositions applicables à la collecte.

Dans l'affaire *Val-des-Cerfs*, la Commission a cependant déterminé que la création d'indicateurs prédictifs du risque de décrochage scolaire, une forme claire d'inférence, équivaut à une collecte⁶⁹³. La Commission estime que cette précision revêt une telle importance qu'elle ne peut être consacrée que par une seule décision.

Par ailleurs, comme spécifié à la section 2.1.3.2.2.2, d'autres obligations s'ajoutent en fonction de la source de la collecte des renseignements, que ce soit auprès des personnes ou de tiers. Ce sont ces obligations qui confèrent aux personnes un contrôle sur le traitement de leurs renseignements personnels. Toutefois, si la production de renseignements personnels par inférence peut être considérée comme une collecte, il n'est pas clair qu'elle corresponde à une collecte *auprès des personnes concernées ou de tiers*. En effet, les inférences sont une nouvelle collecte à partir des renseignements déjà collectés.

Ainsi, il n'est pas clair qu'une organisation doit respecter son obligation d'information lors d'une collecte *auprès de la personne concernée* afin de l'informer qu'elle entend produire des inférences sur la base des renseignements personnels recueillis auprès d'elle. Cette situation contribue à la perte de contrôle des personnes sur leurs renseignements personnels, dans la mesure où elles ne peuvent évaluer correctement ce que les organisations ont le potentiel d'apprendre sur elles.

À cet égard, la Commission souligne que les lois semblent construites dans l'esprit de prémunir les personnes contre des traitements de renseignements personnels particulièrement invasifs de la vie privée. En effet, elles prévoient que, lorsque la collecte de renseignements personnels auprès des personnes est faite en ayant recours à des technologies qui permettent de les identifier, de les localiser ou de les profiler, elles doivent en être informées, et il leur revient spécifiquement d'activer ces fonctions si elles le

⁶⁹¹ Samuel D. WARREN et Louis D. BRANDEIS, « Warren and Brandeis, "The Right to Privacy" », (1890) 4-5 *Harvard Law Review*, en ligne : <https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html?utm_source=pocket_saves> (consulté le 22 janvier 2024).

⁶⁹² Des typologies des préjudices à la vie privée ont été développées; elles démontrent bien toute l'étendue des atteintes possibles. L'une des plus connues est la suivante : Danielle Keats CITRON et Daniel J. SOLOVE, « Privacy Harms », (2022) 102 *Boston University Law Review* 793-863, en ligne : <<https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf>>.

⁶⁹³ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 681, par. 28.



souhaitent⁶⁹⁴. Comme cette disposition s'applique uniquement lors de la collecte auprès des personnes concernées, elle ne semble pas viser les collectes subséquentes par inférence.

De plus, il subsiste un doute quant à la possibilité, selon les règles actuelles, pour les organisations d'inférer des renseignements personnels concernant des mineurs de moins de 14 ans, alors que la loi prévoit que le consentement de l'autorité parentale ou du tuteur doit être obtenu lorsque la collecte est faite auprès de ces mineurs, sauf lorsqu'elle est manifestement à leur bénéfice.

2.1.3.4. Recommandations

La production d'inférences algorithmiques est désormais un phénomène bien ancré dans la société. Considérant les préjudices qui peuvent découler de la production et de l'utilisation d'inférences, la Commission recommande que les lois en matière de protection des renseignements personnels en tiennent compte davantage.

2.1.3.4.1. Intégrer plus clairement la notion d'inférence à la définition des renseignements personnels

La Commission croit que la notion d'inférence devrait être mieux intégrée à celle de renseignement personnel. Par la même occasion, la notion d'inférence pourrait être associée à celle de profilage afin de clarifier les situations où des renseignements inférés sont accumulés et utilisés sans que les organisations cherchent forcément à identifier les personnes concernées.

De l'avis de la Commission, le CPVPC apporte une réponse pertinente à ces enjeux dans sa position de principe sur la publicité comportementale en ligne⁶⁹⁵. Il s'est particulièrement penché sur le statut de renseignement personnel des identifiants en ligne par lesquels les acteurs du milieu peuvent distinguer et suivre les personnes, par exemple les témoins de connexion et les adresses IP. Tenant compte de l'objectif, des moyens puissants qui sont mis en branle pour la collecte et l'analyse des renseignements et du caractère potentiellement très personnalisé du résultat, soit la publicité ciblée, le CPVPC a choisi d'adopter une approche pragmatique en affirmant que les informations recueillies dans ce cadre sont des renseignements personnels.

Selon la Commission, la même réflexion s'applique aux inférences algorithmiques servant au profilage, quelle que soit sa finalité. En elle-même, la production d'inférences repose sur des moyens puissants, et plus d'inférences sont produites, plus elles risquent de mener à l'identification des personnes.

C'est dans le même esprit que certains États ont intégré la notion d'inférence à la définition même des renseignements personnels. La loi californienne, dont un extrait est fourni à la section 2.1.3.5, peut être prise en exemple à ce sujet. Elle prévoit, à la suite de la définition de la notion de renseignement personnel, une liste non limitative de renseignements qui doivent être considérés comme personnels, y compris les inférences visant à constituer le profil d'une personne.

⁶⁹⁴ COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, COMMISSION D'ACCÈS À L'INFORMATION, COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE LA COLOMBIE-BRITANNIQUE, et COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ALBERTA, préc., note 496, par. 153.

⁶⁹⁵ COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 687.

Recommandation 33

Intégrer explicitement les inférences faites par profilage au sein de la définition de renseignement personnel dans la Loi sur l'accès et la Loi sur le privé ainsi que dans la définition de renseignement de santé et de services sociaux prévue à la LRSSS.

2.1.3.4.2. Élargir la définition des renseignements personnels

Malgré les considérations précédentes concernant le profilage, il demeure possible que des renseignements concernant des personnes puissent être inférés et utilisés sans que le régime de protection des renseignements personnels soit applicable, puisqu'ils ne permettraient pas de les identifier directement ou indirectement.

Selon la Commission, le critère d'identification ne permet plus de tenir compte de l'ensemble des préjudices qu'une personne pourrait vivre à la suite du traitement de renseignements la concernant et qui justifient la protection consacrée dans les lois. Partant, deux solutions peuvent être envisagées.

La première serait l'adoption d'un critère moins restrictif que celui de l'identification. S'il n'est plus requis d'identifier les personnes pour les profiler et exercer un pouvoir sur elles, il demeure nécessaire de les « distinguer dans la foule ». La portée matérielle des lois sur la protection des renseignements personnels pourrait ainsi être étendue pour viser tout renseignement permettant cette distinction. C'est dans ce sens que le concept d'*individualisation* a déjà été proposé, soit⁶⁹⁶ :

[...] la capacité d'individualiser, ou "d'isoler" une personne dans la foule, si bien qu'elle pourrait être tracée, profilée, ciblée ou contactée à un niveau individuel, ou sujette à des décisions ou à des actions ayant un effet sur elle – même si son "identité" n'est pas connue (ou possible à connaître).

L'individualisation n'est pas si éloignée de la conception de l'identification endossée par la jurisprudence québécoise. La Commission propose d'effectuer un pas supplémentaire, soit de séparer le renseignement personnel de l'identité concrète de la personne pour l'étendre à tous les renseignements permettant de la distinguer d'autres personnes.

La deuxième solution serait de préciser la façon dont les renseignements peuvent *concerner* une personne, même non identifiée. En contexte européen, le Groupe de travail « Article 29 » sur la protection des données⁶⁹⁷ s'y est penché, et ce, afin de répondre aux défis amenés par certaines technologies numériques⁶⁹⁸. L'analyse du groupe de travail précise trois conditions non cumulatives faisant en sorte qu'un renseignement concerne une personne :

- Le **contenu** du renseignement, lorsqu'il a directement trait à la personne.

⁶⁹⁶ A. JOHNSTON, préc., note 688, p. 7.

⁶⁹⁷ Il s'agit de l'ancêtre du Comité européen de la protection des données, organe qui voit à la cohérence de l'application du RGPD à travers tous les États membres de l'Union européenne.

⁶⁹⁸ GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, « Avis 4/2007 sur le concept de données à caractère personnel » (20 juin 2007), en ligne : <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_fr.pdf> (consulté le 27 novembre 2025).



- Sa **finalité**, qui réfère aux situations où le renseignement sera utilisé ou est susceptible de l'être, « afin d'évaluer, de traiter d'une certaine manière ou d'influer sur le statut ou le comportement d'une personne physique⁶⁹⁹ ».
- Son **résultat**, lorsque l'utilisation des renseignements, indépendamment du contenu ou de la finalité, risque « d'avoir un impact sur certains des droits et intérêts d'une personne, compte tenu de l'ensemble des circonstances du cas d'espèce⁷⁰⁰ ».

La Commission estime que ces trois liens entre les personnes et les renseignements décrivent bien comment des renseignements en viennent à concerner quelqu'un, ainsi que les effets qu'ils peuvent avoir sur les personnes, identifiables ou non.

Le législateur pourrait souhaiter conserver le critère d'identification au sein de la définition de renseignement personnel, d'autant que cela permettrait de maintenir une interopérabilité plus forte avec les lois d'autres États. Cependant, les critères susmentionnés pourraient y être ajoutés puisqu'ils permettent de tenir compte des utilisations de renseignements et de leurs effets que les régimes de protection des renseignements personnels doivent baliser. Ainsi, un renseignement qui ne permettrait pas l'identification de la personne, mais qui la concerne par ailleurs, pourrait être considéré comme un renseignement personnel.

L'État québécois ne serait d'ailleurs pas le premier à élargir de cette façon les critères constitutifs de sa définition des renseignements personnels. La loi californienne pourrait encore servir d'inspiration : dans son cadre, les renseignements sont personnels s'ils identifient, concernent ou décrivent une personne ou un ménage, ou s'ils peuvent rationnellement leur être associés ou reliés, directement ou indirectement.

Recommandation 34

Élargir la portée de la notion de renseignement personnel dans les lois québécoises, par exemple :

- en remplaçant le critère d'identification par un critère plus englobant; ou
- en ajoutant des critères complémentaires à l'identification.

2.1.3.4.3. Reconnaître expressément que la création et l'inférence de renseignements personnels équivalent à une collecte

Considérant l'importance des obligations associées à la collecte des renseignements personnels, la Commission estime qu'il devrait être explicite dans les lois les concernant que la création et l'inférence de tels renseignements sont assimilables à une collecte. Cette inclusion permettrait un gain en cohérence et en clarté, en plus de consolider une importante décision de la Commission⁷⁰¹.

⁶⁹⁹ *Id.*, p. 11.

⁷⁰⁰ *Id.*, p. 12.

⁷⁰¹ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 681.



Recommandation 35

Préciser que la création et l'inférence de renseignements personnels sont assimilables à une collecte pour l'application des lois sur la protection des renseignements personnels.

2.1.3.4.4. Adapter l'obligation d'information aux renseignements personnels inférés

Il est important que les organisations aient l'obligation de préciser aux personnes concernées les types de renseignements qui pourraient être inférés à partir des renseignements personnels les concernant. Il est possible, en effet, que ces inférences concernent des types de renseignements personnels que les personnes auraient autrement refusé de divulguer.

De l'avis de la Commission, il importe que la situation soit corrigée de façon que les personnes soient dûment informées de toute pratique d'inférence algorithmique. Elles devraient être avisées par les organisations des activités de profilage et des inférences dont elles feront l'objet au moment où elles choisissent de divulguer leurs renseignements personnels. Plus précisément, elles devraient être informées des moyens et des fins de la création ou de l'inférence de renseignements personnels, et de la nature des renseignements personnels produits.

Recommandation 36

Modifier les lois afin que les obligations d'information des organisations s'appliquent également à la création et à l'inférence de renseignements personnels.

Enfin, la Commission recommande que la création et l'inférence de renseignements personnels concernant des mineurs de moins de 14 ans soient sujets au consentement de l'autorité parentale ou du tuteur. Cette mesure s'impose dans un souci de cohérence et afin d'éviter que des organisations puissent inférer des renseignements personnels qu'elles n'auraient pas pu recueillir sans autorisation préalable.

Recommandation 37

Requérir le consentement du titulaire de l'autorité parentale ou du tuteur d'un mineur de moins de 14 ans pour que des inférences algorithmiques soient produites à son sujet, à moins que ces inférences soient manifestement à son bénéfice.

2.1.3.5. Pour aller plus loin : les définitions de la loi californienne

La loi californienne sur la protection des renseignements personnels est pionnière en ce qui a trait à l'encadrement des inférences. À l'instar du RGPD européen, elle fait suivre sa définition des renseignements personnels d'une liste non limitative d'éléments qui ont trait aux technologies numériques



et qui doivent être considérées comme des renseignements personnels. Les inférences faites dans l'objectif de profiler les personnes ou les ménages s'y retrouvent.

Le procureur général de la Californie a d'ailleurs observé que ce sont des pratiques comme celles de Cambridge Analytica, c'est-à-dire la collecte massive d'informations et leur utilisation dans le but d'identifier et d'exercer une influence sur des personnes à leur insu, qui animaient le législateur au moment d'écrire cet article. Plus largement, il conclut que « les inférences semblent être au cœur des problèmes dont [la loi] cherche à s'occuper⁷⁰². »

Les passages pertinents de la loi californienne sont reproduits ci-après⁷⁰³.

« (v) (1) “Personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

[...]

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.

(G) Geolocation data.

[...]

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

[...]

(r) “Infer” or “inference” means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data. »

⁷⁰² Rob BONTA et Susan DUNCAN LEE, *Opinion No. 20-303*, Bureau du Procureur général de Californie, 2022, p. 12-13, en ligne : <https://oag.ca.gov/system/files/opinions/pdfs/20-303.pdf>.

⁷⁰³ CCPA, art. 1798.140. (v).



2.1.4. Le moissonnage de renseignements personnels

Sommaire

Le moissonnage de données consiste en l'extraction automatisée de vastes quantités de données disponibles sur le Web. Il s'agit d'une pratique répandue, qui sert notamment au développement des modèles d'IA les plus avancés. Cette extraction massive de données implique souvent la collecte de renseignements personnels accessibles en ligne.

Dans cette section, la Commission expose les enjeux suivants :

- **Le moissonnage de renseignements personnels est incompatible à plusieurs égards avec les lois garantissant leur protection.**
- **Cette pratique cause des risques de préjudices importants pour les personnes concernées.**
- **Les entreprises ont parfois une conception erronée de la notion de renseignement à caractère public.**

Considérant la prévalence du moissonnage et les enjeux qui y sont associés, la Commission recommande l'encadrement plus explicite de cette pratique.

2.1.4.1. Contexte

Le moissonnage de données consiste en l'extraction, par le truchement de programmes informatiques, de vastes quantités de données disséminées sur le Web. À terme, il permet la transformation de sommes de données non structurées en des ensembles qui peuvent être enregistrés et analysés dans une base de données centralisée ou des feuilles de calcul⁷⁰⁴. Généralement, le contenu de tous les sites Internet ouverts au public⁷⁰⁵ est susceptible d'être moissonné, permettant alors à des programmes de collecter automatiquement des données qui pourraient être collectées manuellement. Ce qui distingue ces deux approches, c'est l'étendue et la rapidité vastement supérieures du traitement de données typique de l'automatisation. Le moissonnage permet ainsi à ceux qui y ont recours d'acquérir un grand capital informationnel.

Le moissonnage n'est pas une pratique nouvelle : il est contemporain au développement du Web commercial dans les années 1990. Il sert aussi plusieurs finalités, comme l'indexation des sites Web, les recherches journalistiques et scientifiques, les études de marché, la surveillance des prix et des pratiques d'entreprises en compétition, ou encore l'analyse de modes et d'activités⁷⁰⁶. Toutefois, dans les dernières

⁷⁰⁴ Daniel J. SOLOVE et Woodrow HARTZOG, « The Great Scrape: The Clash Between Scraping and Privacy », *California Law Review* 2025.1521-1584, p. 1526, en ligne : <<https://www.californialawreview.org/print/great-scrape>>.

⁷⁰⁵ Les sites ouverts sont ceux où les utilisateurs peuvent accéder librement à l'information, sans limitation. Par exemple, les médias sociaux sont des sites Internet ouverts. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Internet ouvert », *Grand dictionnaire terminologique*, en ligne : <<https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26529672/internet-ouvert>> (consulté le 16 avril 2026).

⁷⁰⁶ D. J. SOLOVE et W. HARTZOG, préc., note 704, p. 1527.



années, le développement de l'**IA** s'est largement appuyé sur le moissonnage. Le développement des grands modèles de langage et d'autres modèles d'**IA** générative exige en effet le traitement d'une quantité incommensurable de données. Des initiatives comme Common Crawl ou LAION, qui ont moissonné le contenu de milliards de pages Web, notamment au bénéfice du développement de l'**IA**, ne suffisent plus⁷⁰⁷. Dans la course à la performance de leurs modèles d'**IA**, les entreprises propriétaires des plus grands modèles s'appuient sur de grandes quantités de données collectées depuis de multiples sources⁷⁰⁸, sans que les personnes concernées en aient nécessairement une conscience claire. La pression est si grande que ces entreprises se tournent vers des solutions comme le moissonnage et la transcription de vidéos hébergés par de grandes plateformes, le moissonnage de livres protégés par le droit d'auteur, ou encore l'utilisation de données appartenant aux utilisateurs de leurs propres services⁷⁰⁹.

Puisqu'il est à la racine du développement de technologies de pointe, le marché du moissonnage est plus actif que jamais⁷¹⁰ :

Aujourd'hui, le moissonnage est semblable à la ruée vers l'or – une accapARATION effrénée des données de la plus haute envergure. Le marché des logiciels de moissonnage dépasse le demi-milliard de dollars en 2023, et il est attendu qu'il croisse de 13 % dans les 12 prochaines années.

La pratique est si prévalente que, depuis l'année 2025, il est estimé que plus de la moitié du trafic Web mondial est attribuable aux programmes automatisés⁷¹¹.

Les sites qui recèlent d'abondantes quantités de renseignements personnels n'échappent pas au moissonnage. Ces renseignements peuvent être convoités par les moissonneurs à diverses fins, dont le développement de l'**IA**. Les grands médias sociaux, riches en contenus, sont fréquemment la cible d'opérations de moissonnage, mais les moissonneurs peuvent aussi s'abreuver à d'autres sources, par exemple les registres publics, des blogues, des revues laissées sur des sites d'indexation, ou encore des sites d'hébergement de contenu vidéo. **Cette collecte à grande échelle de renseignements personnels préoccupe la Commission.**

⁷⁰⁷ Cade METZ, Cecilia KANG, Sheera FRENKEL, Stuart A. THOMPSON et Nico GRANT, « How Tech Giants Cut Corners to Harvest Data for A.I. », *The New York Times* (6 avril 2024), en ligne : <<https://www.nytimes.com/2024/04/06/technology/tech-giants-harvest-data-artificial-intelligence.html>> (consulté le 8 avril 2024).

⁷⁰⁸ Marie LANGÉ, Aurélie SIMARD, Bertrand MONTHUBERT, Jean CONSTANTIN et Yann DIETRICH, « Rethinking AI data: From scraping to sustainable and ethical data sharing », *OECD.AI* (31 mars 2026), en ligne : <<https://oecd.ai/en/wonk/rethinking-ai-data-from-scraping-to-sustainable-and-ethical-data-sharing>> (consulté le 2 avril 2026).

⁷⁰⁹ C. METZ, C. KANG, S. FRENKEL, S. A. THOMPSON et N. GRANT, préc., note 707.

⁷¹⁰ D. J. SOLOVE et W. HARTZOG, préc., note 704, p. 1529, notre traduction.

⁷¹¹ Sead FADILPAŠIĆ, « Bots now account for over half of all internet traffic », *TechRadar* (16 avril 2025), en ligne : <<https://www.techradar.com/pro/security/bots-now-account-for-over-half-of-all-internet-traffic>> (consulté le 2 avril 2026).



D'ailleurs, concernant le moissonnage de données, la Commission a notamment participé à des enquêtes communes sur les pratiques des entreprises Clearview AI⁷¹² et Open AI⁷¹³ avec ses homologues fédéral, albertain et britanno-colombien. Elle constate que les lois, dans leur état actuel, n'encadrent que partiellement cette pratique qui soulève pourtant des enjeux majeurs.

2.1.4.2. Situation actuelle

Les lois sur la protection des renseignements personnels imposent des obligations à la fois aux organisations qui détiennent et diffusent des renseignements personnels qui pourraient être moissonnés et à celles qui procèdent à l'extraction des données.

Les organisations qui diffusent publiquement des renseignements personnels doivent avant tout s'assurer de la légitimité de cette fin. Elles doivent respecter leur obligation d'information auprès des personnes qui leur fournissent leurs renseignements personnels⁷¹⁴. Ainsi, ces dernières doivent être informées, le cas échéant, du fait que les renseignements diffusés peuvent être collectés par des tiers au moyen de techniques de moissonnage et des fins visées, par exemple l'entraînement de l'IA⁷¹⁵.

Ces organisations sont aussi tenues de prendre les mesures propres à assurer la protection des renseignements personnels qui s'avèrent raisonnables compte tenu, notamment, de leur sensibilité, de leur quantité, de leur répartition et de leur support⁷¹⁶. En plus de prêter une attention toute particulière aux renseignements qu'elles diffusent, elles doivent ainsi prendre les mesures de protection raisonnables en fonction du contexte contre tout moissonnage non autorisé de renseignements personnels. Les mesures suivantes, mises de l'avant par des homologues de la Commission dans le cadre d'une déclaration commune sur le moissonnage, en sont des exemples⁷¹⁷ :

- Affecter une équipe à la surveillance des activités d'extraction et définir des rôles précis.
- Limiter le nombre d'accès ou le débit pour une même adresse IP.
- Limiter les accès ou bannir des adresses IP si des activités inhabituelles sont détectées.
- Prendre des mesures pour détecter les robots et les extracteurs de données, comme les tests captcha.

⁷¹² COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, COMMISSION D'ACCÈS À L'INFORMATION, COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE LA COLOMBIE-BRITANNIQUE, et COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ALBERTA, « Conclusions en vertu de la LPRPDE no 2021-001 : Enquête conjointe sur Clearview AI, Inc. par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta » (3 février 2021), en ligne : <<https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2021/lprpde-2021-001/#fn9-rf>> (consulté le 30 mars 2026) (l'ordonnance rendue par la Commission à la suite de cette enquête est présentement en appel devant la Cour du Québec; pris en délibéré, dossier n° 500-80-042393-224).

⁷¹³ COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, « La Commission d'accès à l'information enquêtera conjointement sur ChatGPT avec le Commissariat fédéral et des autorités provinciales de protection de la vie privée » (25 mai 2023), en ligne : <<https://www.cai.gouv.qc.ca/actualites/commission-acces-information-enquetera-conjointement-sur-chatgpt-avec-commissariat-federal-et-autorites-provinciales-protection-vie-privee>> (consulté le 2 avril 2026).

⁷¹⁴ Ces obligations sont présentées dans la section 2.1.1.2.2.

⁷¹⁵ Loi sur l'accès, art. 65; Loi sur le privé, art. 8.

⁷¹⁶ Loi sur l'accès, art. 63.1; Loi sur le privé, art. 10; LRSSS, art. 99.

⁷¹⁷ DIVERSES AUTORITÉS MEMBRES DE L'ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, « Déclaration commune sur l'extraction de données et la protection des renseignements personnels », *Commissariat à la protection de la vie privée du Canada* (24 août 2023), en ligne : <https://www.priv.gc.ca/fr/nouvelles-du-commissariat/discours-et-declarations/2023/js-dc_20230824/> (consulté le 30 mars 2026); DIVERSES AUTORITÉS MEMBRES DU GROUPE DE TRAVAIL SUR LA COOPÉRATION INTERNATIONALE EN MATIÈRE D'APPLICATION DE LA LOI DE L'ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, « Déclaration commune finale sur l'extraction de données et la protection des renseignements personnels », *Commissariat à la protection de la vie privée du Canada* (28 octobre 2024), en ligne : <https://www.priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2023/js-dc_20230824/> (consulté le 28 octobre 2024).



- Spécifier, à même les conditions d'utilisation, que le moissonnage n'est pas autorisé.
- Intégrer des protocoles d'exclusion des robots.
- Mettre en œuvre des éléments de conception des sites pour complexifier le moissonnage, comme l'utilisation d'adresses URL aléatoires, ou encore le chargement de page dynamique.

Les entreprises qui moissonnent des renseignements personnels doivent respecter d'autres prescriptions légales. Avant toute chose, les renseignements personnels collectés doivent l'être en vertu d'un intérêt sérieux et légitime qu'entretient préalablement l'entreprise⁷¹⁸. Les renseignements personnels recueillis doivent se limiter à ceux qui sont nécessaires à la réalisation des fins déterminées avant la collecte⁷¹⁹. En vertu du principe cardinal de la nécessité, ces entreprises doivent appliquer le test de nécessité, et donc mettre en balance leur intérêt et les préjudices subis par les personnes concernées par la collecte afin de déterminer si elles peuvent y procéder. Elles doivent ainsi chercher à minimiser l'atteinte au droit à la vie privée qu'elle constitue. Pour ce faire, elles peuvent entre autres exclure certaines catégories de renseignements personnels de leur moissonnage, que ce soit par l'application de filtres lorsque possible, ou par l'exclusion de certains types de sites. Elles doivent aussi veiller à supprimer les renseignements non nécessaires qui auraient été collectés malgré tout et respecter les consignes des sites qui s'opposent clairement au moissonnage de leur contenu⁷²⁰. Par surcroît, les entreprises qui procèdent à la collecte de renseignements personnels par le truchement du moissonnage doivent s'assurer de tenir compte du contexte de la collecte. D'une part, elles doivent s'assurer que les organisations diffusant les renseignements personnels se sont acquittées de leur obligation d'information envers les personnes concernées. De l'autre, elles doivent aussi s'abstenir de moissonner des renseignements personnels rendus disponibles sans l'autorisation ou contrairement à la volonté des personnes concernées, par exemple à la suite d'un incident de confidentialité.

Enfin, sous réserve d'exceptions très limitées, les entreprises qui collectent des renseignements personnels auprès de tiers, soit les propriétaires des sites Web publics, doivent au préalable s'assurer que les personnes concernées ont validement consenti à cette collecte ou, à défaut, obtenir de leur part un tel consentement⁷²¹. En effet, une entreprise ne peut procéder à la collecte auprès de tiers sans le consentement de la personne concernée que si la loi l'y autorise, ou encore si certaines conditions liées à l'intérêt des personnes concernées ou à la nécessité de s'assurer de l'exactitude des renseignements personnels sont remplies⁷²².

2.1.4.3. Enjeux

Le moissonnage, tant dans son principe que dans sa pratique, soulève plusieurs enjeux liés à la protection des renseignements personnels. Il s'harmonise peu aux fondements mêmes des lois en la matière, et il peut causer des risques importants pour les personnes dont les renseignements personnels sont collectés. En pratique, il arrive aussi que des entreprises qui font du moissonnage aient une conception erronée de la notion de renseignement à caractère public.

⁷¹⁸ Loi sur le privé, art. 4.

⁷¹⁹ *Id.*, art. 5.

⁷²⁰ COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, « La base légale de l'intérêt légitime : fiche focus sur les mesures à prendre en cas de collecte des données par moissonnage (web scraping) » (19 juin 2025), en ligne : <https://www.cnil.fr/fr/focus-interet-legitime-collecte-par-moissonnage> (consulté le 2 avril 2026).

⁷²¹ Loi sur le privé, art. 6.

⁷²² *Id.*, art. 6 al. 2 et 3.



2.1.4.3.1. Le moissonnage cadre mal avec les principes de protection des renseignements personnels

Fondamentalement, le moissonnage enfreint les principes FIP, présentés à l'introduction du présent chapitre, sur lesquels se construisent les lois en matière de protection des renseignements personnels⁷²³. Il constitue souvent une appropriation de renseignements personnels sans l'autorisation des organisations qui les détiennent et sans que les personnes concernées en soient spécifiquement informées.

Partant, cette pratique ne peut être qu'en porte-à-faux avec des principes qui, en grande partie, visent à assurer la préservation de l'autonomie des personnes, l'imputabilité des organisations qui collectent des renseignements personnels ainsi qu'une utilisation équitable de ceux-ci. En outre, le moissonnage est parfois mené pour constituer des bases de données avant même que des fins spécifiques n'aient été déterminées, et il s'inscrit généralement dans une dynamique de collecte immodérée de renseignements. Malgré les mesures mises en place par les organisations pour le prévenir, il peut aussi arriver que les entreprises contournent les mesures de sécurité mises en place par celles qui rendent des renseignements personnels accessibles en ligne.

Cette disharmonie inhérente entre les principes fondamentaux de la protection des renseignements personnels et le moissonnage fait en sorte que cette pratique se concilie mal avec les lois actuelles. Une opposition existe entre le principe de nécessité et le moissonnage. Malgré les mesures d'atténuation qui peuvent être prises, la pratique entre, par définition, en contradiction avec la visée de minimisation de la collecte. Conséquemment, il est possible que plusieurs occurrences de moissonnage ne puissent être justifiées sous le cadre de la nécessité, et ce, sans considération pour la légitimité des fins proposées.

Par ailleurs, considérant la nature automatisée du moissonnage et le volume de données traitées par le truchement de cette pratique, il existe un risque réel que des renseignements personnels soient recueillis par les programmes, et ce, même lorsque telle n'est pas l'intention des entreprises et malgré les mesures techniques qui peuvent être prises. Même involontaire, une telle collecte de renseignements personnels contrevient notamment au principe de nécessité et requiert des mesures correctives.

2.1.4.3.2. Le moissonnage peut entraîner de lourdes conséquences

Le moissonnage de renseignements personnels s'inscrit dans le contexte de l'économie de la donnée. Des experts y reconnaissent une pratique constitutive du capitalisme de surveillance⁷²⁴ qui s'est développé dans les environnements numériques⁷²⁵. Le moissonnage peut d'ailleurs prendre toutes les allures de la surveillance de masse⁷²⁶, notamment lorsqu'il est utilisé à des fins de profilage publicitaire. *A fortiori*, cette surveillance peut même constituer le produit mis en marché. C'est le cas de quelques entreprises qui offrent des services de reconnaissance faciale aux forces de l'ordre ou au grand public.

⁷²³ D. J. SOLOVE et W. HARTZOG, préc., note 704, p. 1549-1558.

⁷²⁴ Shoshana ZUBOFF, *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, New York (É-U), PublicAffairs, 2019.

⁷²⁵ D. J. SOLOVE et W. HARTZOG, préc., note 704, p. 1567-1570.

⁷²⁶ *Id.*, p. 1569-1570.



Présentement, les organisations qui pratiquent le moissonnage de données à grande échelle en retirent tous les bénéfices, alors que les risques pèsent entièrement sur les personnes dont les renseignements personnels sont recueillis.

Considérant l'ampleur des pratiques de moissonnage, ces risques doivent être envisagés à l'échelle de la société.

Par exemple, l'extraction des renseignements personnels diffusés sur les grands médias sociaux peut concerner à elle seule des milliards de personnes. Outre la perte de contrôle inhérente au moissonnage, plusieurs préjudices peuvent découler de l'utilisation de renseignements personnels moissonnés par des organisations ou des individus mal intentionnés, dont :

- des cyberattaques ciblées;
- l'usurpation d'identité;
- le contrôle, le profilage et la surveillance;
- l'utilisation des renseignements personnels à des fins politiques;
- le marketing direct non sollicité et l'envoi de pourriels⁷²⁷.

Au surplus, il est possible que certains acteurs moissonnent d'ores et déjà des données protégées dans l'objectif de les décrypter lorsque la technologie le permettra. En effet, l'informatique quantique permettra de déjouer sans problème les techniques de cryptographie traditionnelles. L'approche dite « récolter maintenant, décrypter plus tard » est l'un des plus grands risques associés à son émergence prochaine. S'il s'avère, des opérations de moissonnage aujourd'hui pourraient être la source de préjudices majeurs demain⁷²⁸.

2.1.4.3.3. Les entreprises peuvent entretenir une conception erronée des renseignements à caractère public

Le moissonnage est fréquemment justifié par ceux qui le pratiquent par la présomption selon laquelle les renseignements personnels accessibles sur Internet sont « publics » et que, par conséquent, les obligations habituellement liées à leur collecte et à leur confidentialité ne s'appliquent pas. C'est l'un des arguments qu'avancait l'entreprise Clearview AI en réponse à la Commission et ses homologues⁷²⁹. Or, aucune loi québécoise ne confère un caractère public aux renseignements personnels du simple fait qu'ils sont diffusés sur Internet⁷³⁰. La Loi sur le privé prévoit plutôt que certains renseignements personnels sont soustraits aux règles relatives à la collecte et qu'ils perdent leur caractère confidentiel lorsqu'ils ont un caractère public en vertu d'une loi⁷³¹. Il s'agit donc d'un statut particulier, conféré non pas par la simple diffusion en ligne des renseignements, mais par le législateur à des fins précises. C'est le cas, par exemple, des renseignements contenus dans des registres publics comme le registre foncier. D'ailleurs, les renseignements à caractère public ne peuvent être utilisés que conformément aux fins pour lesquelles ils sont désignés. Ainsi, malgré ce statut, ils ne sauraient être moissonnés à d'autres fins⁷³².

⁷²⁷ DIVERSES AUTORITÉS MEMBRES DE L'ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, préc., note 717.

⁷²⁸ NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, « What Is Post-Quantum Cryptography? » (13 août 2024), en ligne : <<https://www.nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography>> (consulté le 16 avril 2026).

⁷²⁹ COMMISSION D'ACCÈS À L'INFORMATION, *Enquête à l'égard de Clearview AI Inc.*, dossier 1023158-S, 2021, par. 84, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/decisions-en-surveillance/1023158-S_decision-cai-clearview-ai-inc-2021-12-14.pdf> (en appel devant la Cour du Québec; pris en délibéré, dossier n° 500-80-042393-224).

⁷³⁰ *Id.*, par. 86.

⁷³¹ Loi sur le privé, art. 1.

⁷³² Voir *R.D. c. Racine (Municipalité de)*, 2011 QCCA 148, par. 28, en ligne : <<https://canlii.ca/t/fm4kh>> (consulté le 9 avril 2026).



La Commission est préoccupée par la perception selon laquelle des renseignements personnels accessibles publiquement peuvent être collectés sans restriction et utilisés sans égard pour leur confidentialité. La diffusion par une personne de ses renseignements personnels ne signifie pas qu'elle endosse toute utilisation que toute autre partie voudrait en faire.

2.1.4.4. Recommandation

Compte tenu de la prévalence du moissonnage et de la tension qui existe entre cette pratique et les principes de protection des renseignements personnels, la Commission estime qu'il y a lieu de l'encadrer plus explicitement.

La loi actuelle ne laisse que peu de contrôle aux personnes qui comptent communiquer des renseignements personnels en ligne⁷³³. Avant tout, elles doivent dûment s'informer des pratiques des organisations qui en font la collecte initiale. Cela passe, le plus souvent, par la lecture des politiques de confidentialité et autres contrats d'adhésion. Or, ces documents peuvent être nombreux et complexes, si bien que les pratiques peuvent ne pas être bien comprises. Qui plus est, même en toute connaissance de cause, les personnes sont contraintes à faire un choix entre deux possibilités insatisfaisantes :

- Accepter de divulguer des renseignements personnels, lesquels pourraient être moissonnés par des organisations qu'elles ne connaissent pas, à des fins dont elles ignorent globalement la teneur. Ce faisant, elles acquiescent malgré elles à perdre le contrôle sur leurs renseignements personnels ainsi que les risques associés, et ce, alors même qu'il leur est impossible de les estimer correctement⁷³⁴.
- S'abstenir de diffuser des renseignements personnels, ce qui peut limiter leur liberté d'expression⁷³⁵ ou leur accès à des services dont elles voudraient profiter.

La Commission reconnaît que les individus ont un rôle important à jouer dans la protection de leurs renseignements personnels. **Cependant, elle souligne les attentes légitimes qu'elles ont de pouvoir naviguer au sein d'environnements où ils ne sont pas susceptibles d'être systématiquement épiés ou constamment pris comme source de données.** Dans les conditions actuelles, le moissonnage occasionne un aléa moral⁷³⁶ : les organisations sont fortement incitées à collecter et à utiliser de grands volumes de renseignements personnels puisque les bénéfices leur reviennent et que les risques reposent sur les personnes concernées⁷³⁷.

La Commission ne saurait exclure que le moissonnage de renseignements personnels puisse être utilisé à des fins sérieuses et légitimes, voire à des fins qui s'accordent à l'intérêt public. Conséquemment, le législateur pourrait ne pas souhaiter interdire le moissonnage, qui pourrait toutefois être balisé de telle sorte qu'il ne puisse servir qu'à des finalités socialement acceptables. La Commission suggère deux avenues possibles à cet égard.

D'une part, des pratiques interdites liées au moissonnage pourraient être intégrées aux lois afin de bannir les utilisations les plus problématiques. C'est le chemin qu'a choisi d'emprunter l'Union européenne en

⁷³³ En contexte de moissonnage, le contrôle individuel souffre d'ailleurs des limites exposées à la section 2.1.1.3.

⁷³⁴ M. LANGÉ, A. SIMARD, B. MONTHUBERT, J. CONSTANTIN et Y. DIETRICH, préc., note 708, p. 1563. Voir aussi, sur les notions de risque et d'incertitude, et le fait que la diffusion de renseignements personnels dans l'environnement numérique ne traduit pas une apathie pour la protection des renseignements personnels, l'ouvrage suivant : Ignacio COFONE, *The Privacy Fallacy - Harm and Power in the Information Economy*, Cambridge University Press, 2024, p. 35-37.

⁷³⁵ COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 720.

⁷³⁶ I. COFONE, préc., note 734, p. 59-62.

⁷³⁷ D. J. SOLOVE et W. HARTZOG, préc., note 704, p. 1578.



interdisant, dans son *Règlement sur l'IA*, l'utilisation ou la mise en marché de systèmes d'**IA** qui créent ou développent des bases de données de reconnaissance faciale par moissonnage non ciblé d'images faciales provenant du Web ou de la vidéosurveillance⁷³⁸. La Commission y revient dans la section 2.2.3.1.

D'autre part, le moissonnage de renseignements personnels pourrait n'être permis que pour des fins correspondant à l'intérêt public, à condition que des mesures de protection et des balises appropriées soient mises en place⁷³⁹. Ce critère pour la collecte s'ajouterait, dans le cas des entreprises, à leur intérêt sérieux et légitime. Il viserait essentiellement à aligner les intérêts des organisations et des personnes concernées, de telle sorte que l'aléa moral décrit précédemment soit atténué⁷⁴⁰. Les lois sur la protection des renseignements personnels prévoient d'ailleurs déjà des dispositions semblables dans le cas de la communication de renseignements personnels à des fins d'étude, de recherche ou de production de statistiques. En effet, cette communication n'est permise que si, entre autres choses, la fin visée l'emporte, eu égard à l'intérêt public, sur les conséquences de la communication et de l'utilisation des renseignements sur la vie privée des personnes concernées⁷⁴¹.

Dans ce cadre, les organismes publics qui comptent mener des activités de moissonnage de renseignements personnels devraient être tenus d'en aviser la Commission, qui pourrait ainsi en assurer le contrôle. La Commission formule une recommandation au sein de la section 2.1.5 pour ce qui relève des courtiers en données, dans le secteur privé.

Recommandation 38

Modifier les lois sur la protection des renseignements personnels de manière à définir et à encadrer le moissonnage de renseignements personnels.

⁷³⁸ *Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)*, JO L, 2024/1689, art. 5 (1) (e), en ligne : <<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32024R1689>>.

⁷³⁹ Voir D. J. SOLOVE et W. HARTZOG, préc., note 704, p. 1577 à 1583.

⁷⁴⁰ I. COFONE, préc., note 734, p. 60.

⁷⁴¹ Loi sur l'accès, art. 67.2.1; Loi sur le privé, art. 21.



2.1.5. Le courtage en données

Sommaire

Acteurs peu connus du public, les courtiers en données recueillent, agrègent, analysent et revendent des renseignements personnels, généralement sans aucune interaction directe avec les personnes concernées. La portée de leurs activités leur confère beaucoup de pouvoir, mais soulève des enjeux conséquents pour la vie privée des personnes.

Dans cette section, la Commission offre un aperçu du marché du courtage en données et attire entre autres l'attention sur l'important volume de renseignements que traitent ces courtiers, et ce, souvent dans une forte opacité. De plus, elle souligne la difficulté pour les personnes concernées de faire valoir leurs droits auprès de ces entreprises. Elle rappelle que les renseignements vendus peuvent comporter des inexactitudes préjudiciables aux personnes.

Face à ces enjeux, la Commission recommande l'adoption d'un encadrement renforcé du commerce de renseignements personnels, entre autres par l'extension du régime actuellement prévu par la Loi sur le privé pour les agents de renseignements personnels œuvrant dans le secteur du crédit.

2.1.5.1. Contexte

L'industrie du courtage en données constitue un exemple saillant de la mise à profit des renseignements personnels. En effet, la convergence de l'analyse des mégadonnées, de l'IA⁷⁴² et de la monétisation des renseignements personnels en temps réel dans diverses sphères économiques a contribué à un essor rapide de ce secteur d'activité au cours des dernières décennies. Il est ainsi plus profitable que jamais de vendre des renseignements personnels obtenus entre autres par moissonnage⁷⁴³, observation⁷⁴⁴ ou inférence⁷⁴⁵.

Généralement mené sous un épais voile d'opacité, le courtage mène à la constitution de vastes ensembles de données qui circulent sans transparence ni encadrement adéquats et qui ont des incidences majeures sur la vie privée de tous les citoyens. Pourtant, le public méconnaît le volume et la variété de renseignements personnels qui sont collectés et partagés par les courtiers. Les enjeux en matière de protection des renseignements personnels au sein de cette industrie sont donc généralement sous-estimés. La Commission invite à modifier la Loi sur le privé pour mieux tenir compte de la vente de renseignements personnels.

⁷⁴² Sur ces phénomènes, voir notamment la section 2.1.3.

⁷⁴³ Voir la section 2.1.4.

⁷⁴⁴ Voir la section 2.1.1.3.5.

⁷⁴⁵ Voir la section 2.1.3.



2.1.5.2. Situation actuelle

La Commission présente ci-après l'activité du courtage en données, puis certaines dispositions du cadre actuel en matière de protection des renseignements personnels qui s'y appliquent.

2.1.5.2.1. Le marché du courtage en données

Le courtage en données représente un marché qui devrait passer de 305,33 milliards de dollars américains en 2025 à 629,41 milliards de dollars américains d'ici 2035, affichant ainsi un taux de croissance annuel composé de 7,5 % au cours de cette période de prévision⁷⁴⁶.

Cette industrie regroupe « les entités qui recueillent, agrègent, analysent et revendent des renseignements personnels, souvent sans aucune interaction directe avec les personnes concernées⁷⁴⁷ ». Les fins poursuivies par cette activité sont diverses : on peut notamment penser au marketing, à la vérification d'identité ou à la détection de fraudes⁷⁴⁸. Des courtiers œuvrent dans différents secteurs d'activité, notamment en finance, en gestion du risque et en vérification, en marketing et publicité, en données de mobilité, en recherche de personnes et en santé⁷⁴⁹. Bien que les courtiers en données ne soient souvent pas ceux qui ont initialement collecté les renseignements qu'ils mettent ensuite à la disposition d'autres entreprises⁷⁵⁰, la vente de renseignements personnels peut constituer une activité secondaire pour des entreprises qui entretiennent, elles, des liens directs avec les personnes concernées.

Plusieurs éléments principaux caractérisent les activités des courtiers en données⁷⁵¹ :

- **La collecte à grande échelle de renseignements personnels.** Ceux-ci peuvent être obtenus auprès de diverses sources en ligne et hors ligne, notamment les sources publiques comme les recensements, les plumitifs ou les registres fonciers, mais également par le biais de cartes de fidélité, de concours, d'historique d'achats, de moissonnage de sites Web comme des médias sociaux, d'objets connectés, de trousseaux de développement logiciel intégrées à des applications et par une multitude d'autres moyens⁷⁵².
- **L'absence de contrôle des personnes concernées.** La plupart du temps, en l'absence d'une relation directe entre les courtiers et les personnes concernées, il est difficile pour elles d'exercer un quelconque contrôle à l'égard du commerce de leurs renseignements.

⁷⁴⁶ MARKET RESEARCH FUTURE, « Data Broker Market » (15 avril 2026), en ligne : <https://www.marketresearchfuture.com/reports/data-broker-market-11676> (consulté le 16 avril 2026); GRAND VIEW RESEARCH, « Data Broker Market Size And Share | Industry Report, 2025-2033 » (2025), en ligne : <https://www.grandviewresearch.com/industry-analysis/data-broker-market-report> (consulté le 6 octobre 2025).

⁷⁴⁷ Ruben D'HAUWERS, *Data Brokers Market Study*, coll. Support Pool of Experts Programme, Comité européen de la protection des données, 2026, p. 6, en ligne : https://www.edpb.europa.eu/system/files/2026-03/spe_databorkersmarketstudy_en.pdf, notre traduction; cette définition s'inspire de celle mise de l'avant par la FEDERAL TRADE COMMISSION, *Data Brokers: A Call for Transparency and Accountability*, 2014, p. 3, en ligne : <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>; dans une étude de 2014, le CPVPC reprend une définition similaire : GROUPE DE RECHERCHE DU COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Les courtiers en données - Regard sur les paysages canadien et américain*, 2014, en ligne : https://www.priv.gc.ca/media/1779/db_201409_f.pdf.

⁷⁴⁸ FEDERAL TRADE COMMISSION, préc., note 747, p. 3.

⁷⁴⁹ Tom KEMP, « A Look at the Different Types of Data Brokers », *Medium* (6 octobre 2022), en ligne : <https://tomkemp00.medium.com/a-look-at-the-different-types-of-data-brokers-5ed1d360d3ea> (consulté le 19 novembre 2025); voir aussi R. D'HAUWERS, préc., note 747, p. 9-10.

⁷⁵⁰ Rahul KANWAL et Kevin WALBY, *Tracking the Surveillance and Information Practices of Data Brokers: A Report*, The University of Winnipeg / Centre for Access to Information Justice, 2024, p. 9-10, en ligne : <https://www.uwinnipeg.ca/caij/docs/reports/tracking-the-surveillance-and-information-practices-of-data-brokers.pdf>.

⁷⁵¹ R. D'HAUWERS, préc., note 747, p. 6.

⁷⁵² R. KANWAL et K. WALBY, préc., note 750, p. 10-11.



- **Le profilage et le traitement de données.** En plus d'agréger des données « brutes », les courtiers sont également nombreux à les analyser pour en tirer des inférences au sujet de leurs préférences ou de leurs comportements.
- **La monétisation.** Les courtiers se financent par la vente des renseignements personnels accumulés ou des inférences produites, par transfert ou par l'accès sous licence⁷⁵³.

Les organisations se tournent vers les courtiers en données notamment pour avoir accès à des renseignements afin de mieux orienter leurs activités, parfois dans des contextes qui soulèvent d'importants enjeux pour les droits des personnes.

« Les entreprises de vente au détail s'appuient sur de l'information recueillie par les courtiers en données pour créer des publicités ciblées et ainsi augmenter leurs ventes. Les équipes politiques se servent des analyses des courtiers en données pour effectuer des prédictions sur le comportement des électeurs. Les autorités de santé publique (durant la pandémie de COVID-19) mettent à profit l'information colligée par les courtiers en données pour générer des renseignements à propos des déplacements des personnes et des implications pour la vitesse de propagation de la maladie. Au-delà du secteur privé, des courtiers en données établissent des partenariats avec l'Administration de la sécurité sociale et les départements de la Justice, de la Sécurité intérieure et d'État [des États-Unis]. Le gouvernement [américain] s'appuie aussi sur les courtiers en données pour effectuer des vérifications d'antécédents et du suivi de crédit⁷⁵⁴. »

En raison de l'opacité des activités des courtiers en données, il s'avère généralement difficile d'en quantifier le nombre ou d'en comprendre la répartition géographique⁷⁵⁵. Il est de même difficile d'évaluer l'ampleur de cette industrie au Québec. Tout indique toutefois que les citoyens québécois sont largement concernés par le courtage en données, considérant les méthodes de collecte employées : le moissonnage ou l'intégration de code dans les applications, mais aussi l'adhésion des personnes à des finalités très larges énoncées lors de la collecte de renseignements personnels dans toutes sortes de situations⁷⁵⁶.

2.1.5.2.2. Le cadre légal

Conscient des enjeux soulevés par le commerce des renseignements personnels, le législateur a introduit dès 1994, dans la Loi sur le privé, des règles particulières pour les « agents de renseignements personnels⁷⁵⁷ », en plus des règles générales applicables à toute entreprise qui détient des renseignements personnels⁷⁵⁸.

Ces agents sont définis comme « toute personne qui, elle-même ou par l'intermédiaire d'un représentant, fait le commerce de constituer des dossiers sur autrui, de préparer et de communiquer à des tiers des

⁷⁵³ T. KEMP, préc., note 749; Nicolas BAUDOUX et Benjamin VERBOOGEN, « Vous n'avez rien à cacher? Tant mieux, car tous vos déplacements sont à vendre en ligne », *L'Echo* (4 novembre 2025), en ligne : <<https://multimedia.lecho.be/telephone-localisation>> (consulté le 16 avril 2026).

⁷⁵⁴ R. KANWAL et K. WALBY, préc., note 750, p. 4, notre traduction, références omises.

⁷⁵⁵ R. D'HAUWERS, préc., note 747, p. 8-10.

⁷⁵⁶ La Commission aborde cette perte de contrôle dans la section 2.1.1.

⁷⁵⁷ Loi sur le privé, art. 70 à 79.1.

⁷⁵⁸ Ces règles ont notamment trait à la transparence et au consentement (voir la section 2.1.1.2.1) ou encore à la nécessité (voir la section 2.1.2.2).



dossiers de crédit au sujet du caractère, de la réputation ou de la solvabilité des personnes concernées par ces dossiers⁷⁵⁹ ». Chaque agent doit notamment :

- s'inscrire auprès de la Commission et l'aviser de tout changement en temps opportun⁷⁶⁰;
- adopter et appliquer des règles de conduite permettant aux personnes concernées par des renseignements qu'il détient d'y avoir accès ou de les faire rectifier⁷⁶¹;
- informer le public de ses activités par le moyen d'un avis publié sur leur site Web ou, s'il n'en a pas, par tout autre moyen approprié, l'avis devant entre autres indiquer⁷⁶² :
 - que l'agent détient et communique des renseignements sur autrui;
 - que les personnes concernées peuvent exercer leurs droits d'accès et de rectification;
 - le titre et les coordonnées du responsable de la protection des renseignements personnels;
 - les moyens pris pour garantir que les renseignements communiqués sont à jour et exacts, un principe important de la Loi sur le privé⁷⁶³;
 - les règles de conduite qu'il a établies;
 - les autres mesures prises pour assurer la confidentialité et la sécurité des renseignements personnels;
- détruire tout renseignement personnel recueilli il y a plus de sept ans, dans la majorité des cas⁷⁶⁴.

Plus récemment, en 2021, dans la foulée de grands incidents de confidentialité⁷⁶⁵, la *Loi sur les agents d'évaluation du crédit* est entrée en vigueur⁷⁶⁶. Cette loi, qui vise les agents de renseignements personnels traitant principalement avec les institutions financières autorisées ou les banques⁷⁶⁷, soit Équifax et Trans Union⁷⁶⁸, confère des droits aux personnes concernées par les dossiers détenus par ces agents et prévoit des règles particulières visant la surveillance et le contrôle de leurs pratiques commerciales et de gestion dans le but notamment de renforcer la protection des renseignements personnels⁷⁶⁹.

En somme, l'encadrement législatif spécifique au commerce des renseignements personnels au Québec est limité à celui d'agents qui font le commerce de renseignements personnels liés au crédit.

2.1.5.3. Enjeux

L'industrie du courtage en données soulève des enjeux importants, notamment en raison :

- des énormes quantités de renseignements personnels collectés, analysés, vendus et conservés par les courtiers;
- du manque de transparence de leurs pratiques;

⁷⁵⁹ Loi sur le privé, art. 70.

⁷⁶⁰ *Id.*, art. 70 et 72.

⁷⁶¹ *Id.*, art. 78.

⁷⁶² *Id.*, art. 79.

⁷⁶³ *Id.*, art. 11.

⁷⁶⁴ *Id.*, art. 79.

⁷⁶⁵ ASSEMBLÉE NATIONALE DU QUÉBEC, « Consultations particulières et auditions publiques sur le projet de loi n° 53, Loi sur les agents d'évaluation du crédit », dans *Journal des débats de la Commission des finances publiques*, 45-75, 2020, en ligne : <<https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/cfp-42-1/journal-debats/CFP-200825.html>> (consulté le 2 mars 2026), remarques préliminaires du ministre Éric Girard.

⁷⁶⁶ *Loi sur les agents d'évaluation du crédit*, préc., note 86.

⁷⁶⁷ *Id.*, art. 3.

⁷⁶⁸ AUTORITÉ DES MARCHÉS FINANCIERS, « Registre - Agents d'évaluation du crédit », en ligne : <<https://lautorite.qc.ca/grand-public/registre-agents-devaluation-du-credit>> (consulté le 15 avril 2026).

⁷⁶⁹ *Loi sur les agents d'évaluation du crédit*, préc., note 86, art. 1.



- de l'ampleur des incidents de confidentialité qui peuvent les affecter;
- des difficultés pratiques pour les personnes concernées d'exercer leurs droits auprès d'eux;
- de l'inexactitude potentielle des renseignements dont les courtiers font le commerce⁷⁷⁰.

2.1.5.3.1. Les courtiers recueillent un volume important de données sans transparence suffisante

Les types de renseignements personnels collectés par les courtiers en données sont très vastes, allant des informations de base, comme les renseignements d'identification (nom, adresse, date de naissance, numéro de téléphone, adresse courriel), aux plus sensibles, comme le numéro d'assurance sociale, les antécédents médicaux, les opinions politiques, l'orientation sexuelle ou encore le casier judiciaire⁷⁷¹.

« Le volume de renseignements en ligne et la puissance de l'analyse informatique démontrent clairement que l'information concernant les activités en ligne des individus va bien au-delà du profil sommaire. Le portrait d'un internaute devient moins opaque et plus révélateur lorsque l'on ajoute les activités hors ligne pour étoffer son profil. Il est même possible d'affiner les traits lorsque les renseignements viennent d'un large éventail d'industries et de secteurs avec lesquels l'individu interagit depuis des jours, des semaines, voire des années⁷⁷². »

La collecte de renseignements personnels par l'industrie du courtage en données est d'autant plus préoccupante lorsqu'elle vise des renseignements à fort potentiel d'inférence, telles les données de géolocalisation. À ce propos, des médias ont sonné l'alarme à plusieurs reprises et dans différents contextes quant à la collecte et à la vente quotidienne de données de géolocalisation de millions de téléphones par les courtiers en données, ainsi qu'à propos des risques que cette activité représente pour la vie privée des individus⁷⁷³.

Ainsi, il a été révélé que des courtiers détiennent, dans leurs bases de données, la localisation des utilisateurs de dizaines d'applications⁷⁷⁴, celles de responsables et d'employés du gouvernement ou du système judiciaire, comme les organismes chargés de l'application de la loi, les bases militaires ou les tribunaux⁷⁷⁵, et même les renseignements comportementaux et de géolocalisation de services liés aux véhicules connectés⁷⁷⁶.

⁷⁷⁰ Esma AïMEUR, G. BRASSARD et Muxue GUO, « How data brokers endanger privacy », (2022) 15 *Transactions on Data Privacy* 41-85, p. 42, en ligne : <<https://www.tdp.cat/issues21/tdp.a448a21.pdf>>.

⁷⁷¹ FEDERAL TRADE COMMISSION, préc., note 747, p. B-3 à B-6.

⁷⁷² GROUPE DE RECHERCHE DU COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 747, p. 6.

⁷⁷³ Voir par exemple N. BAUDOUX et B. VERBOOGEN, préc., note 753; Adrien SÉNÉCAT, Martin UNTERSINGER et Romain IMBACH, « Comment des applications grand public facilitent le pistage des utilisateurs à leur insu », *Le Monde* (15 janvier 2025), en ligne : <https://www.lemonde.fr/pixels/article/2025/01/15/comment-des-applications-grand-public-facilitent-le-pistage-des-utilisateurs-a-leur-insu_6498708_4408996.html> (consulté le 15 janvier 2025); Marie-Claude MALBOEUF, « Données de géolocalisation, on vous suit ! », *La Presse* (7 mai 2022), en ligne : <<https://www.lapresse.ca/affaires/2022-05-07/donnees-de-geolocalisation-on-vous-suit.php>> (consulté le 16 avril 2025); Stuart A. THOMPSON et Charlie WARZEL, « Twelve Million Phones, One Dataset, Zero Privacy », *The New York Times* (19 décembre 2019), en ligne : <<https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>> (consulté le 18 avril 2026).

⁷⁷⁴ A. SÉNÉCAT, M. UNTERSINGER et R. IMBACH, préc., note 773; M.-C. MALBOEUF, préc., note 773.

⁷⁷⁵ Justin SHERMAN, « Data Brokers and Threats to Government Employees », *Lawfare Institute* (22 octobre 2024), en ligne : <<https://www.lawfaremedia.org/article/data-brokers-and-threats-to-government-employees>> (consulté le 24 octobre 2024); N. BAUDOUX et B. VERBOOGEN, préc., note 753.

⁷⁷⁶ FEDERAL TRADE COMMISSION, « FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent » (16 janvier 2025), en ligne : <<https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-general-motors-sharing-drivers-precise-location-driving-behavior-data>> (consulté le 16 avril 2025).



Or, les données de géolocalisation, qui sont pratiquement impossible à anonymiser⁷⁷⁷, sont particulièrement sensibles, car elles permettent à leur détenteur de connaître la position géographique d'une personne ou d'inférer d'autres informations sensibles supplémentaires, comme les croyances religieuses, l'orientation sexuelle ou encore l'état de santé⁷⁷⁸. En outre, lorsqu'il s'agit d'employés de structures critiques ou sensibles, la mise en ligne de ces renseignements peut constituer une menace pour la sécurité de ces personnes ou des structures concernées.

Au-delà de leur nature sensible, les renseignements personnels sont parfois collectés par les courtiers en données à l'insu des personnes concernées, dans certains cas en employant des pratiques qui peuvent se révéler trompeuses. Des enquêtes médiatiques ont révélé par exemple que de nombreuses applications ont collecté des renseignements de localisation alors que les paramètres de confidentialité des téléphones l'interdisaient ou sans le mentionner dans la section « Sécurité des données » de l'application⁷⁷⁹.

2.1.5.3.2. Les courtiers en données ont connu plusieurs incidents de confidentialité

Les nombreux incidents de confidentialité survenus chez des courtiers en données dans les dernières années ont mis en lumière l'étendue des banques de renseignements personnels détenues par ces entreprises, mais également leurs vulnérabilités en matière de sécurité de l'information. Pensons aux incidents suivants :

- En 2017, un cybercriminel a eu accès à des renseignements personnels concernant 143 millions de personnes dans le monde, dont 19 000 Canadiens, détenus par l'agence de crédit Équifax⁷⁸⁰.
- En 2018, un courtier en données aurait vu fuiter 340 millions de dossiers⁷⁸¹.
- En 2024, 270 millions de personnes auraient à leur tour vu leurs renseignements personnels volés auprès d'un courtier en données spécialisé en vérification d'antécédents⁷⁸².
- En 2025, des cybercriminels auraient obtenu l'accès à une vaste quantité de données de géolocalisation fines recueillies par un autre courtier⁷⁸³.
- En 2025, un courtier aurait subi une cyberattaque ayant permis à un tiers d'accéder aux renseignements de 364 000 personnes⁷⁸⁴.

⁷⁷⁷ Yves-Alexandre DE MONTJOYE, César A. HIDALGO, Michel VERLEYSEN et Vincent D. BLONDEL, « Unique in the Crowd: The privacy bounds of human mobility », (2013) 3-1 *Nature Scientific Reports* 1-5, DOI : 10.1038/srep01376.

⁷⁷⁸ J. SHERMAN, préc., note 775.

⁷⁷⁹ M.-C. MALBOEUF, préc., note 773; N. BAUDOUX et B. VERBOOGEN, préc., note 753.

⁷⁸⁰ COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Conclusions en vertu de la LPRPDE no 2019-001 : Enquête sur la conformité d'Equifax Inc. et d'Equifax Canada à la LPRPDE à la suite de l'atteinte à la sécurité des renseignements personnels en 2017 » (9 avril 2019), par. 1 et 86, en ligne : <<https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2019/lrpde-2019-001/>> (consulté le 16 avril 2025).

⁷⁸¹ Andy GREENBERG, « Marketing Firm Leaked Database With 340 Million Records », *Wired* (27 juin 2018), en ligne : <<https://www.wired.com/story/exactis-database-leak-340-million-records/>> (consulté le 16 avril 2025).

⁷⁸² Colin LECHER, « Following Markup investigation, Congress finds data brokers cost consumers tens of billions of dollars », *The Markup* (27 février 2026), en ligne : <<https://themarkup.org/privacy/2026/02/27/following-markup-investigation-congress-finds-data-brokers-cost-consumers-tens-of-billions-of-dollars>> (consulté le 18 mars 2026); Kevin MAIMANN, « Florida company faces multiple lawsuits after massive data breach », *CBC News* (16 août 2024), en ligne : <<https://www.cbc.ca/news/national-public-data-breach-lawsuits-1.7297197>> (consulté le 16 avril 2025).

⁷⁸³ Kevin COLLIER, « Location data broker Gravy Analytics was seemingly hacked, experts say », *NBC News* (10 janvier 2025), en ligne : <<https://www.nbcnews.com/tech/security/location-data-broker-gravy-analytics-was-seemingly-hacked-experts-say-rcna187038>> (consulté le 16 avril 2025).

⁷⁸⁴ Connor JONES, « Attack on LexisNexis Risk Solutions exposes data on 300k + », *The Register* (28 mai 2025), en ligne : <https://www.theregister.com/2025/05/28/attack_on_lexisnexis_risk_solutions/> (consulté le 28 mai 2025).



L'ampleur de ces incidents illustre que la quantité de renseignements personnels détenus par les courtiers en données peut susciter la convoitise d'acteurs malveillants et qu'en cas d'incident, les préjudices peuvent concerner pratiquement tout le monde.

2.1.5.3.3. L'opacité des pratiques des courtiers en données complique l'exercice des droits d'accès et de rectification

La méconnaissance par les individus de l'écosystème du commerce des renseignements personnels ainsi que des renseignements qui sont détenus à leur égard a pour conséquence qu'ils exercent un faible contrôle sur leur circulation, leur utilisation et leur exactitude.

Par exemple, pour des raisons semblables à celles présentées dans les sections 2.1.1.3.3 et 2.1.1.3.5, l'absence de lien direct entre la plupart des courtiers en données et les personnes concernées et la quantité de courtiers susceptibles de détenir des renseignements personnels à leur sujet rendent l'exercice des droits d'accès et de rectification pratiquement impossible. Certes, le cadre légal spécifique applicable aux agents de renseignements personnels vise à améliorer cette situation. Il prévoit la publication d'un registre des agents inscrits auprès de la Commission et impose à ces agents des obligations de transparence et de facilitation de l'exercice des droits par les personnes concernées. Mais ces protections ne concernent que le commerce de renseignements liés au crédit. Compte tenu de la variété des activités aujourd'hui accomplies par les agents, ce cadre paraît insuffisant.

À titre d'exemple pour exposer la complexité du problème, même lorsqu'ils sont tenus de mettre à la disposition des personnes des moyens simplifiés d'exercer leurs droits à l'égard de leurs renseignements personnels, comme c'est le cas, par exemple, en Californie, certains courtiers en données emploient des stratégies visant à rendre les pages Web concernées difficilement repérables dans des moteurs de recherche⁷⁸⁵.

2.1.5.3.4. Les inexactitudes dans les renseignements peuvent engendrer des préjudices importants

De plus en plus, les organisations se tournent vers des courtiers en données pour obtenir des renseignements personnels servant à prendre des décisions susceptibles d'avoir des effets importants sur la vie des individus, notamment en matière de crédit, d'assurances, d'emploi, de location de logements ou de biens ou de contrats de service, comme en téléphonie mobile. Lorsque ces décisions s'appuient sur des renseignements inexacts ou désuets, des conséquences préjudiciables majeures dans la vie de ces personnes peuvent en résulter.

En particulier, le fait que de nombreux courtiers en données réunissent des informations tirées de plusieurs sources et qu'ils vendent parfois des inférences obtenues à partir de ces renseignements, elles-mêmes sujettes à incertitude, rend les erreurs pratiquement inévitables⁷⁸⁶.

⁷⁸⁵ Dell CAMERON, « Data Broker Breaches Fueled Nearly \$21 Billion in Identity-Theft Losses », *Wired* (27 février 2026), en ligne : <<https://www.wired.com/story/data-broker-breaches-fueled-dollar209-billion-in-identity-theft-losses/>> (consulté le 27 février 2026).

⁷⁸⁶ R. KANWAL et K. WALBY, préc., note 750, p. 11.



« Une fois que l'information a été amenée dans le marché du courtage en données, il devient difficile de rattacher une information donnée à sa source originale pour toute combinaison des raisons suivantes : (1) les courtiers en données soutiennent que les sources d'information et les processus analytiques sont des secrets commerciaux, (2) plusieurs degrés de séparation éloignent les acheteurs et les vendeurs d'information de la collecte de renseignements personnels en raison de marchés complexes et (3) une proportion significative des données des courtiers est générée par [calcul informatique] et n'a pas de source empirique "réelle"⁷⁸⁷. »

Ici encore, bien que la Loi sur le privé prévoit des obligations particulières à ce sujet pour les agents de renseignements personnels, elles ne concernent que ceux qui font le commerce de renseignements liés au crédit.

2.1.5.4. Recommandation

En définitive, si l'agrégation et la vente de données par les courtiers peuvent parfois s'avérer positives dans certains contextes, comme en matière de santé publique, leurs pratiques de commercialisation des renseignements personnels génèrent des enjeux de grande ampleur, entre autres en raison du pouvoir considérable dont jouissent les courtiers en données⁷⁸⁸. **La mauvaise utilisation des renseignements personnels qu'ils commercialisent peut engendrer des préjudices majeurs à la fois pour la vie privée et, par voie instrumentale, pour la sécurité physique ou les finances des personnes, ou encore pour la démocratie s'il s'agit d'utilisation dans un contexte politique ou électoral.**

L'acceptabilité sociale du courtage en données pourrait nécessiter une réflexion approfondie : la Commission y invite d'ailleurs dans la section 2.2.3.1. Dans l'intervalle, les courtiers en données n'en jouent pas moins un rôle majeur dans la collecte et la circulation de renseignements personnels souvent sensibles, et ce, à propos de toute personne utilisant des appareils numériques ou apparaissant dans un registre public – c'est-à-dire à peu près tout le monde. Ce rôle justifie, selon la Commission, un élargissement du cadre actuel applicable aux agents de renseignements personnels dans la Loi sur le privé. En ce moment, seuls les courtiers en données dont les activités correspondent à ce qui est défini par la Loi sur le privé et la *Loi sur les agents d'évaluation du crédit*, soit des entreprises dont le commerce a pour objet le crédit, font l'objet d'un encadrement plus robuste tenant compte des risques liés à leurs activités.

Déjà en 1993, lors de l'adoption de la Loi sur le privé, la Commission des droits de la personne estimait qu'il était étonnant « qu'une loi sur la protection des renseignements personnels dans le secteur privé n'ait pas prévu un cadre particulier pour l'ensemble des entreprises dont la principale activité est le commerce de ces renseignements⁷⁸⁹ ».

La Commission estime que ce commentaire reste aujourd'hui pertinent dans un contexte où le courtage en données est en plein essor et où les risques pour la protection des renseignements personnels sont décuplés par l'étendue et le volume des renseignements personnels accessibles et les capacités

⁷⁸⁷ *Id.*, p. 11, notre traduction, références omises.

⁷⁸⁸ Urbano REVIGLIO, « The untamed and discreet role of data brokers in surveillance capitalism: a transnational and interdisciplinary overview », (2022) 11-3 *Internet Policy Review*, p. 10-11, DOI : 10.14763/2022.3.1670.

⁷⁸⁹ ASSEMBLÉE NATIONALE DU QUÉBEC, « Consultation générale sur le projet de loi n° 68, Loi sur la protection des renseignements personnels dans le secteur privé », dans *Journal des débats de la Commission de la culture*, 32-11, 1993, en ligne : <<https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/cc-34-2/journal-debats/CC-930223.html>> (consulté le 17 avril 2025), peu après 11 h 30.



croissantes d'analyse des données. Ainsi, elle recommande de renforcer les exigences applicables aux courtiers en données dans l'objectif notamment d'une meilleure transparence, tant à l'égard des personnes concernées que des autorités. La loi californienne, dont un survol est présenté à la section 2.1.5.5, pourrait servir d'inspiration à cet égard, d'autant que certaines des mesures qu'elle prévoit s'apparentent à celles déjà en place pour les agents de renseignements personnels dans la Loi sur le privé. Entre autres, cette loi prévoit la mise sur pied d'un registre public plus complet des courtiers en données et d'un guichet unique permettant aux personnes concernées d'exercer leurs droits d'accès ou de rectification à un seul endroit et par une seule action.

Quelques précisions s'imposent à l'égard de cet encadrement renforcé. En effet, il devrait :

- concerner toute entreprise faisant le commerce de renseignements personnels, qu'il s'agisse d'une activité principale ou secondaire;
- couvrir adéquatement le commerce de tout renseignement personnel, même anonymisé. La Commission considère que le statut anonymisé d'un renseignement n'amoindrit pas les préjudices lorsqu'il s'agit de la vente de vastes ensembles de données révélant des patrons quant aux habitudes, aux comportements ou aux caractéristiques de groupes de personnes⁷⁹⁰.
- viser à ce que des personnes ou des organisations malveillantes ne puissent faire le commerce de renseignements personnels. À l'instar de ce qui se fait notamment en matière d'offre de services monétaires⁷⁹¹, la Commission soulève l'idée qu'un principe d'exigence d'une habilitation sécuritaire puisse être considéré pour l'inscription des agents de renseignements personnels, en ce qui concerne tant les dirigeants que d'autres personnes exerçant un contrôle significatif dans l'entreprise.

Recommandation 39

Prévoir un encadrement législatif pour l'ensemble des entreprises faisant le commerce de renseignements personnels, passant notamment par :

- l'extension, à tous les courtiers en données, des règles particulières de la Loi sur le privé applicables aux agents de renseignements personnels;
- l'introduction d'une obligation, pour les courtiers en données, de déclarer à la Commission toute activité de moissonnage;
- la mise en place d'un registre public des courtiers en données qui collectent des renseignements personnels concernant des Québécois, comportant notamment des informations sur les types de renseignements vendus, les coordonnées de leur siège social ou de leurs établissements au Québec ainsi qu'un lien vers un site Web qui détaille la manière d'exercer ses droits en matière de protection des renseignements personnels;
- la mise en place d'un guichet unique gouvernemental permettant à toute personne d'exercer ses droits simultanément auprès de tous les courtiers en données enregistrés.

⁷⁹⁰ À cet égard, voir la section 2.1.1.3.9.

⁷⁹¹ *Loi sur les entreprises de services monétaires*, RLRQ, c. E-12.000001, art. 5 à 8.



2.1.5.5. Pour aller plus loin : l'encadrement californien du courtage de renseignements personnels

La loi californienne prévoit depuis 2019 un encadrement particulier à l'égard des courtiers en données dans le *Data Broker Registration Act*⁷⁹², qui a été bonifié en 2023. Le courtier en données y est défini comme une entreprise qui, sciemment, recueille et vend des renseignements personnels à propos d'un consommateur avec qui elle n'a pas de relation directe⁷⁹³.

Cette loi exige que les courtiers en données s'enregistrent annuellement auprès de l'agence californienne de protection des renseignements personnels, CalPrivacy⁷⁹⁴. Lors de cette inscription, les courtiers en données, en plus de payer des frais d'inscription, doivent fournir plusieurs informations, en déclarant notamment s'ils collectent des renseignements personnels de personnes mineures, des données de géolocalisation précises des consommateurs ou encore des données sur la santé reproductive des consommateurs. Ils doivent également fournir le lien d'une page de leur site Web qui détaille comment les consommateurs peuvent exercer leurs droits à l'égard de leurs renseignements personnels. CalPrivacy met à la disposition des consommateurs un registre des courtiers en données répertoriant l'information fournie par les courtiers lors de l'inscription⁷⁹⁵.

En outre, la loi instaure un mécanisme de « guichet unique⁷⁹⁶ » (appelé DROP pour *Delete Request and Opt-out Platform*), entré en vigueur en janvier 2026⁷⁹⁷. Ce guichet permet aux consommateurs californiens, par le biais d'une demande unique, d'exiger de chaque courtier en données détenant des renseignements personnels les concernant qu'il les supprime, qu'ils soient détenus par ce courtier ou par un prestataire de services ou sous-traitant associé. En ce sens, cette solution s'apparente à un mécanisme unifié d'exercice d'un droit comme ce que préconise la Commission à la section 2.1.1.5.1.

À partir d'août 2026, les courtiers en données enregistrés en Californie seront tenus d'accéder à ce guichet unique au moins une fois tous les 45 jours et de traiter toutes les demandes de suppression, sauf exception conformément à la loi⁷⁹⁸. Après qu'un courtier en données aura supprimé les renseignements personnels déjà détenus, ce dernier devra, tous les 45 jours, supprimer à nouveau tous les renseignements qu'il pourrait avoir recueillis sur le consommateur et ne pourra plus vendre ou partager de nouveaux renseignements personnels le concernant. Enfin, à partir de janvier 2028 et tous les trois ans à compter de cette date, chaque courtier devra être audité par un tiers indépendant afin de garantir sa conformité à ces dispositions⁷⁹⁹.

⁷⁹² *Data Broker Registration Act*, code civil de la Californie, division 3, partie 4, titre 1.81.48, en ligne : <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.48.&part=4.&chapter=&article=>>.

⁷⁹³ *Id.*, art. 1798.99.80(c).

⁷⁹⁴ *Id.*, art. 1798.99.82 et suiv.

⁷⁹⁵ CALPRIVACY, « California Data Broker Registry », en ligne : <https://cippa.ca.gov/data_broker_registry/> (consulté le 15 avril 2026).

⁷⁹⁶ CALPRIVACY, « Delete request and opt-out platform (DROP) », en ligne : <<https://privacy.ca.gov/drop/>> (consulté le 15 avril 2026).

⁷⁹⁷ *Data Broker Registration Act*, préc., note 792, art. 1798.99.86.

⁷⁹⁸ *Id.*, art. 1798.99.86(c) et (d).

⁷⁹⁹ *Id.*, art. 1798.99.86(e).



2.1.6. L'anonymisation des renseignements personnels

Sommaire

Depuis 2023, les organisations québécoises peuvent, à certaines conditions, anonymiser les renseignements personnels qu'elles détiennent au lieu de les détruire une fois leurs finalités accomplies. Cette opération vise à faire en sorte qu'ils ne permettent plus d'identifier directement ou indirectement une personne. Elle doit être réalisée en suivant des critères et modalités prévus dans un règlement édicté en 2024.

Malgré les attentes élevées envers l'anonymisation pour la revalorisation des renseignements, elle soulève des enjeux majeurs quant à leur protection. Les renseignements anonymisés présentent encore un risque de réidentification, lequel croît dans le temps et à mesure que progresse la technologie. Selon la Commission, le cadre législatif et réglementaire actuel n'en tient pas suffisamment compte, et sa portée reste trop limitée.

Dans cette section, la Commission aborde principalement les enjeux suivants :

- L'encadrement actuel ne vise pas explicitement l'anonymisation réalisée à d'autres étapes du cycle de vie du renseignement personnel.
- Les critères et modalités d'anonymisation sont insuffisamment définis.
- La communication de renseignements anonymisés engendre une perte de contrôle.

Elle formule diverses recommandations pour :

- étendre l'encadrement et ainsi unifier les règles et éviter les interprétations divergentes;
- clarifier les critères et modalités applicables à l'anonymisation;
- interdire en tout ou en partie la diffusion de renseignements anonymisés.

2.1.6.1. Contexte

Les renseignements personnels peuvent être vecteurs de valeur commerciale ou sociétale au-delà de la première utilité pour laquelle ils ont été recueillis. C'est pourquoi les lois sur la protection des renseignements personnels ont toujours prévu des possibilités pour les réutiliser à d'autres fins dans certaines circonstances, notamment en matière de recherche⁸⁰⁰. En temps normal, le cycle de vie du renseignement personnel prend fin par sa destruction, lorsque les fins auxquelles il a été recueilli ou utilisé sont accomplies, afin d'éviter la survenance d'atteintes supplémentaires à la vie privée des personnes concernées. C'est le cas, par exemple, si elles sont victimes d'un incident de confidentialité.

⁸⁰⁰ D'ailleurs, tant la Loi 25 que la LRSSS ont considérablement revu et facilité l'accès aux renseignements personnels à des fins de recherche.



En cette ère de revalorisation des données, le législateur a introduit des dispositions qui font en sorte que les renseignements personnels, une fois la finalité initiale de leur utilisation accomplie, peuvent encore servir à l'organisation qui les détient, notamment à des fins s'appuyant sur d'importantes masses de données comme la recherche, le développement de produits ou encore l'entraînement de l'IA. En 2023, il est donc devenu possible, au Québec, d'anonymiser les renseignements personnels plutôt que de les détruire, à certaines conditions. On recherche ainsi un équilibre entre utilité et protection. La pondération de ces deux objectifs détermine, en bonne partie, l'ampleur des transformations à appliquer aux ensembles de renseignements personnels pour les anonymiser.

Pourtant, l'anonymisation est un statut temporaire : les renseignements anonymisés d'aujourd'hui pourraient ne plus l'être demain.

Le risque de réidentification augmente en permanence : les technologies ne cessent de progresser, le raffinement des méthodes d'analyse permet des inférences toujours plus pointues⁸⁰¹, et les sources de données accessibles se multiplient, ce qui facilite leur recoupement.

Il est donc reconnu qu'il faut aborder l'anonymisation de renseignements personnels comme un processus continu visant à maintenir un très faible degré de risque de réidentification.

Le cadre législatif et réglementaire québécois n'apporte qu'une réponse partielle à ce défi. Il ne prend pas suffisamment en compte les risques résiduels d'identification des renseignements anonymisés. Par ailleurs, en introduisant l'anonymisation principalement comme solution de rechange à la destruction des renseignements personnels, il conserve un angle mort relatif à l'anonymisation intervenant à d'autres étapes du cycle de vie de ces renseignements.

2.1.6.2. Situation actuelle

La Loi sur l'accès⁸⁰², la Loi sur le privé⁸⁰³ et la LRSSS⁸⁰⁴ abordent l'anonymisation des renseignements personnels comme une option supplémentaire à leur destruction, une fois accomplies les finalités pour lesquelles ils ont été recueillis ou utilisés. Un renseignement est anonymisé « lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement » la personne qu'il concerne.

⁸⁰¹ Pour ne donner qu'un exemple, le développement des modèles d'IA appartenant à la famille des grands modèles de langage ou des modèles langage-vision laisse entrevoir une augmentation marquée des possibilités d'inférence et de réidentification de données, avec un taux de précision potentiellement élevé; voir, en matière de modèles de langage et dans le contexte de la réidentification de données non structurées : Simon LERMEN, Daniel PALEKA, Joshua SWANSON, Michael AERNI, Nicholas CARLINI et Florian TRAMÈR, « Large-scale online deanonymization with LLMs », 2026, DOI : 10.48550/arXiv.2602.16800; voir aussi, en matière de modèle langage-vision : PRIVACY INTERNATIONAL, *Nowhere to Hide - Privacy Risks and Policy Implications of AI Geolocation*, 2026, en ligne : <https://privacyinternational.org/sites/default/files/2026-02/Nowhere%20to%20Hide%20Privacy%20International_0.pdf>.

⁸⁰² Loi sur l'accès, art. 73.

⁸⁰³ Loi sur le privé, art. 23.

⁸⁰⁴ *Loi sur les renseignements de santé et de services sociaux*, RLRQ, c. R-22.1, art. 111 [ci-après LRSSS], en ligne : <<https://www.legisquebec.gouv.qc.ca/fr/document/lc/R-22.1>>.

La Loi sur l'accès et la Loi sur le privé limitent les raisons pour lesquelles les organisations peuvent anonymiser des renseignements plutôt que de les détruire :

- dans le secteur public, ce doit être pour les utiliser à des fins d'intérêt public⁸⁰⁵;
- dans le secteur privé, ce doit être pour les utiliser à des fins sérieuses et légitimes⁸⁰⁶.

La LRSSS, quant à elle, ne contient pas de telle balise.

L'anonymisation repose sur une vision différente de la conception binaire, traditionnelle, du renseignement personnel ou non. L'identifiabilité est plutôt comprise sur un spectre de probabilité d'identification de la personne concernée. Les renseignements personnels permettent d'identifier directement ou indirectement une personne concernée. Les renseignements personnels dépersonnalisés ne permettent plutôt que l'identification indirecte⁸⁰⁷. Les renseignements personnels anonymisés, quant à eux, ne conservent qu'un très faible risque de permettre l'identification directe ou indirecte.

Potentiel de réidentification



Dans les trois lois, on prévoit aussi que les renseignements doivent être anonymisés selon les meilleures pratiques généralement reconnues et selon les critères et les modalités déterminés par règlement. C'est en ce sens que le *Règlement sur l'anonymisation des renseignements personnels*⁸⁰⁸ (le Règlement sur l'anonymisation) a été édicté en 2024. Parmi les précisions opérationnelles qu'il apporte, il énonce qu'il n'est pas nécessaire de démontrer un risque nul pour appliquer le critère d'irréversibilité prévu dans les lois : il faut plutôt que l'analyse de l'organisation démontre que les risques résiduels de réidentification sont « très faibles⁸⁰⁹ ».

Le Règlement sur l'anonymisation prévoit la réévaluation périodique des renseignements anonymisés afin de confirmer que les risques de réidentification demeurent très faibles⁸¹⁰. L'analyse des risques doit « notamment considérer les avancées technologiques qui peuvent contribuer à réidentifier une personne ».

2.1.6.3. Enjeux

Selon la Commission, l'encadrement actuel de l'anonymisation au Québec n'est pas suffisamment englobant. Il semble propice aux interprétations divergentes, engendrant le risque que ce ne soient pas

⁸⁰⁵ Loi sur l'accès, art. 73.

⁸⁰⁶ Loi sur le privé, art. 23.

⁸⁰⁷ Loi sur l'accès, art. 65.1 al. 5; Loi sur le privé, art. 12 al. 4 par. 1.

⁸⁰⁸ *Règlement sur l'anonymisation des renseignements personnels*, RLRQ, c. A-2.1, r. 0.1, art. 7 [ci-après *Règlement sur l'anonymisation*].

⁸⁰⁹ *Id.*, art. 7 al. 3.

⁸¹⁰ *Id.*, art. 8.

toutes les démarches d'anonymisation qui suivent les règles définies dans les lois et dans le Règlement sur l'anonymisation. De plus, l'arrimage de ces instruments normatifs laisse planer certaines questions. Plus généralement, l'encadrement ne semble pas aller suffisamment loin pour tenir compte du risque persistant de réidentification des renseignements anonymisés.

2.1.6.3.1. L'encadrement actuel ne vise pas explicitement les démarches d'anonymisation menées à différentes étapes du cycle de vie

L'opérationnalisation de l'anonymisation n'est actuellement encadrée que lorsqu'elle constitue une solution de rechange à la destruction. C'est le contexte visé par les lois et le Règlement sur l'anonymisation.

Or, on peut envisager que l'anonymisation soit effectuée à d'autres étapes du cycle de vie des renseignements personnels. Une organisation pourrait ainsi appliquer des techniques d'anonymisation pendant la phase d'utilisation des renseignements, à titre de mesure de protection, par exemple, ou en vue de les communiquer.

Dans ce contexte, l'omission de la part du législateur d'encadrer l'anonymisation d'une manière plus générale soulève de nombreuses questions, dont quelques-unes occupent une place centrale :

- Est-ce que l'anonymisation à d'autres étapes du cycle de vie nécessite une autorisation légale pour être permise?
- Si l'anonymisation est permise à d'autres étapes du cycle de vie, est-ce qu'elle nécessite un consentement de la part des personnes concernées?
- Est-ce que le Règlement sur l'anonymisation est applicable aux démarches d'anonymisation menées lors des autres étapes du cycle de vie?

Il est clair pour la Commission que le mutisme des lois sur ces aspects entraînera des interprétations divergentes. Notamment, certaines organisations pourraient être amenées à conclure qu'il leur est permis d'anonymiser un renseignement personnel *avant* que les fins initialement prévues soient accomplies, dans la mesure où cette anonymisation constitue une fin identifiée lors de la collecte, une fin compatible avec celle-ci ou autorisée par la loi, ou encore si le consentement de la personne concernée a été obtenu⁸¹¹. Elles pourraient estimer que le Règlement sur l'anonymisation ne trouve pas application en ce cas, et dès lors ne pas se soumettre à ses dispositions, notamment en matière de méthode d'anonymisation, de recours à une personne compétente, d'analyse du risque de réidentification et de réévaluation périodique.

Par conséquent, toutes les démarches d'anonymisation ne seraient pas encadrées de la même manière selon leurs visées et l'étape du cycle de vie dans laquelle elles s'insèrent. Or, comme elles impliquent les mêmes enjeux, il importe que des règles similaires s'y appliquent, peu importe les circonstances.

2.1.6.3.2. Les critères applicables à l'anonymisation ne sont pas suffisamment définis

La précision du standard applicable pour conclure qu'un renseignement est anonymisé prend toute son importance dans un contexte où il ne peut être considéré comme tel de manière permanente et immuable.

⁸¹¹ COMMISSION D'ACCÈS À L'INFORMATION, *Avis [2 février 2024] de la Commission d'accès à l'information sur le projet de règlement sur l'anonymisation des renseignements personnels* publié dans la *Gazette officielle du Québec* du 20 décembre 2023, 2024, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/Avis-de-la-CAI_Projet-de-reglement-sur-lanonymisation_2-fevrier-2024.pdf>.



Il apparaît cependant que les lois et le Règlement sur l'anonymisation prévoient des critères distincts, potentiellement incompatibles :

- Les lois énoncent qu'un renseignement est anonymisé lorsqu'il est en tout temps raisonnable de prévoir dans les circonstances qu'il ne permet plus, *de façon irréversible*, d'identifier, même indirectement, la personne qu'il concerne.
- Le Règlement sur l'anonymisation prévoit que, pour appliquer le critère d'irréversibilité de l'identification, il n'est pas nécessaire de démontrer un risque nul, mais plutôt « *très faible* ».

Il paraît difficile de concilier ces deux critères puisqu'ils ne semblent pas prévoir le même seuil concernant les risques de réidentification⁸¹². Pourtant, cet élément touche à la définition même de l'anonymisation.

Cette possible incohérence est accentuée par l'absence, dans le Règlement sur l'anonymisation, d'une méthode d'évaluation du risque et d'échelle de niveaux de risques quantifiés correspondante. Cette situation soulève des questions qui demeurent sans réponse dans le cadre actuel :

- Quelles seront les interprétations et les applications pratiques de la notion de risque « *très faible*⁸¹³ »?
- Quel est l'écart entre le risque nul et le risque très faible⁸¹⁴?

Sans ces précisions, le critère de « risque résiduel de réidentification très faible » apparaît subjectif. Il laisse place à l'interprétation et entraîne la possibilité que des renseignements insuffisamment anonymisés échappent à des règles importantes de protection des renseignements personnels.

Certains types de renseignements ne peuvent probablement pas être adéquatement anonymisés⁸¹⁵ : ainsi, pour ceux-ci, le risque de réidentification pourrait ne jamais être considéré comme « *très faible* ». Il s'agit généralement de données extrêmement distinctives par nature, ou encore de données très détaillées, comportant par défaut de nombreuses dimensions. On peut par exemple penser aux :

- a) **données spatiales.** Vu le très haut degré de spécificité des déplacements individuels, il a été démontré qu'il est aisé de réidentifier une succession de points de géolocalisation assemblés sous la forme de trajets⁸¹⁶;

⁸¹² Ulrich AïvODJI, Caroline DESCHÊNES et Frédéric WILSON, « L'anonymisation des renseignements personnels au Québec : pistes de conformité technologiques et pratiques pour les entreprises privées », dans BARREAU DU QUÉBEC - SERVICE DE LA FORMATION CONTINUE (dir.), *Développements récents en matière de protection des renseignements personnels et droit de l'intelligence artificielle*, coll. Développements récents, n°571, Montréal, Éditions Yvon Blais, 2025, p. 113-160 à la page 134, en ligne : <<https://app.caij.qc.ca/fr/doctrine/document/developpements-recents-vol-571-c-ac8208b874e24a6c8364f7d8b5cc4372-lanonymisation-des-renseignements-personnels-au-quebec-pistes-de-conformite-technologiques-et-pratiques-pour-les-entreprises-privées>> (consulté le 17 mars 2025).

⁸¹³ Le seuil d'un risque « *très faible* » peut varier de plusieurs ordres de grandeur, en fonction de plusieurs paramètres comme la diffusion ou non des données, la probabilité d'une attaque et l'impact potentiel d'une réidentification. Voir notamment INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, « ISO/IEC 27559:2022: Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework » (2022), en ligne : <<https://www.iso.org/standard/71677.html>>, annexe B.

⁸¹⁴ U. AïvODJI, C. DESCHÊNES et F. WILSON, préc., note 812 à la page 134.

⁸¹⁵ INFORMATION COMMISSIONER'S OFFICE, « Introduction to anonymisation » (1 avril 2025), en ligne : <<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/anonymisation/introduction-to-anonymisation/>> (consulté le 6 mars 2026); AGENCIA ESPAÑOLA PROTECCIÓN DATOS et CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, *10 misunderstandings related to anonymisation*, 2021, p. 4, en ligne : <https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf>.

⁸¹⁶ Y.-A. DE MONTJOYE, C. A. HIDALGO, M. VERLEYSSEN et V. D. BLONDEL, préc., note 777.



- b) données génétiques ou biométriques.** Ces données sont si discriminantes qu'elles constituent justement le cœur d'analyses visant à établir l'identité exacte des individus;
- c) neurodonnées.** Amassées par des capteurs de l'activité cérébrale et neurologique, ces données sont hautement granulaires et multidimensionnelles et, malgré la variabilité inhérente due à ces capteurs, elles resteraient fortement distinctives⁸¹⁷.

La clarté des critères et modalités d'anonymisation est par ailleurs essentielle, d'une part en raison des répercussions pour les personnes en cas de mauvaise application et de l'autre, pour les organisations elles-mêmes. En effet, en cas de non-conformité, les répercussions peuvent être significatives compte tenu des sanctions associées. Or, des organisations peuvent croire à tort que les renseignements qu'elles utilisent sont anonymisés, alors qu'ils ne le sont pas au regard des meilleures pratiques en cette matière⁸¹⁸. Toute ambiguïté dans le Règlement sur l'anonymisation contribue à cette situation.

2.1.6.3.3. La circulation de renseignements anonymisés engendre une perte de contrôle

Étant donné qu'ils ne permettent plus d'identifier directement ou indirectement une personne, même temporairement, il y a lieu de croire que les renseignements anonymisés pourraient être communiqués ou diffusés à l'extérieur de l'organisation qui a procédé à l'anonymisation :

- Le partage de renseignements constitue l'un des principaux cas d'usage de l'anonymisation du point de vue des organisations⁸¹⁹. En interprétant l'encadrement actuel, certaines pourraient donc juger possible de communiquer ces renseignements à des tiers.
- Des renseignements anonymisés pourraient aussi être intégrés dans des jeux de données ouvertes, un contexte de diffusion très risqué vu l'absence de limites sur la circulation de ces données⁸²⁰.
- Des organismes publics pourraient devoir donner accès à des renseignements anonymisés en réponse à une demande d'accès aux documents. Le cas échéant, rappelons que s'ils sont assujettis au Règlement sur la diffusion, ils devraient également diffuser les documents transmis sur leur site Web, augmentant ainsi la portée de la circulation des renseignements anonymisés⁸²¹.

Ces possibilités de circulation sans balises soulèvent un enjeu de perte de contrôle. Comme déjà mentionné, les renseignements anonymisés restent sujets à un risque de réidentification, qui doit être « très faible » sur le moment, mais qui est appelé à croître. Dès lors qu'un tel renseignement quitte le giron de l'organisation, sa capacité à réévaluer périodiquement son statut pour limiter ce risque peut diminuer ou disparaître. Ainsi :

- Lorsqu'il y a communication de renseignements anonymisés à un destinataire connu et identifiable, l'organisation initialement détentrice est appelée à travailler de concert avec lui pour continuer d'assurer cette réévaluation du risque.

⁸¹⁷ Voir Takashi NISHIMOTO, Hiroshi HIGASHI, Hiroshi MORIOKA et Shin ISHII, « EEG-based personal identification method using unsupervised feature extraction and its robustness against intra-subject variability », (2020) 17-2 *Journal of Neural Engineering* 026007, DOI : 10.1088/1741-2552/ab6d89.

⁸¹⁸ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 811.

⁸¹⁹ Quatre des cinq cas d'usage courants impliquent effectivement une communication de renseignements personnels : COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, *De-identification Guidelines for Structured Data*, 2025, p. 18 à 24, en ligne : <<https://www.ipc.on.ca/en/media/5946/download?attachment>>.

⁸²⁰ Rapport quinquennal 2016, p. 158-159; COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, préc., note 819, p. 19-20.

⁸²¹ Règlement sur la diffusion, art. 4, par. 8.



Lorsqu'il y a diffusion de renseignements anonymisés, laquelle vise un public non identifié et ne peut être encadrée par entente, l'organisation détentrice perd définitivement le contrôle de la réévaluation. De plus, les destinataires du renseignement sont susceptibles de considérer qu'il ne répond pas à la définition d'un renseignement personnel, et ainsi de le traiter sans respecter les lois sur la protection des renseignements personnels.

« Une fois que des renseignements anonymisés sont rendus publics, le détenteur des données sera confronté à des limites importantes quant à sa capacité à imposer des conditions d'utilisation des données, ce qui signifie concrètement qu'il n'aura que très peu de contrôle sur celles-ci. L'efficacité de l'anonymisation dépendra presque entièrement des transformations appliquées au jeu de données. Les organisations devraient généralement partir de la prémisse qu'une attaque de réidentification aura lieu, que ce soit immédiatement ou dans le futur, puisque les utilisateurs pourront généralement conserver des copies locales des données diffusées publiquement⁸²². »

2.1.6.3.4. La LRSSS ne balise pas suffisamment l'anonymisation

Les renseignements de santé et de services sociaux sont, dans la plupart des cas, sensibles et fort distinctifs par nature. De ce fait, ils semblent plus difficiles à anonymiser, et les personnes concernées s'exposent de plus à des préjudices importants en cas de réidentification. Il importe dès lors que les organismes de santé et de services sociaux n'aient recours à l'anonymisation que dans des situations bien circonscrites.

La LRSSS ne prévoit pourtant aucune balise quant aux finalités qui permettent l'anonymisation, contrairement à la Loi sur l'accès et à la Loi sur le privé, qui exigent respectivement des fins d'intérêt public et des fins sérieuses et légitimes. La LRSSS contient cependant un renvoi explicite au Règlement sur l'anonymisation. Or, bien que celui-ci réitère que les organisations doivent respecter les balises de finalité, il ne fait référence qu'à la Loi sur l'accès ou à la Loi sur le privé. Dans ces circonstances, il existe un certain vide qu'il y aurait lieu de combler.

Notons par ailleurs que la limite à la commercialisation des renseignements inscrite à la LRSSS⁸²³ ne s'applique qu'aux renseignements de santé et de services sociaux. Or, dès qu'un renseignement est considéré anonymisé, il ne serait plus visé par cette restriction, puisqu'il ne permettrait plus d'identifier un individu. Cet enjeu est traité plus en détail dans la section 3.2.1.2.

2.1.6.4. Recommandations

Compte tenu de la complexité du processus d'anonymisation et des risques résiduels de réidentification, la Commission estime impératif de compléter l'encadrement actuel afin de le rendre plus englobant et de clarifier l'interprétation et l'application de ses dispositions.

⁸²² COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, préc., note 819, p. 19, notre traduction.

⁸²³ *Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives*, LQ 2023, c. 5, en ligne : https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2023/2023C5F.PDF, art. 1.



2.1.6.4.1. Étendre le cadre de l'anonymisation pour englober l'ensemble des cas d'usage et unifier les règles

La clarification du cadre légal en vigueur au Québec permettrait de consolider le régime applicable, au bénéfice de l'ensemble des acteurs concernés. La Commission estime que des modifications législatives s'imposent afin de préciser les circonstances dans lesquelles l'anonymisation de renseignements personnels est permise et d'établir les règles qui s'y appliquent.

Il y a notamment lieu de s'assurer qu'il soit explicite que toute démarche d'anonymisation, même lorsqu'elle n'est pas une solution de rechange à la destruction, soit soumise aux dispositions prévues par le Règlement sur l'anonymisation. En outre, puisque certains types de renseignements ne peuvent vraisemblablement être suffisamment anonymisés pour présenter réellement un risque faible pour les personnes concernées, il serait souhaitable de prévoir un véhicule réglementaire pour les exclure de toute possibilité d'anonymisation.

Il importe également que des règles claires s'appliquent à tout le cycle de vie des renseignements une fois anonymisés. Notamment, il convient d'imposer des balises explicites concernant les communications permises et interdites et des modalités pour les encadrer, comme la conclusion d'une entente interdisant, par exemple, toute communication subséquente des renseignements. À plusieurs égards, le législateur québécois pourrait s'inspirer du régime adopté par l'Alberta, notamment en ce qui concerne la manière d'aborder la création, l'utilisation et la communication de renseignements anonymisés. Ce régime est présenté dans la section 2.1.6.5.

Le fait de prévoir un encadrement plus complet s'appliquant aux renseignements une fois qu'ils ont été anonymisés permettrait aussi d'éviter toute interprétation selon laquelle ils ne sont plus encadrés par les lois sur la protection des renseignements personnels après cette transformation. L'anonymisation est un statut conféré à des renseignements qui demeurent, fondamentalement, personnels.

Recommandation 40

Préciser l'encadrement législatif applicable en matière d'anonymisation afin que :

- le Règlement sur l'anonymisation s'applique à toutes les démarches d'anonymisation, peu importe le moment du cycle de vie du renseignement personnel auquel elles sont réalisées;
- l'autorité réglementaire puisse prévoir des règles s'appliquant aux renseignements une fois qu'ils ont été anonymisés, à travers tout leur cycle de vie subséquent, notamment en ce qui concerne la communication;
- l'autorité réglementaire puisse exclure la possibilité d'anonymiser certains types de renseignements personnels.

2.1.6.4.2. Clarifier les critères et les modalités applicables à l'anonymisation

L'anonymisation exige une vigilance continue, des réévaluations périodiques et des mécanismes robustes de surveillance afin de préserver la confiance du public et d'assurer la conformité aux principes de protection de la vie privée. Pour ces raisons, il apparaît primordial que les exigences soient claires pour tous, ce qui passe par un standard clair concernant le statut de renseignement anonymisé. Ce standard



devrait être cohérent entre la législation et la réglementation et s'accompagner de prescriptions plus explicites quant à la quantification du risque qu'il implique.

Recommandation 41

Clarifier l'arrimage du standard d'anonymisation entre le Règlement sur l'anonymisation et les lois et préciser, dans le Règlement, une méthode d'évaluation du risque ou une échelle de niveau de risque.

Afin d'assurer l'harmonisation de la LRSSS avec la Loi sur l'accès et la Loi sur le privé, la Commission recommande aussi de prévoir, dans cette loi, une balise limitant les fins pour lesquelles les renseignements de santé et de services sociaux peuvent être anonymisés plutôt que détruits.

Recommandation 42

Ajouter une balise à la LRSSS pour restreindre l'utilisation possible des renseignements anonymisés, soit pour les seules fins d'intérêt public dans le cas des établissements du secteur public, et pour des fins sérieuses et légitimes dans le cas des établissements du secteur privé.

2.1.6.4.3. Permettre l'interdiction de la diffusion de renseignements anonymisés

Compte tenu de la perte de contrôle inhérente à la diffusion de renseignements anonymisés à l'extérieur d'une organisation, notamment en données ouvertes, il doit être possible, grâce à un règlement, de fermer la porte à cette pratique en tout ou en partie. En parallèle, les renseignements anonymisés devraient être exclus de la portée du droit d'accès aux documents. L'anonymisation devrait ainsi rester centrée sur l'extension des possibilités d'utilisation à l'intérieur de l'organisation détentrice, entre autres en étendant indéfiniment la période de conservation, ou encore sur la communication à des tiers connus, encadrée par une entente.



Recommandation 43

Prévoir :

- un pouvoir réglementaire permettant d'interdire en tout ou en partie la diffusion de renseignements anonymisés;
- une mention explicite, dans la Loi sur l'accès, que les renseignements anonymisés sont exclus de la portée du droit d'accès aux documents.

2.1.6.5. Pour aller plus loin : le régime albertain, un exemple d'encadrement législatif

Le gouvernement de l'Alberta a récemment réformé sa loi sur la protection des renseignements personnels applicable au secteur public en adoptant la *Protection of Privacy Act*⁸²⁴, désormais distincte de la loi sur l'accès à l'information.

L'une des nouveautés de ce régime est l'introduction de dispositions à l'égard des renseignements dits « non personnels », autrement dit anonymisés (*non-personal data*). La loi albertaine aborde plusieurs aspects discutés dans le présent rapport, notamment :

- l'anonymisation à d'autres étapes du cycle de vie, outre la destruction – la loi albertaine encadre la création, l'utilisation et la communication de renseignements non personnels, sous certaines conditions;
- la communication des renseignements non personnels et ses conditions, en précisant notamment :
 - les fins autorisées d'une telle communication;
 - les mesures d'évaluation du processus d'anonymisation;
 - les mesures de sécurité et de confidentialité;
 - les conditions de communication subséquente;
 - les ententes à conclure pour les communications;
 - les informations à consigner dans un registre;
- les règles d'accès aux renseignements non personnels, en prévoyant qu'ils ne peuvent être communiqués dans le cadre d'une demande d'accès à l'information en vertu de la loi sur l'accès à l'information albertaine.

Le nouveau régime de la loi albertaine concernant l'anonymisation est intelligible et succinct. Les dispositions pertinentes sont reproduites ci-après pour fins d'inspiration⁸²⁵.

« Non-personal Data

Creation of non-personal data

21(1) A public body may create non-personal data only for one or more of the following purposes:

⁸²⁴ *Protection of Privacy Act*, SA 2024, c. P-28.5, en ligne : <https://kings-printer.alberta.ca/1266.cfm?page=p28p5.cfm&leg_type=Acts&isbncln=9780779851348&display=html>.

⁸²⁵ *Id.*, art. 21 à 24.



- (a) research and analysis;
 - (b) planning, administering, delivering, managing, monitoring or evaluating a program or service;
 - (c) one or more prescribed purposes.
- (2)** Non-personal data created under subsection (1) must be created in accordance with
- (a) generally accepted best practices, and
 - (b) the prescribed requirements, including,
 - (i) in the case of synthetic data, any prescribed requirements respecting the creation of synthetic data, and
 - (ii) in the case of another type of non-personal data identified in the regulations, any prescribed requirements respecting the creation of that type of non-personal data.
- (3)** For the purpose of creating non-personal data under subsection (1), a public body may use the following only if it is already in the custody or under the control of the public body:
- (a) personal information;
 - (b) data derived from personal information.
- (3.1)** Subsection (3) does not apply to the Office of Statistics and Information.
- (4)** Each time a public body creates non-personal data under subsection (1), the public body must maintain a record, in accordance with any prescribed requirements, of
- (a) a description of the personal information or data derived from personal information used to create the non-personal data,
 - (b) the purpose for creating the non-personal data,
 - (c) the method used for creating the non-personal data, and
 - (d) the assessment done to ensure that the identity of the individual who is the subject of the non-personal data cannot be identified or re-identified from the data.

Use of non-personal data

22 A public body may use non-personal data created under section 21(1) for any purpose.

Disclosure of non-personal data

23(1) A public body may disclose non-personal data created under section 21(1)

- (a) to another public body for any purpose, and
- (b) to a person other than a public body only if
 - (i) the disclosure is for one or more of the following purposes:
 - (A) research and analysis;
 - (B) planning, administering, delivering, managing, monitoring or evaluating a program or service;
 - (C) one or more prescribed purposes,
 - (ii) the head of the public body has approved conditions relating to the following:
 - (A) security and confidentiality;
 - (B) the prohibition of any actual or attempted re-identification of the non-personal data;
 - (C) the prohibition of any subsequent use or disclosure of the non-personal data without the express authorization of the public body;



(D) the destruction of the non-personal data at the earliest reasonable time after it has served its purpose under subclause (i), unless the public body has given the express authorization referred to in paragraph (C),

and

(iii) the person has signed an agreement to comply with the approved conditions, this Act, the regulations and any of the public body's policies and procedures relating to non-personal data.

(2) A public body may give the express authorization referred to in subsection (1)(b)(ii)(C) only if

(a) the subsequent use or disclosure is for one or more of the purposes allowed under subsection (1)(b)(i),

(b) the head of the public body approves conditions, relating to the matters described in subsection (1)(b)(ii), that apply to the subsequent use or disclosure, and

(c) there is a signed agreement, as described in subsection (1)(b)(iii), that applies to the subsequent use or disclosure.

(3) For greater certainty, nothing in this section is intended to restrict the disclosure of a report, summary or other publication containing non-personal data that is in aggregate or statistical form.

(4) This section prevails to the extent of any inconsistency or conflict with the *Access to Information Act*

Protection of non-personal data

24 The head of a public body must protect non-personal data created under section 21(1) by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclose or destruction. »



2.1.7. L'évaluation des facteurs relatifs à la vie privée

Sommaire

L'évaluation des facteurs relatifs à la vie privée (EFVP) est une démarche de réflexion axée sur la prévention et la protection de la vie privée dès le début d'un projet impliquant des renseignements personnels. Elle permet d'éviter des atteintes aux droits des personnes. La façon dont elle est intégrée aux lois québécoises devrait toutefois être améliorée pour en favoriser l'application.

Dans cette section, la Commission aborde divers enjeux liés :

- à la conceptualisation de l'EFVP dans la loi et à sa compréhension par les assujettis;
- au nombre de situations exigeant une EFVP;
- à l'absence de transparence proactive des résultats de l'EFVP pour de grands projets dans le secteur public;
- à l'absence d'un registre interne d'EFVP dans les organisations.

Elle formule diverses recommandations pour :

- mieux définir la notion d'EFVP dans les lois;
- resserrer et préciser les situations où elle est obligatoire;
- accroître la transparence de certaines EFVP dans le secteur public;
- obliger la tenue d'un registre interne des EFVP dans les organisations.

2.1.7.1. Contexte

L'EFVP est une analyse d'impact permettant aux organisations de réfléchir aux effets sur la vie privée des projets impliquant des renseignements personnels. Elle vise à éclairer la prise de décision et à éviter ou à diminuer les risques.

Pour la Commission, l'intégration de l'EFVP dans les lois générales sur la protection des renseignements personnels au Québec représente une avancée indéniable.

En tant que démarche réflexive, elle permet de structurer l'analyse des organisations, non seulement quant à la conformité légale de leurs projets, mais aussi – et surtout – quant à leur responsabilité à l'égard de la protection des droits des personnes concernées.

Pour ne donner qu'un exemple de la grande pertinence de l'EFVP, pensons à la réflexion qu'elle impose avant la communication de renseignements personnels à l'extérieur du Québec. Les mouvances dans le contexte géopolitique international amènent à prêter une attention particulière au cadre juridique en place dans les États où des renseignements personnels sont communiqués. L'EFVP permet toute la circonspection voulue pour la sélection du territoire de destination.

Le bien-fondé de l'obligation d'EFVP n'est donc plus à remettre en question. Cependant, ayant pu observer la manière dont cette démarche est comprise et réalisée au Québec, la Commission constate



qu'il y a lieu de revoir la manière dont elle est codifiée dans les lois, le tout dans un objectif de clarté, de proportionnalité des efforts et de transparence.

2.1.7.2. Situation actuelle

La notion d'EFVP a un long historique. Ses prémisses remontent aux années 1970, et elle est largement recommandée depuis les années 1990 à titre de bonne pratique⁸²⁶. Elle constitue désormais une obligation légale courante dans les lois sur la protection des renseignements personnels à travers le monde.

Au Québec, d'abord prescrite par règlement dès 2008 pour certains projets technologiques dans le secteur public⁸²⁷, elle a fait son entrée dans les lois en 2019⁸²⁸ et s'est généralisée depuis 2021 avec son intégration à la Loi sur l'accès et à la Loi sur le privé, puis à la LRSSS et à d'autres lois⁸²⁹.

Un grand nombre de dispositions dans les lois générales sur la protection des renseignements personnels concernent l'EFVP. L'obligation de la réaliser est ainsi répétée pour chaque situation particulière qui la justifie : il y en a cinq, globalement, dans les lois québécoises. Certaines sont assorties de critères que l'EFVP sert à évaluer. Le tableau suivant brosse un portrait des situations visées.

Situations imposant la réalisation d'une EFVP dans la Loi sur l'accès, la Loi sur le privé et la LRSSS

Situation imposant la réalisation d'une EFVP	Critères et modalités	Lois concernées
Projet d'acquisition, de développement ou de refonte d'un système d'information ⁸³⁰ ou de prestation électronique de services	<i>Aucun critère prévu dans la loi.</i>	Loi sur l'accès ⁸³¹ Loi sur le privé ⁸³² LRSSS ⁸³³
Projet de communication de renseignements personnels à l'extérieur du Québec	1. Les renseignements personnels doivent bénéficier d'une protection adéquate, notamment compte tenu des principes de protection des renseignements personnels généralement reconnus. L'analyse de la protection adéquate doit considérer la sensibilité et la finalité d'utilisation des renseignements personnels, les mesures de protection y compris contractuelles dont ils bénéficieraient et le régime juridique applicable dans l'État de destination.	Loi sur l'accès ⁸³⁴ Loi sur le privé ⁸³⁵ LRSSS ⁸³⁶

⁸²⁶ R. CLARKE, préc., note 614.

⁸²⁷ Règlement sur la diffusion, version de 2008, art. 7 al 2.

⁸²⁸ Loi favorisant la transformation numérique de l'administration publique, RLRQ, T-11.003, art. 9.

⁸²⁹ LGRI, art. 12.16; Loi sur l'administration fiscale, préc., note 80, art. 69.1.1, al. 1, par. a); Loi sur le ministère de l'Éducation, du Loisir et du Sport, RLRQ, c. M-15, art. 6.4.

⁸³⁰ Ceux-ci sont appelés « produits ou services technologiques » dans la LRSSS.

⁸³¹ Loi sur l'accès, art. 63.5.

⁸³² Loi sur le privé, art. 3.3.

⁸³³ LRSSS, art. 106.

⁸³⁴ Loi sur l'accès, art. 70.1.

⁸³⁵ Loi sur le privé, art. 17.

⁸³⁶ LRSSS, art. 45, 47, 48, 57, 73, 78, 81, 83 et 84.



Situation imposant la réalisation d'une EFVP	Critères et modalités	Lois concernées
Projet d'entente de communication de renseignements personnels sans consentement à des fins d'étude, de recherche ou de production de statistiques	1. Il est incontournable d'utiliser des renseignements sous une forme identificatoire. 2. Le consentement ne peut être raisonnablement obtenu. 3. L'objectif poursuivi l'emporte, en tenant compte de l'intérêt public, sur les conséquences pour le droit à la vie privée des personnes concernées. 4. La confidentialité des renseignements est assurée. Seuls les renseignements nécessaires aux fins poursuivies sont communiqués.	Loi sur l'accès ⁸³⁷ Loi sur le privé ⁸³⁸ LRSSS ⁸³⁹
Autres projets de communication de renseignements personnels sans consentement encadrés par des ententes	Les critères 1, 2, 3 et 4 ci-dessus doivent aussi être évalués.	Loi sur l'accès ⁸⁴⁰ LRSSS ⁸⁴¹
Projet d'entente de collecte de renseignements personnels par un organisme public pour le compte d'un autre	<i>Aucun critère prévu dans la loi.</i>	Loi sur l'accès ⁸⁴²

Les organismes publics, lorsqu'ils mènent des EFVP associées à des projets technologiques, doivent d'emblée consulter leur comité sur l'accès à l'information et la protection des renseignements personnels⁸⁴³ alors que les entreprises doivent consulter leur responsable de la protection des renseignements personnels⁸⁴⁴. Ceux-ci peuvent alors « suggérer des mesures de protection des renseignements personnels applicables⁸⁴⁵ » au projet étudié.

Les lois précisent que la réalisation des EFVP « doit être proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support⁸⁴⁶ ».

⁸³⁷ Loi sur l'accès, art. 67.2.1.

⁸³⁸ Loi sur le privé, art. 21.

⁸³⁹ LRSSS, art. 44 à 48, 55 et 57; bien que cette loi ait ses particularités, une lecture globale des dispositions citées et de l'article 5 laisse entrevoir la présence des mêmes critères.

⁸⁴⁰ Loi sur l'accès, art. 68.

⁸⁴¹ LRSSS, art. 79 à 82 et 84; la LRSSS ne précise pas que l'EFVP doit conclure au respect de ces critères, mais plutôt que le gestionnaire délégué aux données numériques gouvernementales doit, notamment grâce à l'EFVP du demandeur, évaluer s'ils sont respectés.

⁸⁴² Loi sur l'accès, art. 64.

⁸⁴³ *Id.*, art. 63.5.

⁸⁴⁴ Loi sur le privé, art. 3.3.

⁸⁴⁵ Loi sur l'accès, art. 63.6; Loi sur le privé, art. 3.4.

⁸⁴⁶ Loi sur l'accès, art. 63.5; Loi sur le privé, art. 3.3; LRSSS, art. 45 et 106; par le truchement des articles 57, 73, 78, 81 et 83 de la LRSSS, la mesure de proportionnalité prévue à l'article 45 s'applique dans les cas d'ententes et de communication hors Québec.



2.1.7.3. Enjeux

La Commission constate que les organisations interprètent parfois inadéquatement la notion d'EFVP, en se concentrant notamment sur leurs propres risques réputationnels ou financiers plutôt que sur les risques pour les personnes concernées. L'obligation de mener une telle évaluation tend également à être perçue comme un fardeau administratif important, entre autres en raison du nombre de situations visées. La Commission remarque aussi que les résultats des EFVP ne sont pas adéquatement valorisés. En effet, une plus grande transparence serait de mise, tant pour le public que pour des fins de surveillance de l'application des lois.

2.1.7.3.1. L'EFVP est mal conceptualisée et mal comprise

Pour faciliter la réalisation des EFVP, la Commission rend disponibles un guide d'accompagnement destiné à tout type d'organisation⁸⁴⁷ et un modèle de rapport d'EFVP⁸⁴⁸. Elle a aussi diffusé une capsule vidéo à ce sujet, à l'intention des entreprises⁸⁴⁹. Malgré ces efforts de vulgarisation, la Commission constate que l'EFVP reste mal comprise.

Cela semble dû aux contours flous de la notion d'EFVP dans les lois. La résultante est que les assujettis n'ont pas une bonne compréhension de ce qu'implique cette évaluation. Cette situation contribue à faire percevoir l'exercice de l'EFVP comme lourd et inutile, alors qu'il a le potentiel de réellement améliorer la prévention en matière de vie privée.

2.1.7.3.1.1. Les lois ne définissent pas la notion d'EFVP

Les lois québécoises ne définissent pas clairement l'EFVP. Selon un grand nombre d'autorités de vie privée à travers le monde⁸⁵⁰, l'organisme de normalisation ISO⁸⁵¹ et plusieurs experts des EFVP⁸⁵², une telle évaluation devrait s'articuler fondamentalement en trois volets :

1. L'évaluation de la **conformité légale** du projet, y compris le respect des critères particuliers lorsqu'il en existe.
2. L'évaluation des **risques** soulevés par le projet.
3. La mise en place de **stratégies pour éliminer ou atténuer ces risques**.

Pour certains experts, l'essence de l'EFVP réside dans les deux derniers volets, plus substantiels. Le premier serait de toute façon nécessaire, même sans EFVP : en tout temps, les organisations doivent

⁸⁴⁷ COMMISSION D'ACCÈS À L'INFORMATION, *Réaliser une évaluation des facteurs relatifs à la vie privée*, version 3.1, 2024, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_GU_EFVP.pdf>.

⁸⁴⁸ COMMISSION D'ACCÈS À L'INFORMATION, *Modèle de rapport d'évaluation des facteurs relatifs à la vie privée*, version 1.1, 2024, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_GAB_RAP_EFVP.docx>.

⁸⁴⁹ COMMISSION D'ACCÈS À L'INFORMATION, « Capsule 11 - L'évaluation des facteurs relatifs à la vie privée », *YouTube* (3 octobre 2024), en ligne : <<https://www.youtube.com/watch?v=X2bogxAwFzI>>.

⁸⁵⁰ Konstantina VEMOU et Maria KARYDA, *An Evaluation Framework for Privacy Impact Assessment Methods*, *Mediterranean Conference on Information Systems 2018 Proceedings*, Mediterranean Conference on Information Systems (MCIS), 2018, en ligne : <<https://core.ac.uk/download/pdf/301378875.pdf>>.

⁸⁵¹ INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, « ISO/IEC 29134:2023: Information technology — Security techniques — Guidelines for privacy impact assessment » (2023), en ligne : <<https://www.iso.org/standard/86012.html>>.

⁸⁵² David WRIGHT, « Making Privacy Impact Assessment More Effective », (2013) 29-5 *The Information Society* 307-315, DOI : 10.1080/01972243.2013.825687; Michael FRIEDEWALD, Ina SCHIERING, Nicholas MARTIN et Dara HALLINAN, « Data Protection Impact Assessments in Practice: Experiences from Case Studies », dans Sokratis KATSIKAS, Costas LAMBRINOUDAKIS, Nora CUPPENS, John MYLOPOULOS, Christos KALLONIATIS, Weizhi MENG, Steven FURNELL, Frank PALLAS, Jörg POHLE, M. Angela SASSE, Habtamu ABIE, Silvio RANISE, Luca VERDERAME, Enrico CAMBIASO, Jorge MAESTRE VIDAL et Marco Antonio SOTELO MONGE (dir.), *Computer Security. ESORICS 2021 International Workshops*, 13106, coll. Lecture Notes in Computer Science, Cham, Springer International Publishing, 2022, p. 424-443, DOI : 10.1007/978-3-030-95484-0_25.



respecter la loi. Il reste toutefois bénéfique de structurer l'évaluation de la conformité légale au sein d'un exercice plus large.

Dans tous les cas, ces volets ne sont pas mentionnés dans les lois québécoises.

Des questions se posent aussi quant à la nature des risques que l'EFVP devrait considérer. Puisque l'obligation figure dans les lois sur la protection des renseignements personnels, les risques en la matière doivent à l'évidence être pris en compte. Toutefois, le nom « évaluation des facteurs relatifs à la vie privée » fait explicitement référence à la notion de *vie privée*, ce qui pose deux difficultés.

Premièrement, qu'est-ce qu'un « facteur relatif à la vie privée »? Cette expression semble générer une confusion sur les risques à considérer. **Elle laisse croire que l'évaluation permet d'envisager tout type de facteur lié à la vie privée, y compris la protection de l'organisation elle-même contre les risques financiers, réputationnels ou juridiques qui pourraient être causés en lien avec des atteintes à la vie privée des personnes**⁸⁵³. Actuellement, ce sont ces objectifs organisationnels qui semblent animer plusieurs démarches d'EFVP. Or, la Commission et la majorité des spécialistes et des autorités de vie privée s'entendent sur le fait que l'EFVP doit porter sur les risques *pour les personnes concernées*. Les bénéfices pour les organisations sont un effet positif secondaire.

Au Québec, cette évaluation a d'abord été appelée « évaluation [...] des risques d'atteinte à la protection des renseignements personnels » dans le Règlement sur la diffusion, en 2008⁸⁵⁴. En 2019, le législateur a plutôt opté pour « évaluation des facteurs relatifs à la vie privée » lorsqu'il a intégré l'EFVP dans une loi pour la première fois⁸⁵⁵, un choix réitéré dans la Loi 25.

Cette appellation semble provenir du gouvernement fédéral canadien. L'expression anglaise *privacy impact assessment* remonte aux années 1970⁸⁵⁶. En français, dans les premiers documents traitant du concept, elle a été traduite tantôt par « analyse d'impact en matière de protection des renseignements personnels⁸⁵⁷ », tantôt par « évaluation des répercussions sur la vie privée⁸⁵⁸ », tantôt par « étude d'impact sur la vie privée⁸⁵⁹ ». L'expression ne semblait donc pas avoir de précédent lorsqu'elle a été retenue par le Secrétariat du Conseil du Trésor fédéral

⁸⁵³ M. CARBONNEAU, préc., note 569, p. 54.

⁸⁵⁴ GOUVERNEMENT DU QUÉBEC, « Décret 408-2008 du 23 avril 2008 concernant le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels », dans *Gazette officielle du Québec*, 140^e année, numéro 20, Québec, Éditeur officiel du Québec, 2008, p. 2081-2085, art. 7, al. 2, par. 2, en ligne : https://www.publicationsduquebec.gouv.qc.ca/fileadmin/gazette/pdf_encrypte/lois_reglements/2008F/49839.pdf.

⁸⁵⁵ *Loi favorisant la transformation numérique de l'administration publique*, préc., note 828, art. 9.

⁸⁵⁶ R. CLARKE, préc., note 614.

⁸⁵⁷ Rapport quinquennal 2002, sect. 2.1.3.2.

⁸⁵⁸ COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, « Les principes de protection de la vie privée et la messagerie vocale », *Internet Archive Wayback Machine [site original: Commissaire à l'information et à la protection de la vie privée de l'Ontario]* (octobre 1995), en ligne : http://web.archive.org/web/19970707112156/http://www.ipc.on.ca:80/web_site.fre/matters/sum_pap/papers/vmail-f.htm#6 (consulté le 2 septembre 2025).

⁸⁵⁹ COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « ARCHIVÉ - Rapport annuel au parlement 1999-2000 », *Internet Archive Wayback Machine [site original: Commissariat à la protection de la vie privée du Canada]* (23 mai 2013), en ligne : http://web.archive.org/web/20130523013342/http://www.priv.gc.ca/information/ar/02_04_08_f.asp (consulté le 2 septembre 2025).



en 2002⁸⁶⁰. Malgré le nom retenu, l'EFVP est assimilable à d'autres types d'analyses d'impact : elle vise à bien identifier et à minimiser les répercussions négatives d'un projet.

Deuxièmement, le droit à la vie privée comporte plusieurs facettes, outre la protection des renseignements personnels, comme le droit à l'image ou le droit à la sauvegarde de sa réputation. Ces éléments devraient vraisemblablement être pris en compte dans une EFVP. Plus largement, toutefois, la notion de vie privée suscite des débats complexes. Notamment, la perception de ce qui constitue une atteinte à la vie privée est diffuse⁸⁶¹. Diverses classifications ont été proposées⁸⁶², sans qu'aucune fasse l'unanimité. Pour surmonter l'impasse, plusieurs ont proposé de mettre l'accent sur la valeur instrumentale de la vie privée : la préservation de ce droit permet également d'en protéger d'autres, comme la liberté d'expression ou d'association, le droit à la dignité ou encore la non-discrimination⁸⁶³. Pour cette raison, la loi européenne sur la protection des renseignements personnels évoque une évaluation des risques pour « les droits et libertés » des personnes, en général⁸⁶⁴, plutôt que de cibler la seule vie privée. La Commission adhère à cette vision. En effet, le traitement de renseignements personnels peut affecter plusieurs droits et libertés des personnes concernées. En ce sens, il est pertinent que l'EFVP permette de s'y pencher, tout particulièrement lorsque l'on évalue des projets technologiques reposant sur l'IA, étant donné le large éventail d'effets potentiels de ces systèmes sur les droits des personnes.

Une EFVP qui n'est pas suffisamment centrée sur les risques pour les personnes concernées ne permet pas de prendre en compte adéquatement ce que ces dernières anticipent comme une atteinte à leur vie privée⁸⁶⁵ : « les risques et les préjudices portés à la vie privée existent surtout dans l'œil de la personne qui les subit⁸⁶⁶ ». Il s'agit pourtant là d'un élément clé permettant en partie de solutionner les difficultés associées à la délimitation des atteintes à considérer. À cet égard, la participation d'un comité représentatif des personnes concernées à la phase d'évaluation des risques de l'EFVP constitue une bonne pratique pour éviter les angles morts dans la démarche. Elle peut aussi favoriser la prise en considération des risques de nature collective ou sociale⁸⁶⁷, qui peuvent être importants dans certains projets. Particulièrement pour les grands projets gouvernementaux, cette approche semble donc porteuse afin de ne pas écarter trop vite les risques prospectifs, ou ceux impliquant des préjudices mineurs à l'échelle individuelle, mais majeurs quand on les envisage pour un groupe⁸⁶⁸.

⁸⁶⁰ SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, « Politique d'évaluation des facteurs relatifs à la vie privée », *Internet Archive Wayback Machine* [site original: Secrétariat du Conseil du trésor du Canada] (10 mai 2002), en ligne : <http://web.archive.org/web/20030210211001/http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_f.asp> (consulté le 18 septembre 2025).

⁸⁶¹ M. CARBONNEAU, préc., note 569, p. 55.

⁸⁶² Par exemple D. K. CITRON et D. J. SOLOVE, préc., note 692.

⁸⁶³ COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission des institutions de l'Assemblée nationale – Projet de loi n° 64, Loi modernisant les dispositions législatives en matière de protection des renseignements personnels*, Cat. 2.412.42.8, 2020, p. 86-89, en ligne : <https://www.cdpdj.qc.ca/storage/app/media/publications/memoire_PL64_renseignements-personnels.pdf>.

⁸⁶⁴ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119/1, art. 35(7)(c) [ci-après RGPD], en ligne : <<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:02016R0679-20160504>>.

⁸⁶⁵ M. CARBONNEAU, préc., note 569, p. 54.

⁸⁶⁶ *Id.*, p. 113.

⁸⁶⁷ Nicolas AUBIN, *Les tensions entre les principes juridiques applicables aux systèmes d'intelligence artificielle en droit québécois (explicabilité, exactitude, sécurité et équité)*, mémoire de maîtrise, Université de Montréal, 2022, p. 153 et suiv., en ligne : <<https://umontreal.scholaris.ca/items/038ee9e2-b062-4668-bd56-87fce47cb5f3>>. Voir aussi la section 2.1.1.3.9.

⁸⁶⁸ M. CARBONNEAU, préc., note 569, p. 113 et suiv.



Enfin, les critères dont l'EFVP doit démontrer le respect peuvent également générer de la confusion sur la nature de l'obligation. Comme le montre le tableau de la section 2.1.7.20, ces critères varient d'une situation à l'autre. Certaines n'en prévoient aucun. Or, ces critères constituent actuellement le seul indicateur concernant les finalités de l'EFVP. L'approche du Québec, où des exigences distinctes sont établies pour chaque situation, se distingue des standards canadien, européen et californien⁸⁶⁹. Cette variabilité fait l'objet de critiques, en particulier pour les EFVP visant des projets technologiques, pour lesquels il n'y a pas de critères⁸⁷⁰.

2.1.7.3.1.2. La responsabilité ultime de l'EFVP est imprécise

Pour les projets d'ententes, la Loi sur l'accès et la Loi sur le privé ne précisent pas laquelle des parties porte la responsabilité juridique de l'EFVP associée, ce qui crée des interprétations contradictoires.

Du point de vue de la Commission, plusieurs éléments de risques et de conformité dépendent des actions de toutes les parties. Certaines étapes de l'EFVP devraient donc être réalisées conjointement. La responsabilité ultime incombe toutefois, selon elle, à l'organisation qui détient juridiquement les renseignements personnels faisant l'objet de l'entente. Ainsi⁸⁷¹ :

- Pour les ententes de recherche et les autres ententes de communication, l'EFVP incombe à l'organisation détentrice des renseignements personnels, qui reçoit la demande de communication;
- Pour les ententes où un organisme public collecte des renseignements pour le compte d'un autre, l'EFVP devrait incomber à cet autre organisme, qui sera ultimement le détenteur juridique des renseignements.

Certains observateurs ne partagent pas cette vision. On a par exemple avancé que la responsabilité de l'EFVP, dans le cas des ententes de recherche, revenait au chercheur demandant l'accès aux renseignements personnels⁸⁷².

Cette situation peut s'expliquer par le fait que la LRSSS, elle, attribue à la partie demanderesse, c'est-à-dire au *destinataire* des renseignements personnels, la responsabilité de fournir une EFVP à l'appui de sa demande⁸⁷³. En recherche justement, l'EFVP sera donc réalisée par le chercheur ou une unité administrative de son établissement d'attache.

Toute incertitude quant à la responsabilité ultime de l'EFVP est susceptible de rendre cette évaluation moins efficace, notamment parce que la partie qui la réalise peut ne pas avoir en main toutes les informations pertinentes.

⁸⁶⁹ John BEARDWOOD, « Privacy Impact Assessment Requirements Across Jurisdictions: Just How Different are They? — A comparative analysis of privacy impact assessment legislation and associated guidance for private-sector entities across Canada, the European Union and California », (2024) 25-1 *Computer Law Review International* 6-14, p. 11, DOI : 10.9785/cr-2024-250102.

⁸⁷⁰ Serge KABLAN, Arthur OULAI et Patrick MIGNAULT, « L'évaluation des facteurs relatifs à la vie privée : pour un équilibre entre l'objectif de protection des renseignements personnels et la responsabilité des entreprises », (2023) 64-2 *Les Cahiers de droit* 397-437, p. 411 et suiv., DOI : 10.7202/1101118ar.

⁸⁷¹ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 847, p. 52, 56 et 57.

⁸⁷² Pierre-Luc DÉZIEL, « La valorisation des renseignements personnels au Québec et au Canada : la promesse des projets de loi no 64 et C-11 », (2021) 33-2 *Les Cahiers de propriété intellectuelle* 1193-1240, p. 1207, en ligne : <<https://www.lescpi.ca/articles/v33-volume-33-numero-2/la-valorisation-des-renseignements-personnels-au-quebec-et-au-canada-la-promesse-des-projets-de-loi-no-64-et-c-11/>>.

⁸⁷³ LRSSS, art. 44, al. 2, par. 2 et 81, al. 2, par. 1.



2.1.7.3.1.3. L'EFVP fait l'objet de nombreux articles de lois

Les obligations concernant l'EFVP sont réparties dans plusieurs articles de loi non contigus, soit :

- cinq articles dans la Loi sur l'accès;
- trois articles dans la Loi sur le privé;
- seize articles dans la LRSSS.

Cette codification éparse peut avoir des effets indésirables :

- Une organisation envisageant un projet peut constater qu'une situation obligeant la réalisation d'une EFVP s'applique à celui-ci et s'y arrêter. Elle risque alors de rater des critères à évaluer, car un même projet peut répondre aux conditions d'application de plusieurs obligations d'EFVP. Pensons au cas d'une entente de communication de renseignements personnels (première situation) impliquant qu'ils soient transmis à l'extérieur du Québec (deuxième situation).
- À l'inverse, une organisation peut aussi être forcée de comparer différents articles propres à différentes situations pour dégager les caractéristiques fondamentales de l'EFVP.

2.1.7.3.2. Vu ce qu'exige l'EFVP, la portée des obligations paraît large

Comme le montre la section 2.1.7.20, les lois québécoises prévoient une portée importante à l'obligation de réaliser une EFVP. En effet, celle-ci s'applique dès qu'une situation codifiée est constatée. Cette approche est parfois qualifiée de « mur à mur⁸⁷⁴ » ou de « généraliste⁸⁷⁵ » : l'EFVP s'impose dans un vaste éventail de cas et vise tous les types d'organisations, de toutes les tailles. La Commission constate d'ailleurs que les assujettis se posent beaucoup de questions concernant l'application et la portée des EFVP.

2.1.7.3.2.1. Les situations visées sont courantes

Presque chaque organisation, même petite, utilisant des technologies ou cherchant à valoriser des données peut s'attendre à devoir mener des EFVP. Plusieurs des situations associées à l'obligation d'EFVP sont courantes. Il en va ainsi de :

- la communication de renseignements personnels hors Québec, en cette ère d'infonuagique et d'échanges économiques appuyés par des flux de données transfrontaliers;
- la conclusion d'ententes entre organismes ou entre un organisme et des demandeurs tiers, comme des chercheurs, vu l'intérêt croissant pour la valorisation des données;
- l'acquisition, du développement ou de la refonte de systèmes d'information, essentiels au soutien des activités des organisations, ou de prestations électroniques de services, toujours plus communes étant donné la volonté croissante d'offrir des services aisément accessibles à distance.

De plus, les termes utilisés dans la loi sont particulièrement englobants, surtout en ce qui concerne les technologies. D'une part, une EFVP est obligatoire pour « tout projet » de système d'information ou de prestation électronique de services. D'autre part, les termes « acquisition », « développement » et « refonte » peuvent avoir une vaste portée, d'autant qu'ils ne sont pas définis. Par exemple :

- une « acquisition » peut vraisemblablement désigner tant l'achat d'un système que l'obtention d'une licence pour l'utiliser;

⁸⁷⁴ M. CARBONNEAU, préc., note 569, p. 39.

⁸⁷⁵ S. KABLAN, A. OULAÏ et P. MIGNAULT, préc., note 870, p. 407.



- un « développement » peut vraisemblablement s'entendre tant de la création d'un nouveau code informatique dans un langage de programmation que du recours à des outils d'automatisation de plus haut niveau (p. ex. un flux de travaux), et peut être réalisé par l'organisation concernée ou encore par un fournisseur externe;
- une « refonte » peut vraisemblablement consister dans le remaniement complet d'un système et de ses fonctionnalités, mais également en des travaux plus ciblés, comme la connexion à un autre système, voire le rehaussement technique de certains actifs.

Dans le même ordre d'idées, l'expression « système d'information » fait certainement référence au moins aux systèmes numériques, mais peut aussi viser les systèmes de traitement de l'information au sens large. Il suffit, pour s'en convaincre, de lire la définition du terme proposée par l'Office québécois de la langue française: « [e]nsemble structuré de ressources matérielles, logicielles et humaines qui permettent la collecte, le stockage, le traitement et la diffusion d'information⁸⁷⁶. »

Des débats subsistent quant à l'interprétation de ces termes, puisqu'ils conditionnent l'obligation de réaliser une EFVP⁸⁷⁷.

2.1.7.3.2.2. La loi ne prévoit pas de préanalyse

Si une situation évoquée dans les lois est constatée, l'EFVP est obligatoire. Ainsi, les lois québécoises ne prévoient pas de préanalyse permettant de déterminer si, dans un cas donné, cette évaluation doit être réalisée.

Ce n'est qu'une fois établi qu'une EFVP doit être réalisée qu'une notion de proportionnalité de l'analyse entre en ligne de compte. Ainsi, l'EFVP doit être proportionnée à la sensibilité, à la finalité, à la quantité, à la répartition et au support des renseignements personnels impliqués dans le projet⁸⁷⁸. Pour la Commission, cette précision ne concerne pas *l'étendue* de l'EFVP doit couvrir. Cela signifie qu'elle devrait donc toujours au moins comprendre :

- une analyse de conformité légale;
- une évaluation des risques;
- l'identification de stratégies d'atténuation de ces risques.

La proportionnalité porte plutôt sur la *profondeur* de l'EFVP. Elle peut influencer sur le nombre d'acteurs à impliquer, le temps à investir, le niveau de détail à fournir dans le rapport, la documentation annexe à élaborer et la quantité et le degré d'élaboration des mesures d'atténuation des risques à prévoir.

⁸⁷⁶ Office québécois de la langue française, « système d'information », Grand dictionnaire terminologique (2024), en ligne : <<https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8358435/systeme-dinformation>> (consulté le 16 septembre 2025).

⁸⁷⁷ S. KABLAN, A. OULAÏ et P. MIGNAULT, préc., note 870, p. 404-407.

⁸⁷⁸ Loi sur l'accès, art. 63.5; Loi sur le privé, art. 3.3; LRSSS, art. 45 et 106; par le truchement des articles 57, 73, 78, 81 et 83 de la LRSSS, la mesure de proportionnalité prévue à l'article 45 s'applique dans tous les cas d'ententes et de communication hors Québec.



2.1.7.3.2.3. L'approche généraliste peut induire un risque de banalisation

Le modèle généraliste de l'EFVP au Québec a certes des avantages :

- Il établit une certaine objectivité dans l'application de l'obligation d'EFVP, qui facilite sa compréhension⁸⁷⁹ malgré des doutes exprimés sur la terminologie⁸⁸⁰.
- Il crée un « réflexe » de la protection des renseignements personnels au sein des organisations, puisque l'exercice d'évaluation peut être courant.

Mais ce modèle a les défauts de ses qualités, surtout en raison du volume d'EFVP qu'il engendre.

L'analyse d'impact réglementaire de la réforme en protection des renseignements personnels supposait, d'une manière conservatrice, selon la Commission, que dans le secteur privé uniquement, les entreprises réaliseraient annuellement :

- a) environ 25 000 EFVP pour la communication de renseignements personnels hors Québec⁸⁸¹;
- b) environ 7 300 EFVP pour les systèmes d'information ou les prestations électroniques de services⁸⁸².

Une autre estimation arrivait plutôt à un total de près de 27 000 EFVP pour ce deuxième cas, compte tenu des termes larges utilisés pour définir cette situation⁸⁸³.

Ce volume peut créer un important fardeau financier et administratif pour les organisations⁸⁸⁴, entre autres parce que l'évaluation requiert de réunir des expertises variées. Ce poids peut être particulièrement important pour les petites organisations.

Par voie de conséquence, les organisations peuvent être incitées à faire une lecture restrictive des lois pour éviter de mener une EFVP. Elles peuvent aussi voir cette obligation comme un simple exercice bureaucratique, éloigné de la réflexion de fond que sa nature suppose⁸⁸⁵. **Par certains rapports d'EFVP qu'elle reçoit, la Commission constate déjà cette tendance à traiter l'évaluation comme une étape administrative supplémentaire dans un long processus. Certaines organisations en viennent à s'en tenir à cocher des cases dans des modèles simplifiés. Cette approche dénie l'exercice de son**

⁸⁷⁹ Ainsi, un sondage mené en 2023 auprès de grandes organisations en lien avec leur degré de préparation à la Loi 25 indiquait que près de 70 % des répondants estimaient avoir une bonne compréhension générale des obligations d'EFVP contenues dans la Loi sur le privé, tout en soulevant plusieurs incertitudes terminologiques : Antoine GUILMAIN et Caitlin SCHROPP, « Préparation à la Loi 25 : Rapport de sondage approfondi (en anglais) », *Gowling WLG* (28 août 2023), en ligne : <<https://gowlingwlg.com/fr-ca/insights-resources/reports/2023/law-25-survey-report-qc-new-privacy-legislation>> (consulté le 29 août 2025).

⁸⁸⁰ S. KABLAN, A. OULAÏ et P. MIGNAULT, préc., note 870, p. 404 et suiv.; A. GUILMAIN et C. SCHROPP, préc., note 879.

⁸⁸¹ SECRÉTARIAT À L'ACCÈS À L'INFORMATION ET À LA RÉFORME DES INSTITUTIONS DÉMOCRATIQUES, *Analyse d'impact réglementaire - Projet de loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, 2021, p. 23, en ligne : <https://cdn-contenu.quebec.ca/cdn-contenu/gouvernement/MCE/dossiers-soumis-conseil-ministres/pl64_air.pdf>.

⁸⁸² *Id.*, p. 25.

⁸⁸³ M. CARBONNEAU, préc., note 569, p. 145-147.

⁸⁸⁴ S. KABLAN, A. OULAÏ et P. MIGNAULT, préc., note 870, p. 407; voir le texte accompagnant la recommandation 6 dans : Philippe DUFRESNE, « Mémoire du Commissariat à la protection de la vie privée du Canada sur le projet de loi C-27, la Loi de 2022 sur la mise en œuvre de la Charte du numérique », *Commissariat à la protection de la vie privée du Canada* (11 mai 2023), en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/memoires-presentes-dans-le-cadre-de-consultations/sub_indu_c27_2304/> (consulté le 18 août 2025).

⁸⁸⁵ S. KABLAN, A. OULAÏ et P. MIGNAULT, préc., note 870, p. 421.



sens : une évaluation purement cosmétique ne mène à aucune amélioration significative du respect de la vie privée des personnes concernées.

2.1.7.3.3. Le public n'est pas informé proactivement des EFVP des organismes publics

Aucune disposition prévue dans les lois dont la Commission surveille l'application ne prévoit que le public soit informé proactivement⁸⁸⁶ :

- de la réalisation d'une EFVP en lien avec un projet donné;
- des résultats généraux de cette EFVP.

Si cette situation se comprend pour le secteur privé, qui n'est pas financé par la collectivité, il en va autrement pour le secteur public. La population n'est actuellement pas assurée de pouvoir connaître aisément les travaux réalisés par les organismes publics pour garantir la protection du droit à la vie privée des personnes en amont des projets. La transparence proactive à cet égard est pourtant plus importante que jamais : elle peut contribuer à améliorer la confiance des citoyens dans leurs institutions et permettre une certaine vigilance collective par rapport à des projets d'intérêt public.

Notons que pour certains projets d'envergure, le législateur a prévu une obligation de transparence envers le public. Ainsi, les organismes publics responsables de projets en ressources informationnelles d'intérêt gouvernemental menés sous le régime de la *Loi favorisant la transformation numérique de l'administration publique* doivent publier des EFVP sur leur site Web⁸⁸⁷. Ces projets demeurent rares, et cette mesure de transparence est donc peu appliquée.

2.1.7.3.4. Les organisations ne sont pas obligées de tenir un registre des EFVP

La Loi sur l'accès, la Loi sur le privé et la LRSSS ne prévoient pas la tenue d'un registre des EFVP, comme elles le font par exemple pour les incidents de confidentialité, qui doivent être consignés dans un registre accessible sur demande de la Commission⁸⁸⁸.

Or il importe qu'un régulateur doté d'un regard externe puisse vérifier occasionnellement que les EFVP ont été effectuées adéquatement. En effet, les organisations qui mènent des projets visés par l'obligation de réaliser une EFVP ont généralement une forme d'intérêt naturel à ce que l'évaluation se conclue positivement, entre autres en raison des incitatifs à la transformation numérique et à la valorisation des données⁸⁸⁹.

La transmission d'EFVP à la Commission, pour information⁸⁹⁰, est prévue pour certains projets d'envergure dans le secteur public :

- La mise en place de sources officielles de données numériques gouvernementales⁸⁹¹.
- La désignation d'un système de dépôt et de communication de renseignements en éducation⁸⁹².

⁸⁸⁶ Il reste que les rapports d'EFVP sont des documents susceptibles de faire l'objet d'une demande d'accès, et dont certaines parties pourraient être obtenues par ce moyen.

⁸⁸⁷ *Loi favorisant la transformation numérique de l'administration publique*, préc., note 828, art. 9 al. 2.

⁸⁸⁸ Loi sur l'accès, art. 63.11; Loi sur le privé, art. 3.8; LRSSS, art. 110; *Règlement sur les incidents de confidentialité*, RLRQ, c. A-2.1, r. 3.1.

⁸⁸⁹ Voir à ce sujet notamment M. CARBONNEAU, préc., note 569, p. 124-125; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 863, p. 88-89.

⁸⁹⁰ Il s'agit d'une obligation de notification, mais la Commission n'a pas à rendre d'avis ou à approuver ces évaluations. Elle peut toutefois exercer ses pouvoirs de surveillance au besoin.

⁸⁹¹ LGRI, art. 12.16 al. 1 par. 1; *Loi sur l'administration fiscale*, préc., note 80, art. 69.1.1 al. 1 par. a).

⁸⁹² *Loi sur le ministère de l'Éducation, du Loisir et du Sport*, préc., note 829, art. 6.4.



- Les projets en ressources informationnelles d'intérêt gouvernemental menés sous le régime de la *Loi favorisant la transformation numérique de l'administration publique*⁸⁹³.

Cependant, bien que ses pouvoirs lui permettent d'exiger les documents relatifs à une EFVP dans le cadre d'une démarche de surveillance, la Commission ne peut pas, actuellement, s'appuyer sur des registres comme source d'information générale sur la réalisation d'EFVP dans tout type d'organisation.

2.1.7.4. Recommandations

Malgré les qualités évidentes de l'EFVP à titre de réflexion structurée sur la protection de la vie privée, la façon dont elle est codifiée doit être améliorée de façon à :

- clarifier la notion d'EFVP, au bénéfice de la compréhension des assujettis;
- mieux cibler les cas où elle est obligatoire;
- accroître la transparence de certaines EFVP dans le secteur public;
- obliger la tenue d'un registre interne d'EFVP dans les organisations.

2.1.7.4.1. Mieux définir dans les lois la notion d'EFVP et ce qu'elle implique

La Commission entrevoit plusieurs améliorations possibles afin de mieux définir la notion d'EFVP et de mieux baliser l'évaluation des assujettis en clarifiant les attentes. Le fardeau administratif, en partie causé par l'incertitude, s'en trouverait allégé. De plus, l'EFVP risquerait moins d'être vue comme une suite de cases à cocher.

La Commission juge essentiel que les lois soient plus explicites quant à la portée et aux objectifs de l'EFVP, applicables peu importe la situation qui oblige à la réaliser. La Commission a déjà donné des orientations à cet égard, s'alignant sur les meilleures pratiques internationales⁸⁹⁴. Toutefois, ces orientations n'atteignent pas le degré d'autorité d'un texte législatif ou réglementaire. Il importe que la réalisation d'une EFVP suive toujours la même démarche.

Recommandation 44

Mieux définir l'EFVP dans les lois pour qu'il y soit explicitement indiqué que cette évaluation :

- a pour objectif fondamental la protection des personnes concernées;
- doit porter en premier lieu sur leur droit à la vie privée, mais également sur leurs autres droits et libertés susceptibles d'être affectés par le traitement de leurs renseignements personnels;
- doit toujours comporter trois volets, à savoir :
 - l'analyse de la conformité légale du projet;
 - l'évaluation des risques soulevés par le projet à l'égard du droit à la vie privée et des autres droits et libertés des personnes concernées;
 - la mise en place de mesures d'atténuation de ces risques.

⁸⁹³ *Loi favorisant la transformation numérique de l'administration publique*, préc., note 828, art. 9 al. 2.

⁸⁹⁴ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 847.



La Commission considère aussi que les projets technologiques impliquant la prise de décision automatisée concernant les personnes grâce à des systèmes d'IA devraient faire l'objet d'une réflexion plus approfondie. Une telle réflexion devrait particulièrement être menée si les décisions envisagées peuvent avoir des effets significatifs sur les personnes concernées, notamment dans des cas d'accès au logement ou au crédit ou d'évaluation d'admissibilité à des programmes gouvernementaux, ou encore dans des cas où des décisions ont des effets juridiques.

Dans de telles situations, les projets devraient faire l'objet d'une analyse d'impact algorithmique⁸⁹⁵, laquelle pourrait s'intégrer à l'EFVP. À ce sujet, le cadre mis de l'avant par le gouvernement canadien pour ses ministères et organismes⁸⁹⁶ pourrait servir de modèle.

Recommandation 45

Prévoir que l'EFVP s'accompagne d'une analyse d'impact algorithmique lorsqu'elle concerne un système d'IA visant la prise de décision automatisée concernant les personnes.

Il faut également clarifier la responsabilité ultime de l'EFVP. La Loi sur l'accès et la Loi sur le privé devraient être modifiées pour spécifier que l'obligation d'EFVP incombe à l'organisation détentrice des renseignements personnels. Des précisions seraient aussi prévues pour encadrer la collaboration des parties afin d'éviter, entre autres, que plusieurs EFVP soient réalisées indépendamment par plusieurs acteurs pour un même projet, sans qu'aucune évaluation en concerne la portée complète. C'est dans cet esprit que l'encadrement fédéral prévoit la désignation formelle d'une partie responsable dans les cas d'EFVP multi-institutionnelle⁸⁹⁷.

La LRSSS, qui prévoit déjà que la responsabilité revient aux entités demandant la communication de renseignements personnels ou l'accès à ceux-ci, devrait être harmonisée à la Loi sur l'accès et à la Loi sur le privé.

⁸⁹⁵ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, p. 22, recommandation 7; COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, p. 9, recommandation 4.

⁸⁹⁶ SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, préc., note 411.

⁸⁹⁷ SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, « Directive sur les pratiques relatives à la protection de la vie privée », *Canada.ca* (9 octobre 2024), par. C.2.2.10, en ligne : <<https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=18309>> (consulté le 11 octobre 2024).



Recommandation 46

Préciser dans la Loi sur l'accès et la Loi sur le privé quelle entité est ultimement responsable de l'EFVP lorsque plusieurs parties sont impliquées, notamment :

- en indiquant qu'il s'agit de l'organisation ayant la détention juridique des renseignements personnels concernés;
- en encadrant la collaboration des parties pour la réalisation de l'EFVP.

Recommandation 47

Harmoniser la LRSSS, la Loi sur l'accès et la Loi sur le privé en ce qui concerne l'entité ultimement responsable de l'EFVP lorsque plusieurs parties sont impliquées.

Compte tenu des précisions que recommande la Commission, il serait également opportun de regrouper toutes les dispositions traitant d'EFVP dans les différentes lois générales sur la protection des renseignements personnels. **Un tel regroupement faciliterait l'interprétation et éviterait les dédoublements que l'on constate actuellement.** Dans plusieurs autres juridictions, l'obligation d'EFVP est déjà codifiée dans un article unique et général, ou dans une section spécifique de la loi. Dans le cas de l'Alberta, les modalités sont même précisées dans un règlement⁸⁹⁸.

Recommandation 48

Regrouper les dispositions concernant l'EFVP pour en simplifier l'application et en préciser les modalités par règlement.

Enfin, la Commission préconise de déterminer certaines circonstances dans lesquelles les organismes publics seraient tenus de consulter, pour l'évaluation des risques prévue au cours d'une EFVP, un comité représentatif des personnes concernées par un projet. Il serait ainsi possible de mieux prendre en compte leur perspective concernant les atteintes à la vie privée et à d'autres droits et libertés, de manière à réduire certains angles morts qui peuvent affecter les organismes. Puisque cette étape supplémentaire demande des efforts conséquents, elle devrait uniquement être obligatoire pour certains projets. On pourrait ainsi viser les projets de grande envergure en termes financiers ou en termes de population visée, par exemple ceux qui sont désignés d'intérêt gouvernemental en vertu de la LGRI⁸⁹⁹, ou encore les projets qui

⁸⁹⁸ *Protection of Privacy (Ministerial) Regulation [Alberta]*, Alberta Regulation 143/2025, en ligne : <https://kings-printer.alberta.ca/1266.cfm?page=2025_143.cfm&leg_type=Regs&isbncln=9780779853670&display=html>.

⁸⁹⁹ LGRI, art. 16.3.



reposent sur l'utilisation de technologies encore naissantes, dont les enjeux restent à clarifier, comme les systèmes de prise de décision automatisée.

Recommandation 49

Prévoir des circonstances dans lesquelles les organismes publics sont tenus de consulter, lors de l'étape d'évaluation des risques de la démarche d'EFVP, un comité représentatif des personnes concernées par un projet et de tenir compte de sa contribution.

2.1.7.4.2. Resserrer et préciser les situations où l'EFVP est exigée

Plusieurs modifications devraient être envisagées afin de préciser davantage les situations dans lesquelles une EFVP est obligatoire et pour que cette importante démarche de réflexion structurée sur la vie privée continue d'être menée dans les cas où elle peut avoir le plus grand effet, tout en tenant compte des efforts qu'elle implique.

Bien qu'elle puisse émettre des lignes directrices permettant de faciliter l'application des lois⁹⁰⁰ et que ce pouvoir ait été utilisé par ses homologues européens, la Commission partage le point de vue de certains observateurs qui soutiennent qu'un tel instrument ne suffit pas à atteindre cet objectif de resserrement des situations dans lesquelles une EFVP est obligatoire⁹⁰¹. Des lignes directrices ne peuvent créer ni obligation ni exemption. Elles consistent principalement à préciser et à recommander de bonnes pratiques. Une intervention législative paraît nécessaire.

Il importe donc de mieux baliser la portée des situations visées, d'une part en définissant les termes utilisés, de l'autre en y intégrant, par exemple, des conditions d'application pouvant être liées à des facteurs influençant le risque, comme l'envergure du projet, le recours à de nouvelles technologies ou encore la sensibilité des renseignements concernés. L'EFVP doit demeurer obligatoire dans les cas où une réflexion de fond s'impose, comme dans le cadre de projets susceptibles d'impliquer des risques pour un grand nombre de personnes ou reposant sur des technologies nouvelles, dont les conséquences restent à cerner.

⁹⁰⁰ Loi sur l'accès, art. 123, al. 1, par. 9.

⁹⁰¹ S. KABLAN, A. OULAÏ et P. MIGNAULT, préc., note 870, p. 436.



Recommandation 50

Revoir la portée des situations dans lesquelles une EFVP est obligatoire, notamment :

- en y ajoutant des conditions d'application;
- en définissant les termes utilisés.

La Commission estime par ailleurs que pour plus de clarté et de prévisibilité, un règlement du gouvernement devrait établir :

- une liste de situations exigeant toujours une d'EFVP⁹⁰²;
- une liste de situations exemptées de l'obligation d'EFVP⁹⁰³.

De telles listes existent dans l'Union européenne. Elles sont présentées plus en détail à la section 2.1.7.5. Souples et évolutives, ces listes établies par les autorités de protection des renseignements personnels contiennent des prescriptions plus précises et particularisées que ne le peuvent les lois, habituellement plus générales et technologiquement neutres.

Par exemple, alors que les lois font référence à des « systèmes d'information », un règlement pourrait venir préciser qu'une EFVP est requise pour tout système « de gestion des ressources humaines reposant sur un profilage⁹⁰⁴ ».

Une organisation pourrait donc toujours se référer à ces listes comme première étape de son analyse. Si le type de projet qu'elle envisage se trouve dans l'une ou l'autre, elle saurait déjà si elle doit réaliser une EFVP ou non. Dans le cas contraire, elle pourrait examiner son projet à la lumière des balises générales prévues dans la loi.

Le caractère plus défini de ces listes permettrait également à la Commission d'intervenir plus facilement si elle constatait qu'un projet donné, devant faire l'objet d'une EFVP, n'a pas été adéquatement évalué. À ce chapitre, soulignons qu'il importe de prévoir dans les lois des manquements précis permettant de sanctionner les organisations ne réalisant pas d'EFVP. En ce moment, aucun manquement et aucune infraction ne concerne précisément une telle situation.

⁹⁰² RGPD, art. 34(4).

⁹⁰³ *Id.*, art. 34(5).

⁹⁰⁴ COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise*, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-requise.pdf>.



Recommandation 51

Prévoir un pouvoir réglementaire permettant au gouvernement d'établir une liste de situations :

- exigeant toujours une EFVP;
- exemptées d'EFVP.

Recommandation 52

Ajouter à la Loi sur l'accès, à la Loi sur le privé et à la LRSSS des manquements précis visant le fait de ne pas avoir réalisé une EFVP lorsqu'elle est requise.

2.1.7.4.3. Accroître la transparence de certaines EFVP dans le secteur public

Les organismes publics devraient être tenus de diffuser proactivement des résumés succincts de leurs EFVP afin de permettre au public de comprendre pourquoi les renseignements personnels sont traités au sein d'un projet donné et comment l'organisme en a assuré la protection. Cette diffusion serait également à l'avantage des organismes, car elle pourrait faire diminuer le nombre de demandes d'accès aux documents concernant les EFVP. Elle pourrait aussi permettre d'éviter certains signalements et certaines plaintes transmis à la Commission découlant de doutes quant au sérieux de l'analyse réalisée.

Cette obligation de diffusion pourrait être générale et s'appliquer à tout rapport d'EFVP et à tout organisme, ou être modulée selon certains critères. Il est clair pour la Commission que des projets dépassant un certain budget, présentant des risques élevés ou concernant une grande partie de la population devraient au minimum être visés⁹⁰⁵. Le législateur pourrait s'inspirer de diverses juridictions qui imposent la diffusion de parties de rapports d'EFVP par les organisations, en particulier dans le secteur public⁹⁰⁶. Par exemple, la directive fédérale canadienne oblige les organismes publics à publier un sommaire d'EFVP suivant un gabarit préétabli⁹⁰⁷. Le *E-Government Act* américain de 2002 exige quant à lui la publication du rapport complet dans plusieurs cas⁹⁰⁸. Certaines autorités de protection des renseignements personnels font aussi des recommandations similaires à titre de bonne pratique⁹⁰⁹.

⁹⁰⁵ La Commission note que le MCN a déjà diffusé proactivement un rapport d'EFVP concernant une partie du projet de Service québécois d'identité numérique, notamment vu l'ampleur du projet. Voir MINISTÈRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE, *Service québécois d'identité numérique - Projet 1 – Accès bonifié aux prestations électroniques de services – Citoyens. Rapport d'évaluation des facteurs relatifs à la vie privée*, 2025, en ligne : <https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/cybersecurite_numerique/Publications/RAP_EFVP_SQIN_P1.pdf>.

⁹⁰⁶ M. CARBONNEAU, préc., note 569, p. 33.

⁹⁰⁷ SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, préc., note 897, par. C.2.2.15.

⁹⁰⁸ *E-Government Act of 2002 [États-Unis]*, 116 Stat. 2899, art. 208(b)(B)(iii), en ligne : <<https://www.congress.gov/bill/107th-congress/house-bill/2458/text/pl>>.

⁹⁰⁹ OFFICE OF THE PRIVACY COMMISSIONER - NEW ZEALAND, *How to do a Privacy Impact Assessment*, 2024, p. 17, en ligne : <https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/PIA/2024-PIA-files/PIA-Toolkit-How-to-do-a-PIA_FINAL.pdf>; INFORMATION COMMISSIONER'S OFFICE, « How do we do a DPIA? » (10 juillet 2025), en ligne : <<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/>> (consulté le 25 septembre 2025).



Le fait d'exiger la diffusion d'un résumé, et non d'un rapport complet d'EFVP, permettrait de pondérer à la fois l'intérêt public de la transparence et l'intérêt de la protection de certaines informations sensibles pour l'organisation. Par exemple, les risques et les mesures d'atténuation en matière de sécurité de l'information ne devraient jamais être diffusés de manière à éviter que des vulnérabilités puissent être exploitées.

Recommandation 53

Prévoir des circonstances où les organismes publics sont tenus de diffuser proactivement un condensé de l'EFVP menée.

2.1.7.4.4. Obliger la tenue d'un registre interne des EFVP dans les organisations

La Commission préconise la tenue d'un registre des EFVP par les organisations. Cette obligation pourrait être calquée sur celle qui existe déjà pour les incidents de confidentialité : le registre de chaque organisation serait accessible par la Commission sur simple demande. Le contenu du registre pourrait être prescrit par règlement et on pourrait par exemple souhaiter qu'il contienne notamment, pour chaque EFVP :

- le nom du projet;
- une courte description du projet;
- le nombre approximatif de personnes concernées et leur qualité (citoyens, clients, etc.);
- les catégories de renseignements personnels visés;
- la date de réalisation de l'EFVP;
- la date de mise en œuvre du projet;
- la date de réévaluation prévue de l'EFVP.

Ce registre faciliterait l'exercice des fonctions de recherche et de surveillance de la Commission. En effet, en ayant accès à ces informations déjà colligées, elle pourrait plus facilement documenter la réalisation d'EFVP au Québec, mais également repérer certains projets méritant un examen approfondi.

La tenue d'un registre constituerait également un atout pour les organisations elles-mêmes. Puisque les EFVP devraient être mises à jour lors d'un changement survenant dans le contexte d'un projet ou dans ses paramètres, un registre permettrait d'assurer le suivi périodique des EFVP en un coup d'œil.

Recommandation 54

Obliger les organisations à tenir un registre interne d'EFVP, en prescrivant le contenu de ce registre dans un règlement.

2.1.7.5. Pour aller plus loin : le modèle européen des situations exigeant une EFVP

Le règlement européen prévoit la réalisation d'une analyse d'impact sur la protection des données (AIPD), l'équivalent de l'EFVP, dans l'une des situations suivantes :



1. Lorsqu'un projet est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques⁹¹⁰ », en tenant compte de la nature, de la portée, du contexte et des finalités du traitement, de même que du recours à de nouvelles technologies.
2. Lorsqu'un projet implique soit du profilage ou un traitement automatisé de renseignements personnels, soit un traitement à grande échelle de renseignements sensibles, soit la surveillance systématique d'une zone accessible au public⁹¹¹.
3. Lorsqu'un projet correspond à l'une des situations déclenchant automatiquement une obligation d'AIPD, celles-ci étant déterminées par l'autorité nationale de protection des renseignements personnels de chaque État membre et réunies dans une liste tenue par l'autorité en question⁹¹².

Les autorités nationales de protection des renseignements personnels ont également la responsabilité d'établir une liste de situations où, inversement, une AIPD n'est pas nécessaire⁹¹³.

Ce modèle hybride unit des prescriptions fixes (points 2 et 3 ci-haut) et contextuelles (point 1 ci-haut).

Les projets correspondant aux points 2 et 3 ci-haut doivent toujours faire l'objet d'une AIPD. Les listes établies par les autorités décrivent des types relativement circonscrits de projets. Par exemple, la liste de la Commission nationale de l'informatique et des libertés (France) mentionne entre autres les situations suivantes⁹¹⁴ :

- Traitements de données génétiques de personnes vulnérables.
- Traitement de gestion des ressources humaines reposant sur un profilage.
- Système de surveillance constante du personnel.
- Traitement de données de localisation à large échelle.

Les autres projets requièrent plutôt une préanalyse de risque effectuée en amont de l'AIPD, évoquée ci-haut, au point 1. Cette préanalyse fait l'objet de lignes directrices des autorités européennes de protection des renseignements personnels⁹¹⁵.

⁹¹⁰ RGPD, art. 35(1).

⁹¹¹ *Id.*, art. 35(3).

⁹¹² *Id.*, art. 34(4).

⁹¹³ *Id.*, art. 34(5).

⁹¹⁴ COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 904.

⁹¹⁵ GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679*, 17/FR WP 248 rév. 01, 2017, en ligne : https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf.



2.1.8. Les interfaces truquées

Sommaire

De plus en plus de sites Web et d'applications comportent des interfaces dites truquées, qui exploitent des biais comportementaux pour influencer, manipuler ou contraindre les personnes à poser des actions ou à faire des choix qui ne correspondent pas à leurs intérêts. De telles interfaces viennent nuire à l'autonomie de choix des personnes en matière de protection des renseignements personnels.

Dans cette section, la Commission aborde divers enjeux relatifs aux interfaces truquées, dont :

- leur efficacité, qui les rend très prévalentes – en 2024, une étude internationale à laquelle a participé la Commission a relevé la présence d'au moins une interface truquée dans 97 % des applications et des sites Web consultés;
- leur effet marqué sur la protection des renseignements personnels;
- les zones d'ombre de l'encadrement actuel en lien avec ces interfaces.

La Commission recommande au législateur québécois d'interdire explicitement ces interfaces.

2.1.8.1. Contexte

L'utilisation d'interfaces truquées sur les sites Web et les applications attire l'attention croissante des régulateurs, des chercheurs et, plus largement, de la société civile. Ce phénomène, omniprésent dans un environnement numérique lui-même de plus en plus incontournable dans le quotidien des personnes, a un effet certain sur la protection des renseignements personnels.

Dans cette section, la Commission présente différents types d'interfaces truquées et fait état de leur prévalence actuelle. Elle montre la manière dont elles peuvent nuire à la protection des renseignements personnels des personnes et invite à modifier les lois pour les interdire explicitement.

2.1.8.2. Situation actuelle

Après avoir présenté la notion d'interface truquée et des exemples permettant de l'illustrer, la Commission présente le cadre légal applicable.

2.1.8.2.1. La notion d'interface truquée

Les interfaces truquées sont souvent identifiables par les effets qu'elles engendrent plutôt que par leurs caractéristiques. En ce sens, il peut être complexe d'en donner une définition⁹¹⁶. Dans le présent rapport,

⁹¹⁶ Arunesh MATHUR, Jonathan MAYER et Mihir KSHIRSAGAR, *What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods*, *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 7 mai 2021, p. 27, p. 9, DOI : 10.1145/3411764.3445610.



le terme « interfaces truquées » réfère au résultat d'une variété de pratiques de conception des sites Web et des applications qui ont pour effet d'influencer, de manipuler ou de contraindre leurs utilisateurs à poser des actions ou à faire des choix qui, souvent, ne correspondent pas à leurs intérêts⁹¹⁷. Plus particulièrement, ces pratiques concernent l'architecture des choix offerts aux personnes, qu'il s'agisse des options qui leur sont présentées ou encore du flux d'information permettant de les orienter dans le cadre de leur prise de décision⁹¹⁸.

Au fil du temps, de nombreuses classifications des interfaces truquées ont été proposées⁹¹⁹. Pour des fins d'illustration du présent rapport, la Commission retient la classification avancée par l'Organisation de coopération et de développement économiques (OCDE)⁹²⁰, sur laquelle le Global Privacy Enforcement Network (le GPEN) a pris appui en 2024 pour documenter leur prévalence dans le cadre d'un exercice de ratissage auquel la Commission a contribué⁹²¹. On peut résumer ainsi les différents mécanismes à l'origine des interfaces truquées :

⁹¹⁷ Cette définition large reprend celles de l'OCDE et de la Commission européenne. Voir: ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *Dark commercial patterns*, DSTI/CP(2021)12/FINAL, coll. OECD Digital Economy Papers, 2022, p. 16, en ligne : <<https://read.oecd.org/10.1787/44f5e846-en?format=pdf>>; Francisco LUPIÁÑEZ-VILLANUEVA, Alba BOLUDA, Francesco BOGLIACINO, Giovanni LIVA, Lucie LECHARDY et Teresa RODRÍGUEZ DE LAS HERRAS BALLELL, *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation*, Luxembourg, Publications Office of the European Union, 2022, p. 20, en ligne : <<https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418>>.

⁹¹⁸ A. MATHUR, J. MAYER et M. KSHIRSAGAR, préc., note 916, p. 9.

⁹¹⁹ Plusieurs régulateurs et chercheurs universitaires ont proposé leurs classifications, qui relèvent à la fois de la protection des renseignements personnel et de la protection des consommateurs; voir par exemple F. LUPIÁÑEZ-VILLANUEVA et al., préc., note 917, p. 29 à 39. En particulier, les typologies et classifications suivantes s'intéressent à la protection des renseignements personnels : LABORATOIRE D'INNOVATION NUMÉRIQUE DE LA CNIL, *La forme des choix - Données personnelles, design et frictions désirables*, 06, coll. Cahiers IP, Paris, 2019, p. 28-31, en ligne : <https://linc.cnil.fr/sites/linc/files/2023-02/cnil_cahiers_ip6.pdf> (consulté le 23 octobre 2024); FORBRUKERRÅDET, *Deceived by design - How tech companies use dark patterns to discourage us from exercising our rights to privacy*, 2018, p. 12-31, en ligne : <<https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf>>; Christoph BÖSCH, Benjamin ERB, Frank KARGL, Henning KOPP et Stefan PFATTHEICHER, « Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns », (2016) 2016-4 *Proceedings on Privacy Enhancing Technologies Symposium* 237-254, p. 243-244, DOI : 10.1515/popets-2016-0038; Luiza JAROVSKY, « Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness », *SSRN Electronic Journal* 2022, p. 23-31, DOI : 10.2139/ssrn.4048582; COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Lignes directrices 03/2022 relatives aux interfaces trompeuses dans les interfaces des plateformes de médias sociaux: comment les reconnaître et les éviter?*, 2023, p. annexe 1 (p.65-71), en ligne : <https://www.edpb.europa.eu/system/files/2025-05/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_fr.pdf>; DIRECTION INTERMINISTÉRIELLE DE LA TRANSFORMATION PUBLIQUE, *Protection des données et cookies, l'éclairage des sciences comportementales*, France, 2023, p. 10, en ligne : <https://www.modernisation.gouv.fr/files/2023-06/protection%20des%20donn%C3%A9es%20personnelles%20et%20cookies_l'apport%20des%20sciences%20comportementales_0.pdf>; COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, p. annexe 1 (p.137-139).

⁹²⁰ ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, préc., note 917, p. 53, annexe B.

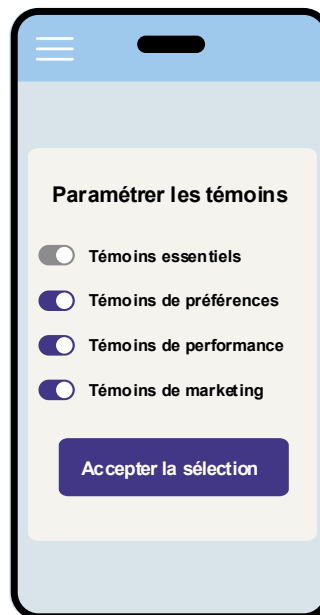
⁹²¹ GLOBAL PRIVACY ENFORCEMENT NETWORK, *Ratissage du GPEN 2024 : « Mécanismes de conception trompeuse »*, 2024, en ligne : <https://www.privacyenforcement.net/system/files/2024-07/GPEN%20Sweep%202024%20-%20%27Deceptive%20Design%20Patterns%27%20-%20FRA_0.pdf>.



- La **fausse hiérarchie**, qui se manifeste lorsque des choix ou des informations sont stratégiquement mis en valeur ou en retrait suivant l'intérêt de l'organisation.

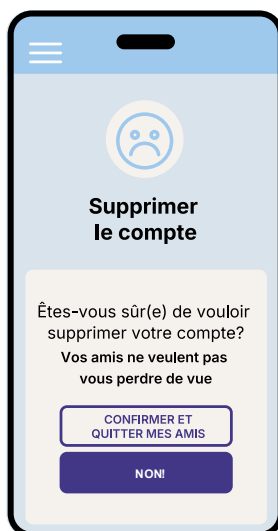


- La **présélection**, qui se manifeste lorsque les options les plus favorables aux intérêts de l'organisation sont sélectionnées par défaut. Il est alors plus rapide pour l'utilisateur de simplement accepter cette présélection.





- La **manipulation émotionnelle**, qui se manifeste lorsque des images ou des textes visent à susciter une émotion et à influencer un utilisateur au moment de faire un choix.



- Le **harcèlement**, qui se manifeste lorsque des invitations répétées et fréquentes sont adressées à l'utilisateur dans le but de le convaincre à l'usure d'accepter ce qui lui est demandé.

LUNDI



MARDI



MERCREDI





- L'**obstruction**, qui se manifeste lorsque plusieurs étapes sont introduites afin de démotiver l'utilisateur. Il y a par exemple obstruction lorsque l'architecture d'un site ou d'une application nécessite de naviguer dans une succession de sous-menus pour trouver l'option désirée ou que des étapes compliquent inutilement la procédure que l'internaute cherche à mener.



- L'**action forcée**, qui se manifeste lorsque l'utilisateur est contraint d'agir d'une certaine façon afin de bénéficier d'une fonctionnalité du site Web ou de l'application, par exemple quand on lui fait croire que cette action est indispensable.

- Le **langage complexe ou déroutant**, qui se manifeste lorsque l'information est présentée de manière à en complexifier la compréhension. Par exemple, le message principal est obscurci par l'utilisation de termes vagues, de nature juridique ou d'une longueur dissuasive. La présentation de l'information peut aussi rendre sa lecture rebutante.



Comme le montrent les exemples ci-dessus, les interfaces truquées compromettent l'autonomie des personnes dans la mesure où elles :

- entraînent une mauvaise représentation de leurs options;
- les influencent fortement à faire un choix;
- les incitent à agir impulsivement⁹²².

2.1.8.2.2. Le cadre légal

Les règles générales de la Loi sur l'accès, de la Loi sur le privé et de la LRSSS relatives aux moyens de contrôle offerts aux personnes concernées peuvent s'appliquer aux interfaces truquées, en particulier celles qui concernent :

- le consentement et ses critères de validité, de même que la transparence, présentées plus en détail à la section 2.1.1.2;
- l'obligation pour les organisations de s'assurer que les paramètres de confidentialité assurent, par défaut, le plus haut niveau de confidentialité sans intervention de la personne concernée⁹²³;

⁹²² ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, préc., note 917, p. 23-26; DIGITAL REGULATION COOPERATION FORUM, COMPETITION AND MARKETS AUTHORITY, et INFORMATION COMMISSIONER'S OFFICE, *Harmful design in digital markets: How Online Choice Architecture practices can undermine consumer choice and control over personal information*, 2023, p. 10-11, en ligne : <<https://www.drcf.org.uk/siteassets/drcf/pdf-files/harmful-design-in-digital-markets-ico-cma-joint-position-paper.pdf?v=380506>> (consulté le 25 septembre 2023).

⁹²³ Loi sur l'accès, art. 63.7; Loi sur le privé, art. 9.1; LRSSS, art. 104.



- l'obligation, pour les organisations, de s'assurer que les technologies de collecte de renseignements personnels comprenant des fonctions permettant l'identification, la localisation ou le profilage sont désactivées par défaut⁹²⁴.

Ces règles ont pour fonction d'assurer l'autonomie des personnes concernées dans leur prise de décision en matière de traitement des renseignements personnels.

2.1.8.3. Enjeux

Très efficaces, les interfaces truquées sont omniprésentes dans l'environnement numérique. Elles affectent considérablement la protection des renseignements personnels des citoyens. Selon la Commission, l'encadrement actuel ne les couvre pas assez explicitement.

2.1.8.3.1. L'efficacité des interfaces truquées les rend très prévalentes

Les interfaces truquées permettent bel et bien d'influencer les choix des personnes, ce qui les rend prévalentes dans l'environnement numérique.

L'efficacité de ces interfaces tient à deux principaux facteurs. D'une part, elles exploitent les limites de la rationalité des personnes, évoquée dans la section 2.1.1.3.1. Plusieurs études et travaux mettent en lumière des caractéristiques et des facteurs comportementaux pouvant être exploités pour introduire des biais dans la prise d'une décision⁹²⁵. Par exemple, une étude comportementale menée pour le compte de la Commission européenne a démontré que les interfaces truquées augmentent significativement l'incohérence entre les choix effectués par les personnes et leurs préférences déclarées, prouvant leur grande influence sur leur comportement⁹²⁶. D'autres recherches ont aussi démontré leur efficacité dans des contextes précis, comme les bannières de témoins de connexion⁹²⁷. Entre autres, il a été établi que les configurations qui favorisent l'acceptation des pratiques proposées par défaut et qui relèguent l'option de refus des témoins à une page secondaire font fortement baisser les taux de refus et de personnalisation. Réciproquement, la mise en évidence de l'option de refus vient doubler ce taux⁹²⁸.

D'autre part, les organisations qui ont recours aux interfaces truquées sont généralement beaucoup plus au fait de ces biais comportementaux que ne le sont les personnes qui consultent leurs sites et applications. Il s'agit là d'une forme d'asymétrie informationnelle⁹²⁹. En particulier, certaines organisations profitent de leur vaste bassin d'utilisateurs pour mener des expériences en continu visant à mesurer l'efficacité de leurs interfaces. Communément appelées « tests A/B », ces expériences reposent sur la présentation de diverses variations d'une même interface à des groupes d'internautes distincts dans le but d'identifier les configurations qui favorisent les choix profitables pour l'organisation⁹³⁰. **Les utilisateurs peuvent donc devenir des cobayes dont le comportement est analysé avec une extrême précision,**

⁹²⁴ Loi sur l'accès, art. 65.0.1; Loi sur le privé, art. 8.1; LRSSS, art. 15.

⁹²⁵ Max WITYNSKI, « Behavioral Economics, Explained », *University of Chicago News*, en ligne : <<https://news.uchicago.edu/explainer/what-is-behavioral-economics>> (consulté le 26 septembre 2025); DIRECTION INTERMINISTÉRIELLE DE LA TRANSFORMATION PUBLIQUE, préc., note 919, p. 13-14; A. ACQUISTI et al., préc., note 595, p. 5-10; L. JAROVSKY, préc., note 919, p. 13-23; LABORATOIRE D'INNOVATION NUMÉRIQUE DE LA CNIL, préc., note 919, p. 16.

⁹²⁶ F. LUPÍÁÑEZ-VILLANUEVA et al., préc., note 917, p. 104.

⁹²⁷ ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, préc., note 917, p. 21-23; F. LUPÍÁÑEZ-VILLANUEVA et al., préc., note 917, p. 92-95.

⁹²⁸ DIRECTION INTERMINISTÉRIELLE DE LA TRANSFORMATION PUBLIQUE, préc., note 919, p. 35-36.

⁹²⁹ ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, préc., note 917, p. 12.

⁹³⁰ *Id.*



et ce, à leur insu. À l'inverse, il est ardu pour les utilisateurs de saisir pleinement comment ces pratiques influencent réellement leurs décisions. Les organisations ont donc un coup d'avance.

Les études indiquent que certains groupes peuvent être davantage susceptibles de subir les effets des interfaces truquées. Ce serait le cas des personnes moins à l'aise avec les technologies ou présentant d'autres facteurs de vulnérabilité, par exemple les personnes mineures, âgées ou peu scolarisées⁹³¹. Cependant, dans la mesure où les interfaces truquées exploitent des facteurs liés à la cognition et aux comportements humains en général et reposent sur une asymétrie informationnelle, l'ensemble de la population est susceptible d'en subir l'influence. C'est d'autant plus vrai que les pratiques concernées pourraient évoluer et se raffiner, avec la possibilité d'une personnalisation des interfaces tirant profit des traits spécifiques de chacun⁹³².

Puisqu'elles sont profitables pour les organisations, les interfaces truquées sont quasi omniprésentes dans l'environnement numérique. **Une étude de 2022 indiquait que 97 % des 45 sites et 30 applications les plus populaires en Europe intégraient au moins une interface truquée⁹³³. Le même taux de prévalence a été constaté dans l'étude par ratissage menée en 2024 par le GPEN sur 1 010 sites et applications⁹³⁴.** D'autres études montrent que les organisations intègrent simultanément plusieurs interfaces truquées à leurs sites et applications⁹³⁵. Cette importante prévalence contribuerait même à entretenir la croyance de plusieurs consommateurs selon laquelle des pratiques commerciales déloyales font partie intégrante des espaces numériques⁹³⁶.

Un facteur systémique peut aussi contribuer à l'adoption répandue des interfaces truquées. Comme le souligne l'OCDE, des pressions liées à la compétitivité peuvent inciter les organisations à y recourir, en particulier lorsque leur utilisation n'est pas clairement prohibée⁹³⁷.

2.1.8.3.2. Les interfaces truquées affectent la protection des renseignements personnels

Il est clair que les modèles d'affaires basés sur la captation de l'attention sont en vogue⁹³⁸. Ils reposent sur l'accumulation et la valorisation de renseignements personnels, par exemple à des fins de publicité et de recommandations ciblées et de captation maximale de l'attention⁹³⁹.

Le recours à des interfaces truquées permet alors d'obtenir un maximum de renseignements personnels, ou de les utiliser et de les communiquer à des fins qui ne sont pas toujours vraiment souhaitées par les personnes concernées.

En conséquence, ces interfaces mettent en jeu la protection de renseignements personnels, car elles peuvent influencer plusieurs décisions en cette matière. C'est le cas lorsqu'une personne :

- doit choisir si elle veut divulguer des renseignements la concernant;
- tente de s'informer sur les pratiques d'une organisation en matière de protection des renseignements personnels;

⁹³¹ *Id.*, p. 43.

⁹³² *Id.*, p. 28; F. LUPIÁÑEZ-VILLANUEVA et al., préc., note 917, p. 91.

⁹³³ F. LUPIÁÑEZ-VILLANUEVA et al., préc., note 917, p. 97.

⁹³⁴ GLOBAL PRIVACY ENFORCEMENT NETWORK, préc., note 921.

⁹³⁵ ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, préc., note 917, p. 19.

⁹³⁶ F. LUPIÁÑEZ-VILLANUEVA et al., préc., note 917, p. 86.

⁹³⁷ ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, préc., note 917, p. 13.

⁹³⁸ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, p. 1-2.

⁹³⁹ La Commission revient sur ce modèle dans la section 2.1.9.



- configure les paramètres de confidentialité liés à l'utilisation de l'interface;
- choisit d'activer ou non des technologies de collecte permettant de l'identifier, de la localiser ou de la profiler;
- cherche à exercer ses droits, notamment d'accès ou de rectification⁹⁴⁰.

En somme, les interfaces truquées ont souvent pour effet de chercher à provoquer la collecte, l'utilisation ou la communication de plus de renseignements personnels que nécessaire ou que souhaité par les personnes concernées.

2.1.8.3.3. L'encadrement actuel contient des zones d'ombre quant aux interfaces truquées

Les règles actuelles relatives au contrôle individuel ou au paramétrage des sites ou des applications, évoquées dans la section 2.1.8.2.2, ne couvrent pas assez explicitement tous les aspects ou les effets des interfaces truquées. Les lois québécoises sur la protection des renseignements personnels ne comportent pas de disposition étoffée concernant la conception même des sites et des plateformes. Bien que certaines dispositions puissent s'appliquer, la nature dissimulée et subtile de ces interfaces peut amoindrir leur efficacité, ou en rendre le contrôle et la surveillance particulièrement ardu dans l'état actuel du droit.

Ainsi, plusieurs dispositions des lois, en matière de transparence, de consentement et de confidentialité par défaut encadrent au moins partiellement la présentation de l'information et des choix.

En matière de transparence, les lois prévoient bien que l'information présentée doit l'être en des termes simples et clairs⁹⁴¹. Les critères de validité du consentement prévoient aussi son caractère éclairé, lequel dépend de la transmission d'informations adéquates par les organisations⁹⁴². Malgré ces dispositions, l'information peut être présentée de manière à moins capter l'attention des personnes, ou à les inciter à adopter les pratiques préconisées par les organisations.

De nombreuses études ont par ailleurs montré que la fourniture d'informations à elle seule ne suffit pas à protéger les personnes de l'influence des interfaces truquées⁹⁴³. À titre d'exemple, lorsqu'elles voient que de nombreuses informations leur sont présentées, plusieurs personnes se sentent immédiatement en confiance, même si elles ne les consultent pas. Elles peuvent être portées à plus facilement « accepter » les pratiques proposées, et l'effet de la transparence peut alors être contraire à celui recherché⁹⁴⁴.

Plus largement, de nombreuses interfaces truquées peuvent enfreindre les critères de validité du consentement. Cependant, toutes les architectures de choix ne sont pas forcément perçues par les concepteurs comme des formes de consentement au sens des lois : tel peut être le cas, par exemple, de la fourniture d'une information, de l'ajustement d'un paramètre de confidentialité ou de la suppression d'un compte. Dès lors, il peut arriver que des concepteurs recourent à des interfaces qui ne permettent pas d'assurer un choix libre et éclairé des personnes concernées.

Dans un autre ordre d'idées, plusieurs interfaces truquées ont pour effet de dissuader les personnes concernées d'exercer leurs droits à l'égard de leurs renseignements personnels, comme le droit d'accès ou de rectification. Par exemple, les pages qui permettent de se prévaloir de ces droits peuvent être

⁹⁴⁰ La Commission européenne montre d'ailleurs des interactions avec des interfaces truquées tout au long du cycle de vie d'un compte ouvert sur une plateforme de réseau social sur la durée complète de son cycle de vie. COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, préc., note 919.

⁹⁴¹ Loi sur l'accès, art. 65; Loi sur le privé, art. 8; LRSSS, art. 14.

⁹⁴² COMMISSION D'ACCÈS À L'INFORMATION, préc., note 486, p. 14-17.

⁹⁴³ Voir ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, préc., note 917, p. 39-40.

⁹⁴⁴ *Id.*



enfouies dans un labyrinthe de sous-menus. Bien que les organisations doivent informer les personnes de leurs droits au moment de la collecte, les dispositions relatives aux critères de validité du consentement et aux paramètres de confidentialité ne semblent pas couvrir de manière suffisamment claire de telles interfaces, ce qui complique l'exercice des droits.

L'obligation qu'ont les organisations de faire en sorte que les paramètres de confidentialité assurent par défaut le plus haut niveau de confidentialité, sans que la personne ait à intervenir, constitue une mesure forte pour la protection des renseignements personnels. Plusieurs interfaces truquées peuvent toutefois altérer la présentation de ces paramètres afin d'inciter fortement les personnes concernées à abaisser le niveau de confidentialité par elles-mêmes. Il en va de même pour les technologies permettant d'identifier, de localiser ou de profiler les personnes. Elles doivent être désactivées par défaut, mais des interfaces truquées peuvent fortement encourager leur activation. La prévalence de telles interfaces dans les bannières de témoins de connexion atteste d'ailleurs de la popularité de cette stratégie.

2.1.8.4. Recommandations

L'impact des interfaces truquées est indéniable : elles peuvent profondément affecter le contrôle des personnes concernées à l'égard de leurs renseignements personnels. Déjà en 2022, la Commission recommandait une interdiction explicite, dans la Loi sur le privé, du recours aux interfaces truquées ayant un effet sur les jeunes⁹⁴⁵ : elle préconise désormais une approche plus large, ces interfaces ayant une incidence sur toute la population sans égard à l'âge.

La Commission note que plusieurs États ont étudié ou adopté des règles à cet effet, qui pourraient inspirer le législateur québécois. À ce titre, la section 2.1.8.5 présente un survol des mesures envisagées ou implantées au Canada, aux États-Unis et dans l'Union européenne.

Les solutions examinées comportent plusieurs traits communs dignes d'intérêt. Généralement, elles définissent les interfaces truquées d'une manière large afin d'éviter d'exclure d'emblée certains mécanismes de conception trompeuse⁹⁴⁶. Ce caractère englobant permet aussi d'anticiper l'utilisation de nouveaux types d'interfaces truquées dans le sillage de l'évolution des pratiques et des technologies. Dans la même perspective, les définitions établissent souvent un lien direct avec l'autonomie des personnes, ce qui permet de couvrir des pratiques qui, même si elles ne sont pas couvertes par les classifications actuelles des interfaces truquées, peuvent y être assimilées. **Certains avancent par exemple que de nouvelles pratiques relevant de la captologie⁹⁴⁷, comme le défilement infini ou la lecture automatique⁹⁴⁸, constituent des interfaces truquées : puisqu'elles sont addictogènes et qu'elles relèguent les personnes à la passivité, ces choix de conception nuisent à l'autonomie⁹⁴⁹.** Ils peuvent

⁹⁴⁵ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, p. 113, recommandation 10; La Commission spéciale sur les impacts des écrans et des réseaux sociaux sur la santé et le développement des jeunes a fait écho à cette recommandation dans son rapport : COMMISSION SPÉCIALE SUR LES IMPACTS DES ÉCRANS ET DES RÉSEAUX SOCIAUX SUR LA SANTÉ ET LE DÉVELOPPEMENT DES JEUNES, *Rapport final*, Assemblée nationale, 2025, p. 94, en ligne : <https://www.assnat.qc.ca/Media/Process.aspx?MediaId=ANQ.Vigie.Bil.DocumentGenerique_211813>, recommandations 41 et 49.

⁹⁴⁶ ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, préc., note 917, p. 13-16.

⁹⁴⁷ KARL PINEAU et AURELIA FABRE, « Évaluer la captologie et le design persuasif des services numériques: Approche empirique de mesure de la persuasion et proposition d'une matrice d'évaluation », (2021) 2-2 *I2D - Information, données & documents* 151-173, DOI : 10.3917/i2d.212.0151.

⁹⁴⁸ A. MATHUR, J. MAYER et M. KSHIRSAGAR, préc., note 916, p. 19.

⁹⁴⁹ *Id.*



garder les personnes actives sur les plateformes plus longtemps qu'elles ne le souhaitent, menant à une collecte accrue de renseignements personnels.

De plus, les définitions retenues ou proposées dans les lois mentionnées à la section 2.1.8.5 ne s'appuient pas, du moins pas uniquement, sur *l'intention* des concepteurs de truquer leurs interfaces, ou sur le caractère trompeur de celles-ci. On juge plus judicieux d'aborder les interfaces truquées par *l'effet* qu'elles peuvent avoir sur l'autonomie et la prise de décision. On évite ainsi des débats visant à déterminer si le problème décelé à propos d'une interface a été introduit sciemment ou s'il résulte plutôt, par exemple, de mauvais choix de conception. De même, ces définitions permettent d'éviter de se référer à l'avantage du concepteur ou au préjudice subi par les personnes, lesquels peuvent aussi être difficiles à identifier ou à démontrer.

Enfin, il n'est pas anodin de constater que plusieurs des lois ou projets de loi examinés prévoient des dispositions visant précisément à protéger les mineurs des interfaces truquées⁹⁵⁰. En effet, les conceptions addictogènes, potentiellement nuisibles au développement et au bien-être des mineurs⁹⁵¹, font partie intégrante de plusieurs plateformes et médias sociaux populaires⁹⁵² que les jeunes fréquentent. Considérant la vulnérabilité des mineurs et la nécessité d'agir dans leur intérêt supérieur⁹⁵³, une attention particulière doit être portée à ce genre d'interfaces truquées.

Recommandation 55

Interdire explicitement le recours aux interfaces truquées ayant un effet sur la protection des renseignements personnels.

Recommandation 56

Interdire explicitement le recours aux conceptions addictogènes sur les plateformes et sur les médias sociaux couramment fréquentés par des mineurs.

⁹⁵⁰ Roger WICKER, *Safe Data Act*, projet de loi n°S.4626 (17 septembre 2020), 116^e lég., 2^e sess. (Congrès des États-Unis), art. 206, en ligne : <<https://www.congress.gov/bill/116th-congress/senate-bill/4626/text>> (consulté le 9 juin 2025); *Bill Text - AB-2273 The California Age-Appropriate Design Code Act.*, projet de loi n°AB2273 (16 février 2022), 2021-22 (Législature de Californie), art. 1798.99.31 (b) (7) [CAADCA], en ligne : <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273>.

⁹⁵¹ COMMISSION SPÉCIALE SUR LES IMPACTS DES ÉCRANS ET DES RÉSEAUX SOCIAUX SUR LA SANTÉ ET LE DÉVELOPPEMENT DES JEUNES, préc., note 945, p. 58.

⁹⁵² COMMISSION D'ACCÈS À L'INFORMATION, *Mieux protéger les renseignements personnels des jeunes pour assurer leur bien-être numérique - Mémoire présenté à la Commission spéciale sur les impacts des écrans et des réseaux sociaux sur la santé et le développement des jeunes*, 2024, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_ME_PRP_Jeunes_CSESJ.pdf>.

⁹⁵³ La Commission revient plus en détail sur les enjeux touchant davantage les mineurs dans la section 2.1.9.



2.1.8.5. Pour aller plus loin : des solutions envisagées ou implantées dans d'autres États

Dans cette section, la Commission présente un aperçu de lois ou projets de loi qui ont été adoptés ou étudiés dans des juridictions comparables au Québec pour encadrer les interfaces truquées.

2.1.8.5.1. Le Canada

Au Canada, le projet de loi C-27, mort au feuillet en 2025, prévoyait l'invalidité de tout consentement obtenu par subterfuge. L'article traitait notamment de « pratiques trompeuses ou mensongères⁹⁵⁴ ».

2.1.8.5.2. Les États-Unis (au fédéral)

Aux États-Unis, plusieurs projets de loi fédéraux concernant la protection des renseignements personnels ont été présentés lors des dernières législatures. S'ils n'ont pas été adoptés, ils témoignent toutefois d'une attention claire envers l'encadrement des interfaces truquées :

- Le *Safe Data Act*, présenté au Sénat pour la seconde fois en 2023, avait notamment pour objectifs l'interdiction des pratiques trompeuses en ligne et la promotion de la transparence et du libre choix. À ce titre, il prévoyait l'interdiction des interfaces truquées, ainsi qu'une interdiction d'exposer des enfants à des interfaces addictogènes⁹⁵⁵.
- Le *American Privacy Rights Act of 2024* proposait un encadrement général de la protection des renseignements personnels au niveau fédéral. Le projet de loi prévoyait l'interdiction des interfaces truquées dans les politiques de confidentialité ainsi que dans l'exercice des droits et du consentement⁹⁵⁶.

Parmi les États, la Californie a été le premier à intégrer les interfaces truquées à sa loi sur la protection des renseignements personnels. Le *California Consumer Privacy Act* fait suivre sa définition du consentement d'une liste de pratiques qui ne sauraient constituer un consentement, dont l'obtention d'un accord par le biais d'une interface truquée⁹⁵⁷. Il convient de noter que le législateur californien a tenu à apporter ces précisions en complément des critères de validité du consentement énoncés par la loi. La Californie a entre autres été suivie par le Colorado⁹⁵⁸, le Connecticut⁹⁵⁹ et le Texas⁹⁶⁰, qui ont adopté des dispositions semblables.

De plus, le *California Age-Appropriate Design Code Act* réitère l'interdiction des interfaces truquées, notamment dans le but de prévenir que les mineurs posent des actions nuisant à leur propre bien-être⁹⁶¹.

⁹⁵⁴ François-Philippe CHAMPAGNE, *Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*, projet de loi n°C-27, 44^e lég., 1^{re} sess. (Chambre des communes du Canada), art. 16, en ligne : <<https://www.parl.ca/DocumentViewer/fr/44-1/projet-loi/C-27/premiere-lecture>>.

⁹⁵⁵ *Safe Data Act*, préc., note 950, art. 206.

⁹⁵⁶ Peter J. BENSON, Jonathan M. GAFFNEY, Chris D. LINEBAUGH, Matthew D. TROUT et Clay WILD, *American Privacy Rights Act of 2024 (draft)*, (7 avril 2024) [APRA], en ligne : <https://d1dth6e84htgma.cloudfront.net/American_Privacy_Rights_Act_of_2024_Discussion_Draft_0ec8168a66.pdf> (consulté le 18 août 2025).

⁹⁵⁷ CCPA, art. 1798.140 (l) et (h).

⁹⁵⁸ La loi du Colorado reprend en tous points celle de la Californie. Elle ne sera pas exposée ci-dessous. *Colorado Privacy Act*, préc., note 585.

⁹⁵⁹ *An Act concerning personal data privacy and online monitoring [Connecticut]*, en ligne : <<https://www.cga.ct.gov/2022/act/pa/pdf/2022PA-00015-R00SB-00006-PA.pdf>>.

⁹⁶⁰ *Texas Data Privacy and Security Act*, préc., note 586, art. 541.001(6)(C) et (10).

⁹⁶¹ *California Age-Appropriate Design Code Act*, (2022) code civil de la Californie, division 3, partie 4, titre 1.81.47, Californie, art. 1798.99.31. (b) (7), en ligne : <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273>.



2.1.8.5.3. L'Union européenne

Les interfaces truquées ne sont pas précisément mentionnées dans le RGPD. Cependant, selon certains spécialistes⁹⁶², ce règlement parvient à les encadrer efficacement par l'entremise de dispositions étoffées, notamment en matière de consentement et de protection des renseignements personnels dès la conception et par défaut, lesquels sont précisés par des lignes directrices⁹⁶³.

De plus, des pièces législatives connexes au RGPD abordent directement les interfaces truquées. C'est le cas du *Règlement sur les services numériques*, qui a pour cible principale la création d'environnements numériques plus sûrs et respectueux des droits fondamentaux des personnes. Les interfaces truquées y sont définies, et leur interdiction y est énoncée⁹⁶⁴.

Similairement, le *Règlement sur les marchés numériques*, qui encadre les pratiques des grandes plateformes en ligne, prévoit que ces plateformes ne peuvent compliquer l'exercice du choix des personnes par l'entremise des interfaces⁹⁶⁵.

Par surcroît, la Commission européenne, constatant les craintes que soulèvent les nouvelles technologies en matière de protection des choix des consommateurs, a lancé un bilan de qualité du droit européen relatif à l'équité numérique en 2022 afin de vérifier si les directives en la matière requièrent des adaptations. Dans ce cadre, une attention particulière est portée aux interfaces truquées, identifiées comme l'un des problèmes principaux et parmi les plus préjudiciables⁹⁶⁶. La Commission européenne prévoit y répondre par le *Règlement sur l'équité numérique*⁹⁶⁷, pièce législative en préparation.

⁹⁶² Ademola ADEYOKUN, « Privacy Dark Patterns: A Case for Regulatory Reform in Canada », *L'Association du Barreau canadien* (8 septembre 2022), en ligne : <<https://www.cba.org/sections/privacy-and-access/resources/privacy-dark-patterns-a-case-for-regulatory-reform-in-canada/>> (consulté le 26 juin 2025).

⁹⁶³ COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679*, 2020, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf>; COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Lignes directrices 4/2019 relatives à l'article 25 - Protection des données dès la conception et protection des données par défaut (version 2.0)*, 2020, en ligne : <https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_fr.pdf>; COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, préc., note 919.

⁹⁶⁴ *Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques)*, (2022), OJ L 2022 277, art. préambule (65) et 25, en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.277.01.0001.01.FRA&toc=OJ%3AL%3A2022%3A277%3AFULL>.

⁹⁶⁵ *Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques)*, (2022), OJ L 2022 265, art. 13 (6), en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2022.265.01.0001.01.FRA&toc=OJ:L:2022:265:FULL>.

⁹⁶⁶ COMMISSION EUROPÉENNE, « Équité numérique - bilan de qualité de la législation de l'UE en matière de protection des consommateurs » (3 octobre 2024), p. 4, en ligne : <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Equite-numerique-bilan-de-qualite-de-la-legislation-de-lUE-en-matiere-de-protection-des-consommateurs_fr> (consulté le 9 juillet 2025).

⁹⁶⁷ JAMES TAMM, « What is the Digital Fairness Act? », *Digital Fairness Act*, en ligne : <<https://digitalfairnessact.com/what-is-the-digital-fairness-act>> (consulté le 9 juillet 2025).



2.1.9. Les enjeux particuliers relatifs à la vie privée des jeunes

Sommaire

Dans les dernières années, la Commission ainsi que plusieurs de ses homologues, des États et des acteurs de la société civile se sont intéressés plus particulièrement à la protection des mineurs en ligne. Entre autres, la Commission a produit en 2022 un rapport consacré à la protection des jeunes, dont elle a repris en 2024 les principaux constats afin d'alimenter les réflexions de la Commission spéciale sur les impacts des écrans et des médias sociaux sur la santé et le développement des jeunes (CSESJ) de l'Assemblée nationale.

Dans cette section, la Commission réitère ses positions concernant la protection des mineurs. En particulier, elle revient sur :

- les caractéristiques des jeunes qui justifient une protection renforcée;
- les modèles commerciaux typiques du numérique et les risques qu'ils entraînent;
- la prise en compte, par les organisations, de la notion d'intérêt supérieur des jeunes.

2.1.9.1. Contexte

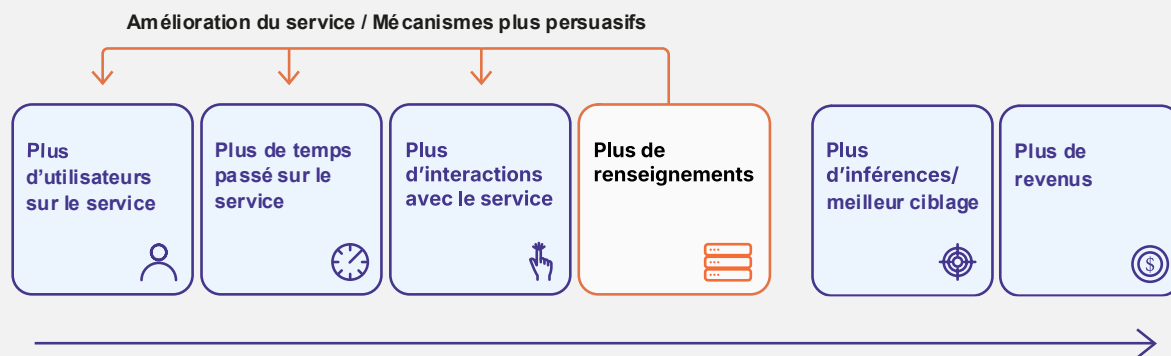
Les jeunes sont fortement attirés par les nouvelles technologies et ont une forte présence en ligne. La plus récente enquête de l'Académie de la transformation numérique de l'Université Laval sur la question le montre bien : **93 % des jeunes de 13 à 17 ans utilisent un téléphone intelligent, et 81 % d'entre eux ont au moins un compte sur les médias sociaux.** Selon leurs parents, 45 % des enfants présents sur les médias sociaux y passent plus de trois heures par jour⁹⁶⁸. Par le biais de plateformes et d'applications de tout genre, ils socialisent, s'expriment, apprennent, se divertissent et se procurent différents biens et services, entre autres choses.

La fréquentation des espaces numériques peut mener à plusieurs bienfaits pour les jeunes. Ils s'accompagnent toutefois d'un ensemble de risques et d'impacts liés à l'utilisation des technologies numériques et à la navigation dans des espaces qui ne sont pas conçus pour eux. Plusieurs de ces risques relèvent de l'exploitation de leurs renseignements personnels, qui s'inscrit au cœur du modèle économique sur lequel s'est développé l'écosystème numérique.

⁹⁶⁸ ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE, « Famille numérique (2024) » (2024), p. 5 et 19, en ligne : <<https://transformation-numerique.ulaval.ca/wp-content/uploads/2025/03/netendances24-famille-numerique.pdf>> (consulté le 13 mars 2026).

Généralement, les plateformes en ligne se financent par l'exploitation des renseignements personnels que leurs utilisateurs fournissent ou laissent dans leur sillage. Ces informations sont revalorisées par les propriétaires des plateformes de deux façons. D'une part, les plateformes sont en mesure de broser le portrait de leurs utilisateurs, de leurs préférences et de leurs caractéristiques, qu'elles peuvent revendre à d'autres organisations. De l'autre, elles donnent l'occasion aux organisations d'acheminer des publicités personnalisées aux utilisateurs. Il s'agit du modèle du capitalisme de surveillance, théorisé par la professeure Shoshana Zuboff⁹⁶⁹. Les utilisateurs jouissent de biens et de services gratuits seulement du point de vue financier : leur paiement prend la forme d'une intrusion dans leur vie privée. L'économie de l'attention, qui se caractérise par la volonté de maintenir le plus possible les utilisateurs sur les plateformes, s'est développée dans la foulée. L'accroissement du temps qu'ils y investissent se traduit par l'accumulation de données servant à l'amélioration continue des plateformes, mais aussi au déploiement d'un profilage plus efficace et à la multiplication des possibilités de ciblage publicitaire⁹⁷⁰.

Le modèle économique des plateformes peut être illustré par l'image suivante.



Dans un rapport spécial sur la protection des renseignements personnels des jeunes, paru en 2022⁹⁷¹, la Commission soulignait que la loi peinait à mettre les jeunes à l'abri de l'exploitation commerciale de leurs renseignements personnels. Le consentement parental apporté par la Loi 25, bien qu'un pas dans la bonne direction, est un ajout insuffisant dans un contexte où une grande asymétrie de pouvoir marque les relations entre les personnes et les organisations qui façonnent l'environnement numérique et où le consentement souffre de plusieurs limites, décrites à la section 2.1.1.3.

Le Québec a récemment tenu un dialogue social élargi par l'entremise des travaux de la Commission spéciale sur les impacts des écrans et des médias sociaux sur la santé et le développement des jeunes (CSESJ) de l'Assemblée nationale. Cette commission transpartisane a livré un rapport contenant de nombreuses pistes d'action en mai 2025⁹⁷². Plusieurs font écho à des préoccupations et des recommandations formulées par la Commission au cours des dernières années. Dans ce contexte, puisque les risques pour les jeunes dans le monde numérique s'accroissent, la Commission invite le

⁹⁶⁹ S. ZUBOFF, préc., note 724.

⁹⁷⁰ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 952, p. 2.

⁹⁷¹ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480.

⁹⁷² COMMISSION SPÉCIALE SUR LES IMPACTS DES ÉCRANS ET DES RÉSEAUX SOCIAUX SUR LA SANTÉ ET LE DÉVELOPPEMENT DES JEUNES, préc., note 945.



législateur à donner rapidement suite à ses recommandations et à celles de la CSESJ concernant la protection des renseignements personnels.

2.1.9.2. Situation actuelle

Les lois de protection des renseignements personnels confient la responsabilité de la protection des mineurs principalement à leurs parents ou à leurs tuteurs légaux. Ceux-ci doivent consentir à toute collecte de renseignements personnels directement auprès d'un mineur de moins de 14 ans, à moins que la collecte ne soit manifestement à son bénéfice⁹⁷³. Par ailleurs, dans les cas où les lois prévoient un consentement à l'utilisation ou à la communication de renseignements personnels, les parents ou tuteurs sont responsables de consentir au nom d'un mineur de moins de 14 ans; les mineurs de 14 à 17 ans peuvent consentir d'eux-mêmes, mais leurs parents ou tuteurs peuvent encore le faire pour eux⁹⁷⁴.

Outre ces modalités liées au consentement, les obligations des entreprises qui prennent part à l'écosystème numérique ne sont pas explicitement modulées selon l'âge des personnes concernées⁹⁷⁵. Le régime de protection des renseignements personnels se montre ainsi moins protecteur à certains égards que d'autres pièces législatives. La *Loi sur la protection du consommateur*, qui interdit sous réserve d'exception la publicité commerciale destinée à des personnes de moins de 13 ans, en est un exemple marquant⁹⁷⁶.

2.1.9.3. Enjeux

Le besoin d'une protection accrue des jeunes ne tient pas qu'à leur utilisation assidue des outils et des espaces numériques : il émane surtout de leur vulnérabilité particulière.

En effet, ils sont en processus d'appropriation graduelle de leur autonomie et de leurs pleines capacités. Cependant, les sites et les applications qu'ils fréquentent sont conçus pour s'aligner à un modèle économique susceptible de causer ou de catalyser des risques liés à la collecte, à l'utilisation ou à la communication des renseignements personnels.

2.1.9.3.1. Les jeunes sont particulièrement vulnérables

Les pratiques courantes du numérique, reliées au modèle d'affaires qui y prévaut, risquent particulièrement d'affecter les jeunes, qui sont en processus de développement de leur autonomie et de leurs capacités de raisonnement. Cela se traduit par des vulnérabilités qui doivent être prises en compte lorsqu'ils évoluent dans les mêmes milieux que les adultes.

Notamment, les jeunes ont une compréhension moins claire des pratiques de l'écosystème numérique et de l'incidence qu'elles peuvent avoir sur eux. Ils n'ont pas encore pleinement conscience de la quantité de renseignements que les organisations peuvent obtenir à leur sujet, notamment par l'observation de leur comportement en ligne et la production d'inférences, telle que décrite à la section 2.1.3, et ils sont moins à même de soupçonner l'ampleur des utilisations qui en sont faites. Les jeunes entretiennent principalement

⁹⁷³ Loi sur l'accès, art. 4.1; Loi sur le privé, art. 64.1.

⁹⁷⁴ Loi sur l'accès, art. 53.1; Loi sur le privé, art. 14; LRSSS, art. 6; dans la LRSSS, notons que le parent ou tuteur ne peut consentir que dans les cas où la Loi le prévoit.

⁹⁷⁵ Comme la collecte de renseignements personnels directement auprès d'un mineur est permise sans consentement parental dès 14 ans, de nombreuses organisations ne permettent la création de comptes qu'à partir de cet âge.

⁹⁷⁶ *Loi sur la protection du consommateur*, RLRQ, c. P-40.1, art. 248.



une vision interpersonnelle de la vie privée⁹⁷⁷ : ils comprennent bien comment ils révèlent par eux-mêmes des renseignements personnels afin de créer et de maintenir des liens sociaux. Cependant, ils sont moins alertes quant aux dimensions institutionnelles et commerciales de la collecte et de l'utilisation des renseignements personnels. Plus largement, ils éprouvent des difficultés à s'approprier des concepts centraux de l'écosystème numérique, comme la circulation des renseignements personnels, leur permanence et la pluralité d'acteurs qui peuvent y accéder et les exploiter⁹⁷⁸.

Les jeunes montrent aussi une perception moins aiguë des risques auxquels ils sont exposés en évoluant dans les milieux numériques. Ils ont tendance à se concentrer sur d'importants risques interpersonnels et immédiats, comme ceux liés au cyberharcèlement, au piratage ou à l'action d'autres acteurs malveillants⁹⁷⁹. Ils se préoccupent toutefois peu des risques à long terme relativement à la circulation de leurs renseignements personnels, et ont tendance à tenir davantage compte des bénéfices que des risques⁹⁸⁰.

L'influence de la publicité ciblée peut également être accrue pour les jeunes, d'autant plus qu'elle se fait de plus en plus intégrée et immersive⁹⁸¹. Par exemple, le marketing d'influence permet de mettre des publicités de l'avant sans que la marque soit directement impliquée, ou sans que le message publicitaire soit explicite⁹⁸². Au surplus, les mineurs sont plus facilement influencés par les interfaces truquées, décrites à la section 2.1.8, ce qui peut aussi nuire à la protection de leurs renseignements personnels.

2.1.9.3.2. L'écosystème numérique cause des risques importants pour les jeunes

Le modèle économique de l'écosystème numérique, qui carbure aux renseignements personnels, peut être la cause ou le catalyseur de nombreux risques auxquels les jeunes sont exposés⁹⁸³. La conception addictogène des plateformes, par exemple le défilement infini, les systèmes de recommandation algorithmiques et les notifications poussées, peut les inciter à y passer trop de temps ou à les consulter compulsivement. **Certaines fonctionnalités, comme le partage de la géolocalisation, peuvent aussi contribuer à la banalisation de la surveillance.**

Alors qu'ils consultent les plateformes, les mineurs peuvent être exposés à des contenus choquants, qui leur sont nuisibles ou qui ne sont pas appropriés pour leur âge. Il a d'ailleurs été avancé maintes fois que les systèmes de recommandation algorithmiques poussent les usagers des plateformes vers des types de contenus extrêmes puisqu'ils favorisent la rétention des utilisateurs⁹⁸⁴. Par exemple, un ratissage récent du GPEN auquel a participé la Commission montre que les jeunes peuvent être exposés, via les fils algorithmiques ou les sections dans lesquelles le contenu est généré par les utilisateurs, à des contenus

⁹⁷⁷ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, p. 10.

⁹⁷⁸ *Id.*, p. 28.

⁹⁷⁹ *Id.*, p. 30.

⁹⁸⁰ *Id.*

⁹⁸¹ COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, COMMISSION D'ACCÈS À L'INFORMATION, COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE LA COLOMBIE-BRITANNIQUE, et COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ALBERTA, préc., note 496, par. 133.

⁹⁸² COMMISSION SPÉCIALE SUR LES IMPACTS DES ÉCRANS ET DES RÉSEAUX SOCIAUX SUR LA SANTÉ ET LE DÉVELOPPEMENT DES JEUNES, préc., note 945, p. 97.

⁹⁸³ Dans son rapport de 2022, la Commission proposait une typologie et une cartographie de ces risques, de même que plusieurs exemples démontrant le rôle central du traitement des renseignements personnels dans leur concrétisation. Voir COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, p. 35-44.

⁹⁸⁴ Par exemple, voir OFCOM et REVEALING REALITY, *Research into risk factors that may lead children to harm online*, 2022, p. 35; et Olivia CARVILLE, « TikTok's Algorithm Keeps Pushing Suicide to Vulnerable Kids », *Bloomberg* (20 avril 2023), en ligne : <<https://www.bloomberg.com/news/features/2023-04-20/tiktok-effects-on-mental-health-in-focus-after-teen-suicide>> (consulté le 25 avril 2023).



haineux ou offensant sur 15 % des sites et applications passés en revue, à du contenu de nature sexuelle dans 11 % des cas, et à des contenus relatifs à l'automutilation ou aux troubles de l'alimentation dans 7 % des cas. L'utilisation du profilage comportemental était associée à environ 60 % des occurrences de ces deux dernières catégories⁹⁸⁵. Les jeunes peuvent aussi faire les frais de la désinformation, notamment par le truchement d'hypertrucages, ou être enfermés dans des bulles de filtre, où ils ne sont exposés qu'aux contenus pour lesquels ils ont déjà montré un intérêt. Enfin, le marketing numérique est aussi susceptible de concrétiser plusieurs risques, notamment la normalisation de certaines pratiques, comme les jeux d'argent, ou encore le vol d'identité et la fraude⁹⁸⁶.

Ces risques sont susceptibles de dépasser les bienfaits que l'ouverture aux écosystèmes numériques apporte aux jeunes. Ils peuvent nuire à leur développement normal et à l'exploration de leur identité, et les mener vers le développement d'une image corporelle négative ou vers une sexualisation précoce⁹⁸⁷. Ils ne sont pas inéluctables : ils découlent plutôt de choix faits par les entreprises qui dictent la conception de l'écosystème numérique pour répondre à leurs impératifs commerciaux.

2.1.9.4. Recommandations

La Commission est d'avis que les recommandations qu'elle a faites en 2022, notamment celles qui ont été reprises par la CSESJ, apportent des réponses nécessaires aux enjeux soulevés par la fréquentation des espaces numériques par les jeunes. Des mesures de protection supplémentaires doivent être avancées afin de protéger les jeunes de l'exploitation de leurs renseignements personnels à des fins commerciales. Un encadrement plus étroit des organisations contribuant à façonner l'environnement numérique, basé sur l'intérêt supérieur des jeunes, devrait aussi être mis en place.

2.1.9.4.1. Prioriser à nouveau la protection des jeunes

En 1978, le Québec faisait un choix de société en interdisant, dans la *Loi sur la protection du consommateur*, la publicité faite auprès des mineurs de moins de 13 ans. Il priorisait la protection de sa jeunesse de l'influence parfois néfaste de la sphère commerciale. **De l'avis de la Commission, la situation actuelle justifie un appui renouvelé à ce choix.** À cet effet, la Commission a recommandé en 2022 l'interdiction de :

- la collecte, de l'utilisation ou de la communication de renseignements personnels d'un mineur dans le but de faire de la publicité commerciale, d'influencer son comportement ou ses décisions dans un contexte commercial ou à toute autre fin présumément ou effectivement préjudiciable⁹⁸⁸;
- la vente de renseignements personnels concernant un mineur, même avec l'obtention d'un consentement⁹⁸⁹.

Pour l'essentiel, la CSESJ a repris ces recommandations⁹⁹⁰.

⁹⁸⁵ GLOBAL PRIVACY ENFORCEMENT NETWORK, *Rapport du ratissage du GPEN: La protection de la vie privée des enfants*, 2026, p. 15-16, en ligne : <<https://www.privacyenforcement.net/system/files/2026-03/GPEN%20Sweep%20Report%20-%20March%202026%20-%20FR.pdf>>.

⁹⁸⁶ COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, COMMISSION D'ACCÈS À L'INFORMATION, COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE LA COLOMBIE-BRITANNIQUE, et COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ALBERTA, préc., note 496, par. 132.

⁹⁸⁷ *Id.*

⁹⁸⁸ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, recommandation 1.

⁹⁸⁹ *Id.*, recommandation 2.

⁹⁹⁰ COMMISSION SPÉCIALE SUR LES IMPACTS DES ÉCRANS ET DES RÉSEAUX SOCIAUX SUR LA SANTÉ ET LE DÉVELOPPEMENT DES JEUNES, préc., note 945, recommandations 38 et 39.



En 2024, la Commission a aussi mis de l'avant⁹⁹¹ la possibilité d'étoffer l'encadrement de la publicité ciblée, y compris pour les mineurs de 13 à 17 ans. Elle a également proposé d'exiger des grandes entreprises du numérique qu'elles rendent publics des registres de publicités à des fins de recherche et de vérification de leur conformité à la loi, comme l'exige l'Europe depuis l'entrée en vigueur du *Règlement sur les services numériques*. La Commission croit toujours que ces avenues méritent d'être explorées.

2.1.9.4.2. Responsabiliser les organisations

Le rôle de la société quant à la protection des jeunes en ligne est clair. Les interdictions proposées par la Commission en seraient une manifestation. Cependant, il est crucial que les organisations à l'origine des produits et services numériques y participent elles aussi. La Commission reconnaît l'importance de la sensibilisation à la protection des renseignements personnels, de même que l'autonomie des personnes. Cependant, elle souligne, dans la section 2.1.1.3 du présent rapport, les limites du contrôle individuel sur les renseignements personnels ainsi que l'asymétrie de pouvoir entre les personnes et les plus grandes organisations. **Comme elles conditionnent en large part les espaces numériques, les entreprises derrière les sites et les applications doivent elles aussi prendre leurs responsabilités et prioriser la protection des jeunes.**

Cette protection doit s'articuler autour de leur intérêt supérieur. Consacré par la Convention des Nations Unies relative aux droits de l'enfant de 1989⁹⁹², ce principe veut que le bien-être et les droits des jeunes soient au cœur des décisions et des actions qui les concernent directement et indirectement⁹⁹³. Il doit ainsi guider la prise de décision lorsque les organisations ont plusieurs intérêts concurrents. En matière de protection des renseignements personnels, plusieurs mesures incombant aux organisations découlent de cet intérêt supérieur, comme la protection de la vie privée des jeunes dès la conception des produits et services et la facilitation de l'exercice de leurs droits sur leurs renseignements personnels.

Plusieurs recommandations faites par la Commission à l'occasion de son rapport de 2022 et de son mémoire de 2024 visent à intégrer le principe de l'intérêt supérieur ainsi que plusieurs responsabilités pour les entreprises à même les lois sur la protection des renseignements personnels⁹⁹⁴ :

- La mention explicite, dans ces lois, de la notion d'intérêt supérieur de l'enfant.
- La modification de la Loi sur le privé afin que les entreprises se voient imposer un devoir particulier de protection envers les mineurs, notamment par l'adaptation aux jeunes des mesures de transparence.
- L'obligation que les projets impliquant la collecte, l'utilisation ou la communication de renseignements personnels de mineurs soient évalués notamment à la lumière des répercussions potentielles sur leurs droits fondamentaux.
- Un meilleur encadrement de la conception des produits et services numériques, notamment par la mise en place de mécanismes simples pour que les mineurs ou leurs parents puissent aisément faire valoir leurs droits d'accès, de rectification, de cessation de diffusion, de désindexation et de portabilité.

⁹⁹¹ COMMISSION D'ACCÈS À L'INFORMATION, *Mieux protéger les renseignements personnels des jeunes pour assurer leur bien-être numérique*, 2024, p. 3, en ligne : <https://cai.gouv.qc.ca/uploads/pdfs/CAI_ME_PR_P_Jeunes_CSESJ.pdf>.

⁹⁹² ORGANISATION DES NATIONS UNIES, *Convention relative aux droits de l'enfant*, (1989), traité n° 27531, en ligne : <<https://www.ohchr.org/FR/ProfessionalInterest/Pages/CRC.aspx>>.

⁹⁹³ COMMISSAIRES FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX À LA PROTECTION DE LA VIE PRIVÉE ET OMBUDS RESPONSABLES DE LA PROTECTION DE LA VIE PRIVÉE, « Mettre l'intérêt supérieur des jeunes à l'avant-plan en matière de vie privée et d'accès aux renseignements personnels », *Commissariat à la protection de la vie privée du Canada* (6 octobre 2023), en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-territoires/res_231005_01/> (consulté le 12 septembre 2024).

⁹⁹⁴ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, recommandations 4, 5, 9 et 11.



En ce qui concerne cette dernière recommandation, la mise en place de codes de pratiques peut aussi être envisagée. Ces codes, adoptés ou en voie de l'être par plusieurs États⁹⁹⁵, servent à poser les jalons d'une conception de plateformes respectueuse de la vie privée des jeunes. Selon les cas, ils peuvent avoir une valeur prescriptive, quasi réglementaire. Les travaux de la CSESJ ont d'ailleurs mené à conclure que les entreprises qui gèrent des médias sociaux doivent être responsabilisées. À cet effet, elle a recommandé⁹⁹⁶ que le gouvernement détermine à quelle instance ou quel organisme devrait revenir la tâche d'élaborer des normes ou des lignes directrices à l'intention des plateformes numériques, traitant notamment de transparence et de l'impossibilité, pour les moins de 14 ans, de consentir seuls au traitement de leurs renseignements personnels. Dans le même esprit, la CSESJ a aussi recommandé que les lois applicables soient mises à jour pour que les plateformes tiennent compte de la santé mentale et physique des jeunes, notamment par l'adoption de pratiques correspondant aux principes de la vie privée dès la conception⁹⁹⁷.

⁹⁹⁵ Le Royaume-Uni fait office de figure de proue en la matière. Voir INFORMATION COMMISSIONER'S OFFICE, *Age appropriate design: A code of practice for online services*, version 2.1.36, 2022 [ci-après *Children's code*], en ligne : <<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/>>; l'Irlande et les Pays-Bas ont notamment emboîté le pas. Voir: UNIVERSITY OF LEIDEN et WAAG ORGANISATION, *Code for Children's Rights*, Ministère de l'Intérieur et des Relations du Royaume, 2021 [ci-après CVK], en ligne : <https://codevoorkinderrechten.nl/wp-content/uploads/2021/07/Code-voor-Kinderrechten-Wordversie_EN.pdf>; et DATA PROTECTION COMMISSION, *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing*, 2021, en ligne : <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf>. L'homologue fédéral de la Commission est quant à lui en cours d'élaboration de son propre code. Voir COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Protection de la vie privée et confirmation de l'âge – Consultation exploratoire » (10 juin 2024), en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultation-age/expl_gd_age/> (consulté le 13 juin 2024).

⁹⁹⁶ COMMISSION SPÉCIALE SUR LES IMPACTS DES ÉCRANS ET DES RÉSEAUX SOCIAUX SUR LA SANTÉ ET LE DÉVELOPPEMENT DES JEUNES, préc., note 945, recommandation 43.

⁹⁹⁷ *Id.*, recommandation 41.



Recommandation 57

Concrétiser les recommandations mises de l'avant par la Commission en matière de protection des jeunes dans l'environnement numérique, notamment :

- en intégrant la notion d'intérêt supérieur des jeunes dans les lois sur la protection des renseignements personnels;
- en interdisant explicitement la collecte, l'utilisation ou la communication des renseignements personnels d'un mineur dans le but de faire de la publicité commerciale, d'influencer son comportement ou ses décisions dans un contexte commercial ou à toute autre fin présumément ou effectivement préjudiciable;
- en interdisant explicitement la vente de renseignements personnels d'un mineur;
- en imposant aux organisations un devoir particulier de protection envers les mineurs;
- en exigeant que l'évaluation de projets impliquant des renseignements personnels de mineurs tienne compte des effets potentiels sur l'ensemble de leurs droits fondamentaux;
- en encadrant davantage la conception des produits et services numériques utilisés par les mineurs.

2.1.9.5. Pour aller plus loin : la vérification de l'âge

La Commission s'abstient, dans le présent rapport, de formuler des recommandations sur l'utilisation de technologies de vérification ou d'estimation de l'âge. Pour autant, elle n'ignore pas qu'elles semblent appelées à gagner de l'importance à mesure que sont adoptées des protections spécifiques aux jeunes. D'autres pays pavent la voie à ce chapitre. Par exemple, l'Australie a choisi d'instaurer une majorité numérique, si bien que les jeunes de moins de 16 ans ne peuvent plus accéder aux médias sociaux⁹⁹⁸. Au Royaume-Uni, le *Online Safety Act* exige quant à lui que les plateformes prennent des mesures afin que les jeunes ne puissent consulter des contenus illégaux ou préjudiciables⁹⁹⁹. En France, la *Loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique* a imposé aux sites pornographiques les plus fréquentés la mise en place de dispositifs de vérification de l'âge afin que les mineurs ne puissent accéder à leurs contenus¹⁰⁰⁰.

Pour que ces nouvelles mesures soient efficaces, les entreprises qui exploitent des sites et des applications doivent adopter des mécanismes robustes de vérification ou d'estimation de l'âge leur permettant de repérer les utilisateurs en deçà d'un certain âge pour les protéger plus spécifiquement, y compris en leur bloquant l'accès dans plusieurs cas.

La Commission considère qu'il peut être justifié, à certaines occasions, d'utiliser la vérification de l'âge pour éviter l'exposition des jeunes à des contenus nuisibles ainsi que la collecte et l'utilisation de leurs

⁹⁹⁸ *Online Safety Amendment (Social Media Minimum Age) Act 2024 [Australie]*, 2024, n° 127, en ligne : <https://www.legislation.gov.au/C2024A00127/latest/text>.

⁹⁹⁹ *Online Safety Act of 2023 [Royaume-Uni]*, UK Public General Acts 2023, c. 50, en ligne : <https://www.legislation.gov.uk/ukpga/2023/50>.

¹⁰⁰⁰ *Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique [France]*, en ligne : <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000049563368/>.



renseignements personnels par les organisations. Cependant, elle souhaite réitérer¹⁰⁰¹ que la vérification de l'âge n'est pas sans contrepartie, et qu'à ce titre, elle doit être employée judicieusement. D'une part, elle suppose la collecte, l'utilisation ou la communication de renseignements personnels supplémentaires, et ce, pour l'ensemble des utilisateurs d'une plateforme donnée. Certaines techniques, comme l'estimation de l'âge par analyse faciale, peuvent entraîner un traitement étendu de renseignements personnels, ou encore la collecte de renseignements personnels sensibles. Ce traitement engendre en lui-même des risques supplémentaires de préjudices à la vie privée, par exemple en cas de fuite de données¹⁰⁰². De plus, il ne peut être pertinent que si les technologies employées sont réellement fiables, et ce, pour l'ensemble de la population. Or, des expériences récentes montrent que certaines d'entre elles présentent encore des limites¹⁰⁰³.

Conséquemment, l'adoption de mesures de vérification de l'âge ne peut faire l'économie d'une réflexion préalable sur la proportionnalité des techniques compte tenu des finalités visées, ainsi que des vérifications quant à l'efficacité réelle des systèmes.

D'autre part, la Commission souhaite éviter que la vérification de l'âge ne soit utilisée par les organisations afin d'exclure simplement les jeunes de certaines plateformes, au-delà d'éventuelles prescriptions légales. Il est possible que certaines d'entre elles optent pour cette avenue dans un souci de sécurité juridique, alors qu'il serait préférable, dans plusieurs cas, que la vérification de l'âge soit utilisée pour que les jeunes puissent toujours accéder aux fonctionnalités et aux espaces adaptés à leur âge, plutôt qu'à ceux les exposant à des risques importants. Hormis les environnements numériques présentant des contenus illicites ou qui leur seraient nuisibles, l'intérêt des jeunes n'est pas d'être privés du monde numérique, mais bien d'évoluer dans des environnements où des mesures de protection proportionnelles aux capacités qu'ils ont en fonction de leur âge sont mises en place.

Cet appel à la prudence de la Commission a été entendu par la CSESJ, qui a aussi recommandé que toute imposition d'un mécanisme de vérification de l'âge soit précédée de travaux d'analyse du gouvernement¹⁰⁰⁴. Par surcroît, dans son mémoire de 2024, la Commission faisait état de la signature, par plusieurs États, d'une déclaration commune sur des principes de vérification de l'âge¹⁰⁰⁵, qu'elle juge encore pertinente à la réflexion en contexte québécois.

¹⁰⁰¹ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 952, p. 3-4.

¹⁰⁰² Par exemple, le fournisseur d'une solution de vérification de l'âge faisant affaire avec la plateforme Discord a été victime d'un incident de confidentialité impliquant les renseignements personnels de plusieurs milliers de ses utilisateurs: « Discord : un prestataire du réseau social victime d'une importante fuite de données », *Le Monde* (10 octobre 2025), en ligne : <https://www.lemonde.fr/pixels/article/2025/10/10/discord-un-prestataire-du-reseau-social-victime-d-une-importante-fuite-de-donnees_6645628_4408996.html> (consulté le 21 janvier 2026).

¹⁰⁰³ Les deux articles suivants montrent quelques exemples des lacunes des technologies et quelques conséquences qui peuvent s'en suivre. Paul TASSI, « The UK's Internet Age Verification Is Being Bypassed By Death Stranding 2, Garry's Mod », *Forbes* (31 juillet 2025), en ligne : <<https://www.forbes.com/sites/paultassi/2025/07/31/the-uks-internet-age-verification-is-being-bypassed-by-death-stranding-2-garrys-mod/>> (consulté le 21 janvier 2026); David GILBERT, « Roblox's AI-Powered Age Verification Is a Complete Mess », *Wired*, en ligne : <<https://www.wired.com/story/roblox-ai-powered-age-verification-is-a-complete-mess/>> (consulté le 21 janvier 2026).

¹⁰⁰⁴ COMMISSION SPÉCIALE SUR LES IMPACTS DES ÉCRANS ET DES RÉSEAUX SOCIAUX SUR LA SANTÉ ET LE DÉVELOPPEMENT DES JEUNES, préc., note 945, recommandation 44.

¹⁰⁰⁵ DIVERSES AUTORITÉS DE PROTECTION DE LA VIE PRIVÉE, « Déclaration commune attestant de l'adoption d'une approche internationale concertée en ce qui concerne le contrôle de l'âge », *Commissariat à la protection de la vie privée du Canada* (19 septembre 2024), en ligne : <https://www.priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2024/js-dc_20240919/> (consulté le 20 septembre 2024).



2.1.10. Les dispositions concernant la biométrie

Sommaire

L'utilisation de technologies utilisant des données biométriques, lesquelles constituent des renseignements personnels sensibles, est à la hausse. Le corpus législatif tient compte de cette réalité.

Cependant, les dispositions concernant explicitement la biométrie sont prévues dans une autre loi que les lois générales sur la protection des renseignements personnels, soulevant ainsi un enjeu de cohérence et de clarté.

Par conséquent, la Commission recommande de rapatrier ces dispositions dans la Loi sur l'accès, la Loi sur le privé et la LRSSS.

2.1.10.1. Contexte

La biométrie désigne traditionnellement l'ensemble des techniques qui permettent d'analyser une ou plusieurs caractéristiques uniques d'une personne¹⁰⁰⁶ afin de vérifier ou de confirmer son identité¹⁰⁰⁷. Le recours aux technologies utilisant des renseignements biométriques est en augmentation : de plus en plus d'organisations se dotent de ces technologies à des fins de contrôle des accès physiques ou numériques ou de gestion des ressources humaines, entre autres. Bien que cette croissance s'accélère, la Commission constatait déjà cet enjeu en 2016¹⁰⁰⁸.

L'usage accru de ce type de renseignements et la banalisation des technologies biométriques engendrent des enjeux importants pour la protection des renseignements personnels des individus. En effet, les renseignements biométriques sont permanents et distinctifs : ce sont des identifiants uniques composés d'informations intimes. Si leur confidentialité est compromise, des conséquences importantes peuvent affecter la personne concernée.

Une carte magnétique ou un mot passe peuvent être remplacés, mais une personne ne peut pas changer son visage ou ses empreintes digitales.

Par ailleurs, bien qu'on les utilise typiquement pour établir ou confirmer l'identité d'une personne, ils peuvent aussi permettre d'inférer d'autres types d'informations à propos de la personne concernée. Notamment en raison des progrès de l'**IA**, de plus en plus de systèmes visent la déduction de renseignements sur l'état de santé ou psychologique ou les caractéristiques démographiques des personnes à partir de renseignements sur leur corps ou leur comportement.

¹⁰⁰⁶ Ces caractéristiques peuvent être physiques, comportementales ou biologiques.

¹⁰⁰⁷ Pour plus de renseignements, voir le guide de la Commission sur le sujet : COMMISSION D'ACCÈS À L'INFORMATION, *Biométrie : principes à respecter et obligations légales des organisations. Guide d'accompagnement pour les organismes publics et les entreprises*, 2022, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_GU_Biometrie_Organisations.pdf>.

¹⁰⁰⁸ Rapport quinquennal 2016, p. 101-103.



« Un domaine émergent de la technologie biométrique porte sur l'estimation de certains attributs propres à une personne, par exemple son âge ou son sexe, en fonction de ses caractéristiques biométriques. On l'appelle communément la "classification biométrique". Dans ce contexte, le système biométrique extrait des caractéristiques biométriques d'un échantillon et les analyse pour prédire la valeur d'un attribut donné.

Prédire le sexe, l'âge ou le degré de fatigue d'une personne à partir d'une image faciale, établir si un ensemble d'habitudes de frappe au clavier correspond à un humain ou à un robot ou examiner une séquence d'ADN pour détecter des problèmes de santé potentiels constituent des exemples de classification biométrique.

Bien que ces utilisations de la biométrie ne visent pas nécessairement à identifier des personnes, les caractéristiques biométriques en cause peuvent quand même permettre d'identifier précisément une personne¹⁰⁰⁹. »

Le corpus législatif québécois tient compte de la nature particulière des renseignements biométriques et leur consacre des dispositions précises. Cependant, elles ne sont pas toutes intégrées aux lois générales sur la protection des renseignements personnels. Selon la Commission, il y a lieu de les y rapatrier en vue d'une meilleure cohérence.

2.1.10.2. Situation actuelle

À titre de renseignements permettant d'identifier une personne physique, les renseignements biométriques, qu'il s'agisse de caractéristiques ou de mesures biométriques « brutes » ou de représentations mathématiques qui en sont dérivées, sont des renseignements personnels¹⁰¹⁰. Les dispositions de la Loi sur l'accès et de la Loi sur le privé s'y appliquent. De manière similaire, la LRSSS peut viser les renseignements biométriques s'ils constituent des renseignements de santé et de services sociaux dans un contexte donné, par exemple s'ils concernent l'état de santé physique ou mentale d'une personne¹⁰¹¹, ou s'ils permettent son identification et sont accolés à d'autres renseignements de santé et de services sociaux¹⁰¹².

Dans la réforme apportée par la Loi 25, le législateur a précisé que les renseignements de nature biométrique revêtent un caractère sensible¹⁰¹³. Ce statut entraîne l'obligation pour les organisations :

- de mettre en place des mesures de sécurité qui tiennent compte de cette sensibilité¹⁰¹⁴;
- d'obtenir un consentement exprès pour communiquer des renseignements biométriques, sauf dans les cas prévus par les dispositions applicables¹⁰¹⁵;

¹⁰⁰⁹ COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Document d'orientation à l'intention des entreprises sur le traitement des renseignements biométriques » (11 août 2025), en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/biometrie/gd_bio_org-final/#toc4-1> (consulté le 11 avril 2026).

¹⁰¹⁰ COMMISSION D'ACCÈS À L'INFORMATION, *Les 3 Piliers Inc.*, dossier 1018507-S, 2020, par. 27 à 37, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/decisions-en-surveillance/1018507-S_decision-cai-les-3-piliers-inc-2020-02-14.pdf>.

¹⁰¹¹ LRSSS, art. 2 al. 1 par. 1.

¹⁰¹² *Id.*, art. 2 al. 2.

¹⁰¹³ Loi sur l'accès, art. 59 al. 3; Loi sur le privé, p. 12 al. 3 par. 2.

¹⁰¹⁴ Loi sur l'accès, art. 63.1, Loi sur le privé, art. 10.

¹⁰¹⁵ Loi sur l'accès, art. 59, Loi sur le privé, art. 13.



- d'obtenir un consentement exprès pour les utiliser à d'autres fins que celles pour lesquelles ils ont été recueillis, sauf dans les cas prévus par les dispositions applicables¹⁰¹⁶;
- de tenir compte de cette sensibilité lorsqu'elles réalisent une EFVP pour un projet impliquant des renseignements biométriques¹⁰¹⁷.

Depuis 2001, la *Loi concernant le cadre juridique des technologies de l'information* prévoit des dispositions particulières relatives au recours aux caractéristiques et mesures biométriques et aux banques qui les contiennent¹⁰¹⁸. Novatrices, elles contribuent à distinguer le Québec en matière de protection des renseignements personnels. La Loi 25 a renforcé ces dispositions compte tenu de la sensibilité particulière des renseignements biométriques. La LCCJTI prévoit ainsi que :

- nul ne peut exiger que la vérification ou la confirmation de l'identité d'une personne soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques¹⁰¹⁹. Pour utiliser un tel procédé, le consentement exprès de la personne concernée est donc requis. Une divulgation préalable doit aussi être faite à la Commission;
- tout autre renseignement pouvant être découvert à partir de caractéristiques ou de mesures biométriques ne peut être utilisé à quelque autre fin que ce soit et ne peut être communiqué qu'à la personne concernée, à sa demande¹⁰²⁰. Une fois la finalité justifiant la vérification ou la confirmation d'identité accomplie, les caractéristiques ou les mesures biométriques doivent être détruites¹⁰²¹;
- la création d'une base de caractéristiques ou de mesures biométriques doit être divulguée à la Commission au plus tard 60 jours avant sa mise en service¹⁰²². Cette divulgation est distincte de celle mentionnée ci-haut.

2.1.10.3. Enjeux

Selon la Commission, l'encadrement qui s'applique globalement aux renseignements biométriques actuellement atteint un niveau satisfaisant, en particulier compte tenu des modifications apportées par la Loi 25. Cependant, elle perçoit des enjeux liés au fait que les importantes mesures de protection prévues par la LCCJTI ne soient pas intégrées aux lois prévoyant le cadre général de protection des renseignements personnels.

Les protections prévues par la LCCJTI ont permis à la Commission de déceler des tendances au fil des années, par le biais de la réception de divulgations liées à la biométrie, et d'agir de manière préventive. Ainsi, plusieurs ordonnances ont été rendues par la Commission concernant des systèmes biométriques, notamment en matière d'horodatage¹⁰²³, contribuant ainsi à dégager des orientations importantes pour la protection du public.

¹⁰¹⁶ Loi sur l'accès, art. 65.1; Loi sur le privé, art. 12.

¹⁰¹⁷ Loi sur l'accès, art. 63.5 al. 4; Loi sur le privé, art. 3.3 al. 4.

¹⁰¹⁸ LCCJTI, art. 44 et 45.

¹⁰¹⁹ LCCJTI, art. 44, al. 1.

¹⁰²⁰ LCCJTI, art. 44 al. 2.

¹⁰²¹ *Id.*, art. 44 al. 3.

¹⁰²² LCCJTI, art. 45.

¹⁰²³ Voir par exemple COMMISSION D'ACCÈS À L'INFORMATION, *Marché d'alimentation Marcanio et fils Inc.*, 1013956-S, 2021, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/decisions-en-surveillance/1013956-S_decision-cai-marche-alimentation-marcanio-fils-inc-2021-01-14.pdf>; COMMISSION D'ACCÈS À L'INFORMATION, *Auberge du lac Sacacomie inc.*, 1014137-S, 2022, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/decisions-en-surveillance/1014137-S_decision-cai-auberge-lac-sacacomie-inc-2022-04-07.pdf>; la Commission a aussi émis des constats généraux sur les systèmes d'horodatage afin de souligner les problèmes les plus fréquents: COMMISSION D'ACCÈS À L'INFORMATION, *Horodateurs et pointeuses biométriques – constats*, 2023, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_DRA_Horodateurs_Biometriques.pdf>.



Ces dernières années, les dispositions de la LCCJTI ont également servi d'appui à des interventions majeures de la Commission sur des sujets d'intérêt, comme :

- la constitution par moissonnage d'une banque de visages pour alimenter un outil de reconnaissance faciale vendu aux forces de l'ordre¹⁰²⁴;
- le contrôle automatisé de la température d'employés lors de leur entrée sur leur milieu de travail en période de pandémie¹⁰²⁵;
- le contrôle d'accès à des locaux industriels pour l'application d'une norme¹⁰²⁶;
- la mise en place d'un système d'identification par reconnaissance faciale visant l'ensemble des clients, dans une chaîne de commerce d'alimentation, afin de contrer le vol à l'étalage et la fraude¹⁰²⁷.

Les dispositions de la LCCJTI sont donc fort utiles, mais le fait qu'elles figurent dans une loi distincte, moins connue, peut malencontreusement contribuer à leur méconnaissance, tant par les organisations devant les respecter que par les personnes qu'elles protègent. Leur impact peut donc se voir limité. Bien que le nombre annuel de divulgations liées à la biométrie ait augmenté ces dernières années¹⁰²⁸, notamment avec l'élargissement par la Loi 25 des situations devant en faire l'objet, la Commission reste convaincue qu'une grande quantité de systèmes ou de banques biométriques ne lui sont pas déclarés en raison de la méconnaissance de ces obligations.

2.1.10.4. Recommandation

Force est de constater que les risques associés à la biométrie se sont accrus, notamment par l'utilisation de l'IA et l'avènement de l'informatique quantique. Les dispositions de la LCCJTI concernant la biométrie conservent plus que jamais leur pertinence vu l'accroissement du recours aux technologies biométriques.

Dans ce contexte, la Commission estime qu'il est plus important que jamais que ces articles contenus à la LCCJTI soient rapatriés au sein des lois générales encadrant la protection des renseignements personnels afin qu'ils soient facilement repérables et applicables.

Recommandation 58

Intégrer les dispositions concernant la biométrie prévues aux articles 44 à 45 de la LCCJTI aux lois générales sur la protection des renseignements personnels.

¹⁰²⁴ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 729 (en appel devant la Cour du Québec; pris en délibéré, dossier n° 500-80-042393-224).

¹⁰²⁵ Commission d'accès à l'information, *Héritage Ébénisterie Architecturale inc.*, 1023688-S, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/decisions-en-surveillance/1023688-S_decision-cai-heritage-ebenisterie-architecturale-inc-2021-06-14.pdf?v=1764589565>.

¹⁰²⁶ COMMISSION D'ACCÈS À L'INFORMATION, *Imprimeries Transcontinental inc.*, 1024350-S, 2024, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/decisions-en-surveillance/1024350-S_decision-cai-societe-imprimeries-transcontinental-inc-2024-09-04.pdf>.

¹⁰²⁷ COMMISSION D'ACCÈS À L'INFORMATION, *Metro Inc.*, 1037199-S, 2025, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/decisions-en-surveillance/1037199-S_decision-cai-societe-metro-inc-2025-02-18.pdf> (contestation à la Cour du Québec reçue le 25 mars 2025, dossier n° 500-8-045996-254).

¹⁰²⁸ Il est ainsi passé de 34 en 2021-2022, avant l'entrée en vigueur de la Loi 25, à plus d'une centaine en 2023-2024 et en 2024-2025, avant de redescendre à 69 en 2025-2026, en date du 28 février 2026.



2.2. Une nouvelle approche de la protection des renseignements personnels à l'ère numérique

Sommaire

Au fil des sections précédentes du présent chapitre, la Commission a exposé de nombreux enjeux liés à l'étendue du traitement de renseignements personnels à l'ère numérique. Les lois actuelles, fondées sur les principes FIP, ne semblent plus suffisantes pour y apporter une réponse adéquate.

Dans cette section prospective, la Commission invite donc à une vaste réflexion sur l'avenir de la protection des renseignements personnels en vue de déterminer une nouvelle approche pouvant rendre les lois plus efficaces, particulièrement face à la nature collective des enjeux et aux asymétries de pouvoir. Elle propose diverses pistes afin d'alimenter cette réflexion, notamment celles :

- d'envisager des balises plus substantielles dans les lois, notamment des interdictions explicites de certaines pratiques;
- d'explorer des modèles de gouvernance collective des données;
- de s'inspirer du droit de la sécurité des produits pour mieux encadrer les technologies impliquant des renseignements personnels.

2.2.1. Contexte

Les principes FIP, évoqués dans l'introduction du présent chapitre, sont la colonne vertébrale des lois sur la protection des renseignements personnels, au Québec comme ailleurs. Ils se traduisent d'une part par une protection reposant sur le contrôle individuel, et de l'autre sur des balises procédurales surtout liées à la responsabilité et à la reddition de comptes des organisations : obligation de documenter leurs pratiques, de tenir des registres, de fournir des avis, de réaliser des évaluations...

Ces mécanismes conservent leur pertinence et leur efficacité lorsqu'il s'agit d'encadrer certaines relations des citoyens avec l'État, ou encore les relations commerciales conscientes et intentionnelles entre une personne et une organisation, dans une approche « un à un ».



À l'ère numérique, les principes FIP ne suffisent plus à la tâche. Face à l'émergence de risques liés aux pratiques commerciales nouvelles, au constat que les garanties en place ne sont pas adaptées pour les encadrer et à la prise de conscience quant à l'importante dimension collective de la protection des renseignements personnels, le Québec doit envisager de nouvelles approches susceptibles de compléter le modèle actuel.

La Commission ne propose pas l'abandon de l'encadrement fondé sur les principes FIP, qui apportent des bénéfices malgré les inadéquations soulevées. Elle estime d'ailleurs que les nombreuses recommandations formulées précédemment peuvent améliorer les lois actuelles en vue de répondre à plusieurs des enjeux évoqués jusqu'ici.

« Mais il serait mal avisé de tenter de marginaliser les principes FIP. Cela serait difficile en pratique, et leurs bénéfices sont beaucoup trop précieux. L'économie numérique mondialisée exige une certaine harmonisation des régimes de protection de la vie privée. L'industrie et la société doivent pouvoir trouver un terrain d'entente concernant les limites à poser à la collecte et à l'utilisation de données. Les principes FIP portent une vision partagée à propos des meilleures pratiques informationnelles et se sont montrés particulièrement résilients. Ce qu'il faut, c'est un peu plus d'imagination et la volonté d'admettre que les principes FIP ne sont pas le seul horizon. La réponse à tous les problèmes de vie privée ne peut pas simplement être « plus de FIP ». Il y a de l'espace, sur l'échiquier international de la réglementation en matière de vie privée, pour considérer les règles liées à la concurrence, à la non-discrimination et au design des technologies de l'information. Reconnaître que les principes FIP sont une partie essentielle, mais non la totalité, des régimes de protection de la vie privée constitue la seule voie vers un futur soutenable pour la vie privée. Les FIP sont morts, vive les FIP¹⁰²⁹. »

C'est plutôt à une réflexion étendue qu'invite la Commission, dans le but de trouver de nouvelles façons de gouverner collectivement l'acceptable et l'inacceptable en matière de traitement des renseignements personnels à l'ère numérique.

L'un des objectifs importants à atteindre devrait être d'empêcher quelque acteur que ce soit, privé ou public, de jouir d'un trop grand pouvoir informationnel¹⁰³⁰. En effet, les enjeux de pouvoir ne sont pas réellement considérés au sein des lois actuelles.

« Dit autrement, les lois sur la protection des renseignements personnels ignorent les dynamiques de pouvoir propres à certaines relations, traitant votre relation avec Google comme celle que vous avez avec votre épicier. [...] Vous êtes significativement plus vulnérable face à Google ou à toute autre plateforme technologique que face à votre épicier¹⁰³¹. »

De même, un éventuel changement de paradigme devrait aussi être à l'avantage des organisations qui s'appuient sur des renseignements personnels pour mener leurs activités et innover. Des règles plus claires et substantielles bénéficieraient ainsi à tous et permettraient d'éviter que les organisations ayant le plus à cœur la vie privée soient désavantagées compétitivement par l'investissement de grands efforts pour respecter des balises procédurales n'offrant pas toujours la protection voulue.

¹⁰²⁹ W. HARTZOG, préc., note 466, p. 983, notre traduction.

¹⁰³⁰ J. MACLURE et S. AUCLAIR, préc., note 641, p. 13.

¹⁰³¹ N. M. RICHARDS et W. HARTZOG, préc., note 475, notre traduction.



2.2.2. Appel à une réflexion collective

Comment envisager une nouvelle approche de la protection des renseignements personnels? Les intérêts à pondérer sont nombreux, les enjeux sont complexes et parfois techniques, les questions sont d'importance capitale sur le plan tant économique que social. Les mouvances dans le contexte géopolitique et technologique justifient une réflexion large et approfondie.

La Commission Paré, à l'origine de la Loi sur l'accès, avait été mise sur pied pour établir les grandes orientations de l'action gouvernementale en matière d'accès à l'information et de protection des renseignements personnels. Ayant ultimement abouti à une proposition de texte législatif, elle avait pu examiner plus de 130 mémoires et tenir diverses rencontres permettant d'enrichir sa réflexion. De tels travaux s'imposaient vu le caractère novateur de la législation à développer et la diversité des intérêts à considérer.

Pour la Commission, il y a lieu aujourd'hui de suivre la même voie, en élargissant même davantage l'éventail des perspectives prises en compte. **C'est à travers un vaste dialogue public sur la protection des renseignements personnels à l'ère numérique que les solutions d'avenir peuvent être créées.** En parallèle, plus que jamais, le Québec doit continuer à être à l'affût des discussions menées ailleurs dans le monde et poursuivre ses efforts de coopération nationale et internationale, alors que tous sont confrontés aux mêmes enjeux. Aucun État ou regroupement d'États dans le monde n'a encore tracé seul le chemin d'une nouvelle philosophie de la protection des renseignements personnels, et le Québec contribue donc au mouvement international de réflexion à cet égard.

Recommandation 59

Organiser un vaste dialogue public sur le futur de la protection des renseignements personnels à l'ère numérique en impliquant des acteurs de tous horizons, par exemple par le biais d'une commission spéciale, en vue de parvenir à une nouvelle approche permettant de compléter le modèle actuel.

Recommandation 60

Poursuivre les initiatives de coopération nationale et internationale sur les questions liées au numérique et à la protection des renseignements personnels.

2.2.3. Pistes pour alimenter la réflexion

Pour alimenter le brassage d'idées collectif qu'elle recommande, sans prétendre détenir toutes les solutions, la Commission propose quelques pistes de réflexion.



2.2.3.1. Envisager des balises plus substantielles

La réflexion devrait permettre d'aller au-delà des balises procédurales sur la protection des renseignements personnels, en vue d'adopter des dispositions plus substantielles, c'est-à-dire qui concernent les usages. **Il s'agirait d'établir plus nettement, dans les lois et les règlements, ce qui est acceptable ou non en matière de traitement des renseignements personnels, et quels renseignements peuvent être traités à ces fins**¹⁰³².

Cette approche substantielle devrait au moins concerner les cas les plus problématiques, c'est-à-dire les utilisations les plus clairement préjudiciables¹⁰³³. Un grand nombre de spécialistes en matière de vie privée, d'ici et d'ailleurs, militent en ce sens¹⁰³⁴. La Commission et ses homologues canadiens ont déjà incité leurs gouvernements respectifs à agir de cette façon, en évoquant la notion de « zones interdites »¹⁰³⁵.

Il s'agit là d'une posture normative qui serait plus engagée, mais aussi plus claire. Elle aurait notamment pour avantages de :

- **produire des effets collectifs**, sans que la propension individuelle des personnes à accepter ou à tolérer certaines pratiques affecte des groupes ou l'ensemble de la population;
- **permettre à toutes les organisations de savoir à quoi s'en tenir**, sans que la volonté des unes et des autres d'adopter des pratiques plus intrusives mène à des avantages indus, en plus des préjudices de vie privée causés.

L'approche substantielle repose sur un débat public plus riche, qui peut intégrer bien plus de perspectives que ne le peut une organisation individuelle dans une réflexion sur une pratique.

« Ultimement, la responsabilité de tenir compte des risques et des préjudices portés à la vie privée devrait peut-être moins reposer sur les organisations que sur une discussion tenue par la société dans son ensemble. Une prise en charge véritable des risques et des préjudices portés à la vie privée repose sans doute moins sur l'évaluation à la pièce de chaque projet individuel que sur une réflexion globale et collective concernant la place du numérique dans nos existences¹⁰³⁶. »

¹⁰³² P.-L. DÉZIEL, préc., note 607 à la page 5.

¹⁰³³ D. J. SOLOVE, préc., note 514, p. 1903.

¹⁰³⁴ P.-L. DÉZIEL, préc., note 568, p. 847; P.-L. DÉZIEL, préc., note 607, sect. 3; J. MACLURE et S. AUCLAIR, préc., note 566, p. 40; M. CARBONNEAU, préc., note 569, p. 157; I. COFONE, préc., note 474, p. 89 et 104; Omer TENE et Jules POLONETSKY, « Privacy in the Age of Big Data: A Time for Big Decisions », (2012) 64 *Stanford Law Review* 63-69, p. 68, en ligne : <<https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data/>>; D. J. SOLOVE, préc., note 514, p. 1902-1903; S. BAROCAS et H. NISSENBAUM, préc., note 479 aux pages 66-67; W. HARTZOG, préc., note 466, p. 978; N. M. RICHARDS et W. HARTZOG, préc., note 475, p. 4-5; D. J. SOLOVE et W. HARTZOG, préc., note 551, p. 1039-1041.

¹⁰³⁵ COMMISSAIRES FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX À LA PROTECTION DE LA VIE PRIVÉE ET DES OMBUDSMANS RESPONSABLES DE LA PROTECTION DE LA VIE PRIVÉE, « Principes pour des technologies de l'intelligence artificielle (IA) générative responsables et dignes de confiance qui protègent la vie privée », *Commissariat à la protection de la vie privée du Canada* (7 décembre 2023), en ligne : <https://priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/intelligence-artificielle/gd_principes_ia/> (consulté le 7 décembre 2023).

¹⁰³⁶ M. CARBONNEAU, préc., note 569, p. 157.



Des règles plus précises pourraient donc tenir compte, entre autres :

- de la position dominante de certaines entreprises sur le marché, ayant un effet sur les préjudices qui peuvent découler de leurs pratiques¹⁰³⁷;
- des capacités réelles des petites et moyennes organisations et des risques que soulèvent leurs activités.

« [Cette approche] se concentrerait sur le vrai problème auquel les lois sur la vie privée et la protection des renseignements personnels devraient s'attaquer – les conséquences en termes de pouvoir des relations informationnelles, de façon à aborder la légitimité du traitement de renseignements en tant que question d'équité fondamentale plutôt que d'hygiène des données¹⁰³⁸ ».

Certaines initiatives législatives des dernières années, comme la *Loi sur la non-discrimination génétique*¹⁰³⁹ adoptée au fédéral en 2017, montrent déjà une approche plus substantielle que procédurale¹⁰⁴⁰. Pour illustrer le propos en lien avec une pratique qui n'est pas encore encadrée explicitement, il pourrait être temps de déterminer collectivement la mesure dans laquelle nous jugeons que la publicité ciblée est un moyen de financement acceptable des services numériques, considérant son incidence majeure pour la vie privée¹⁰⁴¹. Les éditeurs devraient-ils toujours avoir le droit d'y avoir recours? Devrait-elle être seulement permmissible dans certains secteurs? Pourrait-on restreindre ou songer à interdire les systèmes d'enchères en temps réel¹⁰⁴²? Peut-on légitimement bloquer l'accès à une personne qui refuserait que ses renseignements soient traités à cette fin? D'une façon analogue, le moissonnage et le courtage en données, évoqués dans les sections 2.1.4 et 2.1.5, pourraient eux aussi constituer des activités sur lesquelles il serait pertinent de se prononcer collectivement sous l'angle de l'acceptabilité.

¹⁰³⁷ N. M. RICHARDS et W. HARTZOG, préc., note 475, p. 4-5.

¹⁰³⁸ *Id.*, p. 5, notre traduction.

¹⁰³⁹ *Loi sur la non-discrimination génétique*, L.C. 2017, c. 3, en ligne : <<https://laws-lois.justice.gc.ca/fra/lois/G-2.5/>>.

¹⁰⁴⁰ P.-L. DÉZIEL, préc., note 568, p. 847.

¹⁰⁴¹ Des rapports parus ces dernières années ont mis en lumière l'ampleur des échanges informationnels qui ont cours à travers le système d'enchères en temps réel, qui propulse la publicité ciblée en ligne. En l'état, n'importe quel acteur peut facilement recevoir des données très précises sur un très grand nombre de personnes, ou alors sur des personnes en particulier, ce qui induit entre autres des risques sécuritaires. Des hauts responsables peuvent par exemple être identifiés, influencés, voire traqués. Voir entre autres à ce sujet : Johnny RYAN et Wolfie CHRISTL, *Europe's hidden-security crisis*, Irish Council for Civil Liberties, en ligne : <<https://www.iccl.ie/wp-content/uploads/2023/11/Europes-hidden-security-crisis.pdf>> (consulté le 15 novembre 2023); CANADIAN ANTI-MONOPOLY PROJECT, *Electric Eyes: Advertising Monopolies and Canada's National Security*, 2025, en ligne : <<https://antimonopoly.ca/wp-content/uploads/2025/09/CAMP-Electric-Eyes-Advertising-Monopolies-and-Canadas-National-Security.pdf>>; Martin UNTERSINGER, Damien LELOUP, Thomas STEFFEN et Elsa DELMAS, « Espions, policiers ou militaires d'élite français trahis par les données publicitaires de leurs smartphones », *Le Monde* (10 décembre 2025), en ligne : <https://www.lemonde.fr/pixels/article/2025/12/10/espions-policiers-ou-militaires-d-elite-francais-trahis-par-les-donnees-publicitaires-de-leurs-smartphones_6656694_4408996.html> (consulté le 10 décembre 2025).

¹⁰⁴² COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, « Real-time bidding (RTB) ou « enchères en temps réel » », en ligne : <<https://www.cnil.fr/fr/definition/real-time-bidding-rtb-ou-encheres-en-temps-reel>> (consulté le 16 avril 2026).



Voici d'autres exemples de pratiques posant des risques systémiques dont on pourrait considérer l'interdiction explicite dans le cadre d'une réflexion collective :

- L'utilisation de renseignements personnels aux fins considérées comme inacceptables dans le *Règlement sur l'IA européen*¹⁰⁴³, à savoir¹⁰⁴⁴ :
 - la manipulation préjudiciable et la tromperie;
 - l'exploitation préjudiciable des vulnérabilités;
 - la notation sociale;
 - l'évaluation individuelle et la prédiction des risques d'infraction pénale;
 - le moissonnage non ciblé en vue du développement de bases de données de reconnaissance faciale;
 - la reconnaissance des émotions en contexte de travail ou d'enseignement;
 - la catégorisation biométrique afin de déduire des renseignements sensibles;
 - l'identification biométrique à distance en temps réel.
- L'analyse génétique à des fins autres que les soins de santé ou la recherche en santé.
- Le recours à des interfaces truquées ou addictogènes (voir la section 2.1.8).
- L'utilisation d'agents conversationnels pour inciter les personnes à communiquer des renseignements personnels sensibles qu'elles n'auraient pas autrement communiqués¹⁰⁴⁵.
- Le suivi numérique effectué d'une façon que les individus ne peuvent contrôler, par exemple par empreinte numérique¹⁰⁴⁶.
- La collecte et la vente de données de géolocalisation à grande échelle¹⁰⁴⁷.
- La tarification dynamique personnalisée ou tarification algorithmique, c'est-à-dire l'établissement automatique d'un prix spécifique à une personne, pour un bien ou un service, en fonction de son profil – lequel se traduit par une exploitation économique de ses vulnérabilités¹⁰⁴⁸.

¹⁰⁴³ *Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)*, préc., note 738, art. 5.

¹⁰⁴⁴ COMMISSION EUROPÉENNE, *Lignes directrices de la Commission sur les pratiques interdites en matière d'intelligence artificielle au sens du règlement (UE) 2024/1689 (règlement sur l'IA)*, C(2025) 5052 final, p. 3-4, en ligne : <<https://ec.europa.eu/newsroom/dae/redirection/document/118657>>.

¹⁰⁴⁵ COMMISSAIRES FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX À LA PROTECTION DE LA VIE PRIVÉE ET DES OMBUDSMANS RESPONSABLES DE LA PROTECTION DE LA VIE PRIVÉE, préc., note 1035.

¹⁰⁴⁶ COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 687, sect. « Restrictions à la PCL ».

¹⁰⁴⁷ Dans un territoire pourtant couvert par le RGPD, un règlement semblable aux lois du Québec, plusieurs médias européens ont récemment montré à quel point les grands ensembles de données de géolocalisation sont facilement constituables et accessibles: Ingo DACHWITZ et Sebastian MEINECK, « Databroker Files: Targeting the EU », *netzpolitik.org* (4 novembre 2025), en ligne : <<https://netzpolitik.org/2025/databroker-files-targeting-the-eu/>> (consulté le 3 décembre 2025); les données permettent entre autres de cibler des personnes d'intérêt, comme le mentionnent ces deux autres rapports précités: J. RYAN et W. CHRISTL, préc., note 1041; CANADIAN ANTI-MONOPOLY PROJECT, préc., note 1041.

¹⁰⁴⁸ À ce propos, voir notamment : Arthur CHARPENTIER, « Des primes d'assurance personnalisées moins chères grâce à l'IA ? Voici pourquoi il s'agit d'une pente glissante », *The Conversation* (5 août 2025), DOI : 10.64628/AAP.ty9ukwfct; Marie-Eve FOURNIER, « Le prix courant ? Une simple fiction. », *La Presse* (13 décembre 2025), en ligne : <<https://www.lapresse.ca/affaires/chroniques/2025-12-13/le-prix-courant-une-simple-fiction.php>> (consulté le 16 décembre 2025); Samuel A.A. LEVINE et Stephanie T. NGUYEN, *The Loyalty Trap: How Loyalty Programs Hook Us with Deals, Hack our Brains, and Hike our Prices*, Vanderbilt Policy Accelerator, 2025, en ligne : <<https://cdn.vanderbilt.edu/vu-URL/wp-content/uploads/sites/412/2025/10/17195957/The-Loyalty-Trap.pdf>> (consulté le 20 octobre 2025); Katie J. WELLS, Lindsay OWENS, Angel HAN et Alan SMITH, *Same Cart, Different Price: Instacart's Price Experiments Cost Families at Checkout*, Groundwork Collaborative / Consumer Reports / More Perfect Union, 2025, en ligne : <<http://groundworkcollaborative.org/wp-content/uploads/2025/12/Same-Cart-Different-Price.pdf>>. Au Canada, le Manitoba a récemment déposé un projet de loi pour interdire cette pratique, qui retient l'attention de manière croissante à l'échelle du pays : Mintu SANDHU, *Loi modifiant la Loi sur*



- Le profilage nuisible aux mineurs (voir la section 2.1.9).
- Certains systèmes d'IA dans le domaine de l'emploi¹⁰⁴⁹.

Pour la Commission, il n'y a pas d'incompatibilité entre des interdictions claires et une innovation axée sur les données. Des protections solidifiées contribueront à permettre d'améliorer le bien-être collectif à l'intérieur de balises éthiques et législatives adéquates.

« L'amélioration des protections de la vie privée n'est pas un obstacle aux innombrables potentialités offertes par les technologies axées sur les données, mais plutôt la condition pour que ce potentiel soit exploité d'une manière responsable et socialement bénéfique. Il nous faut déterminer comment tirer avantage des données et assurer du même coup la protection du droit à la vie, qui est considérée [comme] une condition essentielle pour que les personnes puissent exercer leur autonomie au sein d'une société. Nous pensons qu'une approche centrée sur la prévention et la réduction des risques de préjudices découlant du traitement des renseignements personnels, tant pour les individus, les groupes d'individus et la société en général, est un élément nécessaire à une innovation responsable en ce qui concerne l'analyse prédictive¹⁰⁵⁰. »

Notons enfin qu'à l'inverse, partant du constat que les renseignements personnels peuvent aussi être mis à profit pour le bien commun, il est envisageable d'autoriser explicitement certaines pratiques dans les lois. C'est déjà en quelque sorte l'approche retenue dans la LRSSS, vu la valeur collective que l'on peut tirer des renseignements de santé¹⁰⁵¹.

Qu'il s'agisse d'interdictions ou d'autorisations explicites, les pratiques concernées ne pourraient évidemment pas être nommées de manière exhaustive. Ainsi, les balises souples et contextuelles des lois actuelles, notamment le critère de nécessité, conserveraient pleinement leur importance pour l'encadrement des autres pratiques.

les pratiques commerciales, projet de loi n°49 (17 mars 2026), 43^e lég., 3^e sess. (Assemblée législative du Manitoba), en ligne : <<https://web2.gov.mb.ca/bills/43-3/pdf/b049.pdf>>. Aux États-Unis aussi, certains corps législatifs se penchent sur la pratique et envisagent de l'interdire: Tim BALK, « N.Y. Law Could Set Stage for A.I. Regulation's Next 'Big Battleground' », *The New York Times* (29 novembre 2025), en ligne : <<https://www.nytimes.com/2025/11/29/nyregion/personalized-surveillance-pricing-ai-new-york.html>> (consulté le 1 décembre 2025); Christopher WARD, *Surveillance pricing*, projet de loi n°AB-446 (2025), 2025-2026 (Assemblée législative de Californie), en ligne : <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB446> (dans le secteur de l'épicerie); Greg CASAR, *Stop AI Price Gouging and Wage Fixing Act of 2025*, projet de loi n°H. R. 4640, 119^e lég., 1^{re} sess. (Congrès des États-Unis), en ligne : <<https://www.congress.gov/bill/119th-congress/house-bill/4640/text>>.

¹⁰⁴⁹ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, p. 10, recommandation 6.

¹⁰⁵⁰ J. MACLURE et S. AUCLAIR, préc., note 566, p. 45.

¹⁰⁵¹ F. LECHEVALIER, préc., note 539, p. 57.



Recommandation 61

Considérer, au sein de la réflexion sur l'avenir de la protection des renseignements personnels, l'adoption d'interdictions ou d'autorisations plus explicites en matière de traitement de renseignements personnels.

2.2.3.2. Explorer des modèles de gouvernance collective des données

De nouveaux modèles de gouvernance des données ont été proposés en réponse à certains des enjeux abordés précédemment dans le présent chapitre. Bien qu'ils ne soient pas appropriés à tous les contextes, ils pourraient rééquilibrer le pouvoir dans certains types de relations impliquant l'échange de renseignements personnels, notamment en imposant des devoirs à la partie dominante¹⁰⁵². Cette approche structure déjà plusieurs relations asymétriques dans nos sociétés, en empêchant par exemple des organisations d'agir à l'encontre des intérêts des personnes qui sont en relation avec elles¹⁰⁵³.

Si plusieurs nouveaux modèles de gouvernance des données existent, la Commission attire l'attention sur ceux que l'OCDE décrit comme impliquant des « intermédiaires de données¹⁰⁵⁴ » :

Les prestataires de services facilitant l'accès aux données et leur partage dans le cadre d'accords commerciaux ou non commerciaux entre les détenteurs, les producteurs et/ou les utilisateurs des données. Les détenteurs des données et les tiers de confiance peuvent agir en tant qu'intermédiaires de données.

La fiducie de données est un exemple d'un tel modèle. Inspirée par les *data trusts* envisagés sous l'angle de la *common law*, elle a notamment été étudiée au Québec ces dernières années¹⁰⁵⁵ en tant que solution pour collectiviser la gestion des renseignements personnels en vue de leur utilisation à des fins bénéfiques. Elle vise à mieux conjuguer le respect des droits des personnes concernées et la valorisation des données. L'idée est de s'inspirer du droit existant des fiducies, un concept de droit commun prévu au Code civil¹⁰⁵⁶. Ce modèle prévoit :

- que les personnes concernées confient leurs renseignements personnels à un tiers de confiance, le fiduciaire;
- que le fiduciaire porte la responsabilité de gérer et de traiter les données selon les paramètres de la fiducie, notamment les finalités que les personnes concernées jugent acceptables, suivant des devoirs de loyauté, de diligence et de prudence;
- qu'en cas de manquement du fiduciaire, sa responsabilité peut être engagée. Il peut être condamné à payer des dommages-intérêts et être destitué de son poste de fiduciaire.

¹⁰⁵² N. M. RICHARDS et W. HARTZOG, préc., note 475, p. 3.

¹⁰⁵³ D. J. SOLOVE et W. HARTZOG, préc., note 551, p. 1039-1041.

¹⁰⁵⁴ ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, « Recommandation du Conseil sur l'amélioration de l'accès aux données et de leur partage », *OECD.org* (6 octobre 2021), en ligne : <<https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0463>> (consulté le 17 novembre 2025).

¹⁰⁵⁵ Voir notamment P.-L. DÉZIEL, préc., note 607 aux pages 30-31; Anne-Sophie HULIN, « Introduction à la fiducie québécoise de données », *Laboratoire de cyberjustice* (26 novembre 2020), en ligne : <<https://www.cyberjustice.ca/2020/11/26/introduction-a-la-fiducie-quebecoise-de-donnees/>> (consulté le 17 novembre 2025); Anne-Sophie HULIN, « De la fiducie de données en droit civil québécois : étude exploratoire pour un outil en construction », (2021) 67-2 *McGill Law Journal* 119, DOI : 10.7202/1093269ar.

¹⁰⁵⁶ *Code civil du Québec*, préc., note 500, art. 1260.



Une fiducie de données permet de redonner du contrôle, réel, mais collectif, aux personnes concernées, qui peuvent exprimer en amont, auprès du fiduciaire, des intentions quant au partage et à l'utilisation de leurs renseignements personnels. L'usage d'une fiducie de données peut encourager l'innovation en fournissant un cadre sécuritaire de partage des données.

Bien qu'on l'ait envisagée ici comme ailleurs¹⁰⁵⁷, la fiducie de données présente certaines limites. Elle n'accorde aucune protection aux renseignements personnels des personnes non membres de la fiducie, et ne peut pas non plus protéger les renseignements une fois communiqués à des tiers¹⁰⁵⁸. De plus, elle soulève certaines questions difficiles. Par exemple, elle implique d'assimiler, du moins en partie, les renseignements personnels à des *biens*, alors qu'ils sont traditionnellement considérés comme rattachés à la personnalité et à la dignité des personnes¹⁰⁵⁹. Quoique la Commission nourrisse des doutes sur ce processus de patrimonialisation, qui peut mener à les réifier encore davantage comme marchandises, elle croit que l'idée est suffisamment méritoire pour être étudiée plus à fond par le législateur.

D'autres approches de collectivisation de la gestion des données existent et pourraient être envisagées, notamment les coopératives de données¹⁰⁶⁰ et les collectifs de données¹⁰⁶¹. En Union européenne, le *Règlement sur la gouvernance des données* adopté en 2022 prévoit des dispositions allant dans le sens de ces modèles, et pourrait être étudié¹⁰⁶².

Recommandation 62

Considérer, au sein de la réflexion sur l'avenir de la protection des renseignements personnels, l'adoption de nouveaux modèles de gouvernance des données permettant une gestion collective des renseignements personnels, en réponse aux limites du paradigme du contrôle individuel, et l'imposition de devoirs aux parties disposant d'un pouvoir dominant.

2.2.3.3. S'inspirer du droit de la sécurité des produits pour mieux encadrer les technologies impliquant des renseignements personnels

La vaste réflexion sociale concernant l'**IA**, pilotée par le Conseil de l'innovation du Québec en 2024, a notamment permis de faire ressortir que « [d]ans le secteur des technologies de l'information, [...] les innovations sont généralement mises sur le marché sans faire l'objet de contrôles préalables¹⁰⁶³ ». Il arrive ainsi qu'un produit tout à fait nuisible à la vie privée soit mis en marché sans vérification ni contrôle en

¹⁰⁵⁷ ADA LOVELACE INSTITUTE et UK AI COUNCIL, *Exploring legal mechanisms for data stewardship - Working group final report*, 2021, en ligne : <<https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/>>; I. COFONE, préc., note 474, p. 107-109.

¹⁰⁵⁸ I. COFONE, préc., note 474, p. 108-109.

¹⁰⁵⁹ A.-S. HULIN, préc., note 1055, p. 137-140.

¹⁰⁶⁰ Cécile PETITGAND, « Qu'est-ce qu'une coopérative de données ? », *Data Lama* (14 novembre 2022), en ligne : <<https://datalama.ca/cooperative-de-donnees/>> (consulté le 16 novembre 2022).

¹⁰⁶¹ Bram KLIEVINK, Haiko VAN DER VOORT et Wijnand VEENEMAN, « Creating value through data collaboratives: Balancing innovation and control », (2018) 23-4 *Information Polity* 379-397, DOI : 10.3233/IP-180070.

¹⁰⁶² *Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données)*, JO L 152/1, en ligne : <<https://eur-lex.europa.eu/eli/reg/2022/868/oj/fra>>.

¹⁰⁶³ CONSEIL DE L'INNOVATION DU QUÉBEC, *Le cadre de gouvernance de l'intelligence artificielle*, 2024, p. 50, en ligne : <<https://conseilinnovation.quebec/wp-content/uploads/2024/02/T1-DossierThematique-3.pdf>> (consulté le 7 février 2024).



amont. La vigilance individuelle des personnes et les interventions de surveillance en aval sont alors le seul filet de sécurité, avec les limites énoncées précédemment. Il faut donc souvent attendre des années avant que les organisations en cause subissent des conséquences et que cessent des pratiques nuisibles, lesquelles peuvent entre-temps s'être intégrées à divers processus d'affaires par effet de cascade.

Or l'encadrement est tout autre pour les produits pharmaceutiques ou alimentaires, les véhicules et les produits financiers, par exemple. Dans ces cas, une importante architecture de contrôle en amont a été mise en place.

« Dans d'autres domaines, la loi ne permet pas aux personnes de consentir à prendre des médicaments dangereux ou inefficaces. La loi ne laisse pas les personnes évaluer elles-mêmes si la nourriture qu'elles achètent les empoisonnera. La loi ne permet pas aux personnes d'acheter des produits non sécuritaires. Mais avec les technologies numériques, la loi tolère souvent des produits dangereux et laisse le soin aux consommateurs de déterminer ce qui est sûr de ce qui est risqué. Les consommateurs ne sont pas en mesure de le faire¹⁰⁶⁴. »

Ainsi, étant donné les risques majeurs qui seraient reliés à la circulation des produits dans un état non achevé ou présentant des défauts, le droit prévoit que leur distribution à la population soit précédée par des phases d'évaluation approfondies et des validations par une autorité de contrôle ou des tiers indépendants. Dans le cas où cela ne pouvait être fait, il conviendrait à tout le moins que ces technologies s'accompagnent d'un avertissement clair concernant les risques en matière de protection des renseignements personnels et l'existence d'un encadrement à cet égard.

De l'avis de la Commission, il serait important d'inverser la logique actuelle pour les technologies traitant des renseignements personnels. Elle préconise ainsi de réfléchir à assujettir les fournisseurs, les développeurs et les distributeurs, en tant que participants de la chaîne de valeur, à des règles contraignantes à suivre en amont, qu'elles soient liées à des normes, à des certifications ou à des audits. Le *Règlement sur l'IA* européen, partiellement basé sur le droit de la sécurité des produits, peut servir d'inspiration¹⁰⁶⁵.

À ce propos, la Commission souligne qu'à l'heure actuelle, il n'est pas toujours évident que les activités de développement des technologies de l'information des fournisseurs soient visées par les lois sur la protection des renseignements personnels. Dans la mesure où ils traitent eux-mêmes des renseignements personnels pour concevoir leurs produits, leurs pratiques sont couvertes par la loi. Cependant, la situation est moins claire lorsque ces entreprises vendent *aux autres organisations* des produits leur permettant à elles, en tant qu'utilisatrices finales, de traiter des renseignements personnels. Pourtant, les fournisseurs détiennent alors un pouvoir manifeste sur la façon dont sont conçus ces produits, qui ont ensuite un effet direct sur les personnes concernées. Il serait donc opportun que la loi permette de les en tenir responsables afin d'intervenir à la source avant que certaines pratiques nuisibles ne se généralisent par l'adoption de ces produits et n'engagent la responsabilité des organisations qui s'en portent acquéreuses.

¹⁰⁶⁴ Daniel J. SOLOVE, « Murky Consent: An Approach to the Fictions of Consent in Privacy Law », (2023) 104 *Boston University Law Review* 593-639, p. 637-638, en ligne : <<https://www.bu.edu/bulawreview/files/2024/04/SOLOVE.pdf>>, notre traduction.

¹⁰⁶⁵ *Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)*, préc., note 738.



Voici un exemple de situation problématique qui peut actuellement survenir en matière de fourniture de produit technologique.

Un fournisseur offrant des solutions logicielles collaboratives pour les organisations choisit d'intégrer des fonctionnalités biométriques à son logiciel de visioconférence. Celles-ci permettent de reconnaître la voix et le visage des participants en vue d'indiquer, dans des transcriptions automatiques, qui a tenu quel propos. Par le biais d'une mise à jour automatique auprès de toutes les organisations clientes de son logiciel, le fournisseur active cette fonctionnalité par défaut pour tous. À partir de ce moment, tous les individus ayant recours aux visioconférences au sein des organisations clientes peuvent procéder à l'enrôlement biométrique en se créant un profil vocal ou facial, une opération qui entraîne la collecte de renseignements biométriques. Dans cette situation, le choix de conception du fournisseur engage la responsabilité des organisations clientes, lesquelles se trouvent à mettre en œuvre une collecte potentiellement non conforme sans avoir décidé d'activer les fonctionnalités biométriques elles-mêmes.

Recommandation 63

Considérer, au sein de la réflexion sur l'avenir de la protection des renseignements personnels, l'imposition de contrôles en amont concernant les technologies de l'information impliquant des renseignements personnels.

Recommandation 64

Considérer, au sein de la réflexion sur l'avenir de la protection des renseignements personnels, de viser explicitement dans les lois sur la protection des renseignements personnels toutes les étapes de conception et de production de technologies impliquant de tels renseignements.

CHAPITRE 3

3. La loi sur les renseignements de santé et de services sociaux





Sommaire

La LRSSS constitue une révolution en matière de circulation, d'utilisation et de protection des renseignements de santé et de services sociaux. Elle a apporté des changements substantiels à leur encadrement et s'applique désormais à tous les organismes du secteur, qu'ils soient publics ou privés. Près de deux ans après son entrée en vigueur, les organismes continuent de s'y adapter.

Malgré le caractère récent de la LRSSS, la Commission relève d'ores et déjà quelques enjeux importants à son sujet, soit :

- l'absence d'outils, de procédures et d'infrastructures technologiques essentiels à la protection des renseignements de santé et de services sociaux prévue par la Loi;
- les moyens pour assurer la transparence prévue par la Loi qui ne semblent pas encore implantés, bien que la circulation des renseignements soit, elle, bien présente;
- des questions relatives à l'interprétation de cette loi, notamment quant à son champ d'application.

Compte tenu de ces éléments, la Commission estime que le gouvernement doit déjà entreprendre une réflexion sur l'application de la LRSSS. Celle-ci devrait militer pour un déploiement rapide d'outils permettant d'assurer que les organisations du réseau de la santé et des services sociaux soient en mesure de respecter leurs obligations découlant de la Loi et mener à certaines précisions législatives.



Introduction

Depuis de nombreuses années déjà, le gouvernement québécois souhaite profiter des avancées technologiques afin de faciliter la prestation des services de santé et des services sociaux, notamment en simplifiant la circulation des renseignements au sein du réseau en question. À cet égard, la multiplicité des régimes législatifs et plusieurs restrictions relatives à la circulation des renseignements en cette matière ont historiquement constitué des obstacles importants.

C'est pourquoi plusieurs changements législatifs ont été adoptés au fil du temps. En 2012, la *Loi concernant le partage de certains renseignements de santé* (LPCRS)¹⁰⁶⁶ a fait son entrée dans le corpus législatif. Cette loi constituait une évolution importante en matière de circulation de renseignements de santé : elle permettait leur circulation électronique ainsi que la consultation de certains renseignements entre différents intervenants sans le consentement de la personne concernée. Malgré cette avancée, la LPCRS demeurait contraignante en raison de sa portée limitée : elle ne s'appliquait qu'à certains renseignements particuliers et ne visait que certains intervenants du secteur de la santé.

Les limites de la LPCRS ont nécessité d'autres modifications législatives ou réglementaires¹⁰⁶⁷. Au surplus, les renseignements concernés demeuraient assujettis à plusieurs régimes juridiques. En 2020, la Commission avait d'ailleurs recommandé l'adoption d'un encadrement spécifique et unifié en matière de protection des renseignements de santé¹⁰⁶⁸.

De nouveaux travaux législatifs ont été entamés afin de remplacer la LPCRS, lesquels ont mené au dépôt d'un premier projet de loi en 2021¹⁰⁶⁹. Cette nouvelle loi visait essentiellement à assujettir l'ensemble du réseau de la santé et des services sociaux à un seul et unique régime législatif en matière de gestion et de circulation des renseignements.

Ce projet de loi étant mort au feuillet, les travaux se sont poursuivis et ont conduit au dépôt subséquent, en 2022, d'un second projet de loi¹⁰⁷⁰. Celui-ci avait essentiellement les mêmes objectifs d'uniformisation du cadre légal pour tous les organismes de ce secteur, et d'établissement de normes assurant la protection des renseignements de santé et de services sociaux, tout en visant l'optimisation de leur utilisation et de leur communication.

Pour souligner l'importance de ce nouveau projet de loi, il suffit de constater qu'une quarantaine de mémoires ont été déposés dans le cadre des consultations particulières de la Commission des finances

¹⁰⁶⁶ *Loi concernant le partage de certains renseignements de santé*, RLRQ, c. P-9.0001 [ci-après LPCRS].

¹⁰⁶⁷ Par exemple, 30 intervenants ont été ajoutés par voie réglementaire aux 15 intervenants qui avaient été prévus dans la LPCRS. Voir *Règlement d'application de la Loi concernant le partage de certains renseignements de santé*, RLRQ, c. P-9.0001, r. 0.1, art. 6; LPCRS, art. 69.

¹⁰⁶⁸ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 480, p. 48.

¹⁰⁶⁹ Christian DUBÉ, *Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives*, projet de loi n°19 (présenté le 3 novembre 2021), 42^e lég., 2^e sess., en ligne : <<https://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-19-42-2.html>>.

¹⁰⁷⁰ Christian DUBÉ, *Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives*, projet de loi n°3 (version présentée le 7 décembre 2022), 43^e lég., 1^{re} sess., en ligne : <https://www.assnat.qc.ca/Media/Process.aspx?MediaId=ANQ.Vigie.BII.DocumentGenerique_185619>.



publiques, dont celui de la Commission¹⁰⁷¹. Celle-ci y saluait le travail colossal que constituait le dépôt du projet de loi, mais signalait les nombreux éléments à bonifier afin de permettre l'atteinte des objectifs énoncés, et ce, tout en assurant la protection des renseignements et en limitant les atteintes aux droits des citoyens¹⁰⁷².

Le 4 avril 2023, le projet de loi a été sanctionné et est devenu, une fois codifié, la LRSSS. Entrée en vigueur en majorité le 1^{er} juillet 2024¹⁰⁷³, elle a entraîné d'importants changements pour de nombreuses organisations. **Notamment, elle constitue un régime unique, applicable à tous les organismes du domaine de la santé et des services sociaux, qu'ils proviennent du secteur public ou privé.**

La Commission a reçu le mandat de surveiller l'application de cette loi au même titre qu'elle le fait pour la Loi sur l'accès et la Loi sur le privé¹⁰⁷⁴. Elle est également chargée de produire un rapport sur son application tous les cinq ans¹⁰⁷⁵. C'est dans ce contexte qu'elle s'y penche pour la première fois dans le cadre d'un rapport quinquennal.

Dans ce chapitre, la Commission présente la LRSSS dans ses grandes lignes, puis :

- fait état de l'absence de certains outils, de certaines procédures et de certaines infrastructures technologiques nécessaires à son application, notamment en matière de communication des renseignements entre intervenants et à la personne concernée ou à ses proches, et plaide pour la correction rapide de cette situation;
- note des obstacles dans la mise en œuvre de la transparence prévue envers les personnes concernées quant à la circulation de leurs renseignements et recommande l'entrée en vigueur de la disposition obligeant la journalisation de tout accès à ces renseignements et de toute utilisation ou communication de ceux-ci;
- constate des enjeux dans l'interprétation de certaines dispositions de la Loi concernant, entre autres, son champ d'application, la monétisation des renseignements, le consentement en matière de recherche et le droit transitoire applicable aux mandats ou aux contrats conclus par les organismes privés assujettis à cette loi, et formule des recommandations pour y faire face.

¹⁰⁷¹ COMMISSION D'ACCÈS À L'INFORMATION, *Projet de loi n° 3, Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives - Mémoire de la Commission d'accès à l'information présenté à la Commission des finances publiques dans le cadre des consultations particulières*, 2023, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_ME_PL-3.pdf>.

¹⁰⁷² *Id.*, p. 5.

¹⁰⁷³ GOUVERNEMENT DU QUÉBEC, « Décret 946-2024 du 5 juin 2024 – Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives — Entrée en vigueur de certaines dispositions », dans *Gazette officielle du Québec*, 156^e année, no 24, Québec, Éditeur officiel du Québec, 2024, p. 3391-3393, en ligne : <https://www.publicationsduquebec.gouv.qc.ca/fileadmin/gazette/pdf_encrypte/lois_reglements/2024F/83484.pdf>.

¹⁰⁷⁴ LRSSS, art. 112.

¹⁰⁷⁵ Loi sur l'accès, art. 179.

3.1. Situation actuelle

Alors qu'auparavant, les renseignements de santé et de services sociaux pouvaient être assujettis à différents régimes législatifs en fonction de l'organisme qui les détenait ou de leur nature¹⁰⁷⁶, ils sont aujourd'hui couverts uniquement par la LRSSS. Sont considérés comme de tels renseignements ceux qui permettent d'identifier une personne, même indirectement, et qui répondent à l'une des caractéristiques prévues à la Loi ou qui permettent l'identification d'une personne lorsqu'ils sont recueillis en vue de son enregistrement, de son inscription ou de son admission dans un établissement ou de sa prise en charge par un autre organisme du secteur de la santé et des services sociaux¹⁰⁷⁷. Par exemple, les renseignements suivants peuvent constituer des renseignements de santé ou de services sociaux :

- les renseignements qui concernent l'état de santé physique ou mentale d'une personne, comme un diagnostic;
- ceux qui concernent le matériel prélevé sur une personne, comme un prélèvement sanguin;
- ceux qui concernent les services offerts à une personne, comme une évaluation médicale ou une chirurgie.



¹⁰⁷⁶ La Commission vise ici les organismes du secteur de la santé et des services sociaux au sens de la LRSSS qui étaient auparavant assujettis à différentes lois. Par exemple : à la Loi sur le privé lorsque détenu par une clinique médicale; à la Loi sur l'accès lorsque détenu par un organisme public comme le ministère de la Santé et des Services sociaux; aux articles 17 à 28 de la *Loi sur les services de santé et les services sociaux (version antérieure au 1^{er} juillet 2024)*, RLRQ, c. S-4.2 [ci-après LSSSS] lorsque détenus par un centre hospitalier; à la LPCRS pour les renseignements de santé visés à cette loi, sans compter l'application de certains régimes particuliers comme celui de la *Loi sur l'assurance maladie (version antérieure au 1^{er} juillet 2024)*, RLRQ, c. A-29.

¹⁰⁷⁷ LRSSS, art. 2.



La LRSSS s'applique à ces renseignements lorsqu'ils sont détenus par un organisme du secteur de la santé et des services sociaux¹⁰⁷⁸, soit, dans les grandes lignes :

- des organismes nommés, comme le ministère de la Santé et des Services sociaux¹⁰⁷⁹, Santé Québec¹⁰⁸⁰ ou Héma-Québec¹⁰⁸¹;
- des organismes devant détenir une autorisation¹⁰⁸² ou recevoir une reconnaissance¹⁰⁸³, ou être titulaires d'un permis¹⁰⁸⁴ ou d'un agrément¹⁰⁸⁵;
- des personnes ou des groupements qui exploitent un cabinet privé de professionnel au sens de certaines lois¹⁰⁸⁶.

La LRSSS marque un virage significatif par rapport à la circulation des renseignements de santé et de services sociaux. En effet, ce qui la distingue nettement des régimes qu'elle remplace est la possibilité pour les intervenants du secteur de la santé et des services sociaux d'accéder, lorsque les conditions à cet égard sont remplies, aux renseignements de santé et de services sociaux d'une personne sans qu'il soit nécessaire que cette dernière consente à cet accès ou à cette communication¹⁰⁸⁷. Autrement dit, un intervenant de ce secteur peut accéder à tous les renseignements de cette nature nécessaires à sa prestation de services de santé ou de services sociaux, et ce, peu importe l'organisme du secteur détenant ces renseignements¹⁰⁸⁸. La seule limite à cet égard est la restriction au droit d'accès ou le refus pouvant être exprimés par la personne concernée¹⁰⁸⁹. Cet accès est donc permis par la personne concernée à *moins* qu'elle n'exprime une volonté contraire suivant les modalités prévues.

¹⁰⁷⁸ *Id.*, art. 4.

¹⁰⁷⁹ *Id.*, art. 4 par. 1.

¹⁰⁸⁰ *Id.*, art. 4 par. 3.

¹⁰⁸¹ *Id.*, art. 4 par. 2 et annexe I, par. 4 D'autres organismes sont identifiés comme l'Institut national de santé publique du Québec ou la Régie de l'assurance maladie du Québec.

¹⁰⁸² C'est le cas pour un centre médical spécialisé, qui doit détenir une autorisation de Santé Québec (article 555 de la LGSSS) : *Id.*, art. 4 par. 2 et annexe II par. 2. Les organismes visés aux paragraphes 6 et 8 de l'annexe II de la LRSSS doivent également détenir une autorisation.

¹⁰⁸³ C'est le cas pour un centre de communication santé, qui doit recevoir une reconnaissance de Santé Québec ou du ministre de la Santé et des Services sociaux (art. 18 de la *Loi sur les services préhospitaliers d'urgence*, RLRQ, c. S-6.2) : *Id.*, art. 4 par. 2, annexe II par. 3. Les organismes visés au paragraphe 7 de l'annexe II de la LRSSS doivent également recevoir une reconnaissance.

¹⁰⁸⁴ C'est le cas pour l'exploitant d'un centre de procréation assistée (article 15 de la *Loi sur les activités cliniques et de recherche en matière de procréation assistée*, RLRQ c. A-5.01). *Id.*, art. 4 par. 2 et annexe II par. 4. Les organismes visés aux paragraphes 5, 9 et 10 de l'annexe II de la LRSSS doivent également détenir un permis.

¹⁰⁸⁵ C'est le cas pour une maison de soins palliatifs (article 3 par. 2 de la *Loi concernant les soins de fin de vie*, RLRQ c. S-32.0001) *Id.*, art. 4 par. 2 et annexe II par. 11.

¹⁰⁸⁶ *Id.*, art. 4 par. 2 et annexe II, 1.

¹⁰⁸⁷ Avant l'entrée en vigueur de la LRSSS, la LPCRS visait l'atteinte d'objectifs similaires en prévoyant le partage de renseignements de santé entre certains intervenants du secteur de la santé. Cette loi est cependant circonscrite à certains renseignements dont la circulation bénéficie à certains intervenants en particulier, alors que la LRSSS vise tous les renseignements de santé et de services sociaux détenus par un organisme du secteur de la santé et des services sociaux.

¹⁰⁸⁸ LRSSS, art. 1 et 38 à 43. À cet égard, les régimes qui prévalaient avant l'entrée en vigueur de la LRSSS s'articulaient généralement autour du concept du consentement. Une personne devait consentir à la communication de ses renseignements entre les différents intervenants de différents organismes qui pouvaient intervenir dans le cadre d'un parcours de soin. En principe, la LRSSS permet à ces mêmes intervenants de différents organismes de recevoir communication des renseignements d'un patient dans le cadre de son parcours de soins sans que ce dernier doive consentir pour chaque communication.

¹⁰⁸⁹ *Id.*, art. 7 et 8.



En ce sens, la LRSSS tente de trouver un équilibre entre la protection des renseignements de santé et de services sociaux et son objectif d'optimiser leur circulation entre les différents organismes du domaine de la santé et des services sociaux qui seront impliqués pendant le parcours de soins d'une personne¹⁰⁹⁰.

De l'avis de la Commission, le respect de cet équilibre, parfois précaire, est primordial et impose une vigilance constante.

L'un des moyens choisis par le législateur pour introduire un certain équilibre dans cette nouvelle réalité a été d'introduire de plus grandes mesures de transparence envers les personnes concernées. La LRSSS prévoit que toute personne a droit d'être informée de l'existence de tout renseignement de santé et de services sociaux la concernant détenu par un organisme de ce secteur ainsi que d'être informée des accès à ces renseignements, de leurs utilisations et de leurs communications¹⁰⁹¹. Cependant, comme on le verra plus loin, cette transparence annoncée et prévue par la LRSSS demeure, pour le moment du moins, davantage théorique.

Un autre pan important lié à la LRSSS est la constitution du système national de dépôt de renseignements¹⁰⁹². À terme, ce système doit permettre aux intervenants des établissements de Santé Québec de collecter, de conserver et d'utiliser les renseignements de santé et de services sociaux¹⁰⁹³. Il doit aussi permettre l'indexation de l'ensemble des renseignements concernés détenus par les autres organismes de ce secteur¹⁰⁹⁴. Ce système est donc une composante essentielle au succès de la mise en œuvre de la LRSSS. Or, près de deux ans après l'entrée en vigueur de la LRSSS, il n'est toujours pas en place. Notons que cette situation freine grandement l'évaluation concrète de la réforme apportée par la LRSSS, en limitant de façon importante la collecte de données de terrain ou de statistiques.

¹⁰⁹⁰ *Id.*, art. 1.

¹⁰⁹¹ *Id.*, art. 7 et 8.

¹⁰⁹² LGSSS, art. 76 à 84.

¹⁰⁹³ *Id.*, art. 76 al. 2(1).

¹⁰⁹⁴ *Id.*, art. 76 al. 2(3).



3.2. Enjeux

Bien que la Commission prenne acte du fait qu'il s'est écoulé, somme toute, peu de temps depuis l'entrée en vigueur de la LRSSS et qu'il existe peu de données concrètes disponibles quant aux effets de l'implantation de cette loi, elle souhaite tout de même aborder certains enjeux lui apparaissant importants et névralgiques. Ceux-ci sont principalement liés aux outils, aux procédures et aux infrastructures technologiques nécessaires à l'application de la LRSSS, à l'absence de journalisation au soutien de la transparence envers les personnes concernées et à des enjeux d'interprétation de la loi.

3.2.1. Des outils, des procédures et des infrastructures technologiques nécessaires à l'application de la LRSSS sont manquants

En premier lieu, la Commission considère que l'atteinte des objectifs de la LRSSS est difficile, voire impossible, sans l'implantation des outils, des procédures et infrastructures technologiques qui étaient prévus pour appuyer sa mise en œuvre. **Plus encore, la Commission estime que le vide alimenté par leur absence soulève des enjeux sérieux en matière de protection des renseignements de santé et de services sociaux.**

Dans ce contexte, la Commission craint fortement que les organismes du secteur de la santé et des services sociaux ne soient pas en mesure de respecter certaines dispositions de la LRSSS. Elle aborde ci-après quelques exemples de situations où l'absence de solutions technologiques fait craindre la possibilité de manquements au respect de la Loi.

3.2.1.1. Enjeux relatifs à la communication des renseignements entre intervenants du secteur de la santé et des services sociaux

Un intervenant œuvrant dans le secteur de la santé et des services sociaux peut utiliser ou communiquer des renseignements de santé et de services sociaux selon deux possibilités distinctes : avec le consentement de la personne concernée ou dans les cas prévus par la LRSSS et suivant ses modalités¹⁰⁹⁵.

En vertu de la LRSSS¹⁰⁹⁶, un tel intervenant peut être informé de l'existence d'un renseignement de santé et de services sociaux détenu par un organisme du secteur en question et y avoir accès si ce renseignement est nécessaire à sa prestation de services, et ce, sans le consentement de la personne concernée. L'organisme du secteur de la santé et des services sociaux qui détient un tel renseignement a l'obligation de le communiquer à l'intervenant¹⁰⁹⁷, et ce, à moins que la personne concernée ait exprimé sa volonté de restreindre une telle communication¹⁰⁹⁸.

¹⁰⁹⁵ LRSSS, art. 5.

¹⁰⁹⁶ *Id.*, art. 38 et 39.

¹⁰⁹⁷ *Id.*, art. 63 et 69.

¹⁰⁹⁸ *Id.*, art. 7.



Ces dispositions permettent d'accroître et de faciliter la circulation de ce type de renseignements dans le cadre de l'offre de services de santé et de services sociaux. Certes, cette circulation présente plusieurs avantages, tant pour la personne concernée que pour les intervenants. En revanche, la Commission est d'avis qu'elle requiert certaines balises et des garde-fous qui doivent être mis en place afin de garantir une protection adéquate des renseignements en cause, d'assurer le contrôle de cette circulation accrue et de réduire les risques y étant associés. Selon la Commission, l'implantation d'outils, de procédures et d'infrastructures technologiques est une avenue à privilégier pour aider les organismes du secteur de la santé et des services sociaux à protéger adéquatement les renseignements concernés et à développer les réflexes nécessaires au respect de la LRSSS.

Actuellement, les organismes du secteur de la santé et des services sociaux n'ont aucun moyen technologique global et formel pour identifier et authentifier les intervenants d'autres organismes, notamment afin de valider qu'ils sont bien des intervenants au sens de la LRSSS ou non¹⁰⁹⁹. Selon la compréhension de la Commission, cette situation prévaut tant pour Santé Québec à l'échelle provinciale¹¹⁰⁰ que pour les autres organismes publics et privés visés par l'application de la LRSSS¹¹⁰¹. Il n'y a également aucun moyen technologique permettant aux organismes détenteurs des renseignements de santé et de services sociaux de s'assurer que la personne concernée est bel et bien un patient de l'intervenant d'un autre organisme qui demande accès aux renseignements.

Dans le contexte actuel, les organismes de ce secteur ne disposent pas davantage de moyen standardisé leur permettant de communiquer les renseignements de santé et de services sociaux entre eux. Bien que la LRSSS prévoie un pouvoir réglementaire d'édicter des règles encadrant la qualité des renseignements détenus par les organismes et, plus précisément, les normes ou les standards techniques devant être utilisés, notamment en matière de catégorisation des renseignements ainsi que de mobilité et de valorisation des renseignements¹¹⁰², un tel règlement n'a toujours pas été adopté. Ainsi, chaque organisme du secteur de la santé et des services sociaux peut déterminer sa propre façon de procéder et, par exemple, utiliser des moyens technologiques qui ne sont pas nécessairement accessibles à tous les autres organismes. En ce sens, certains pourraient, faute d'avoir les connaissances nécessaires à cet égard, choisir des moyens inappropriés pour communiquer des renseignements particulièrement sensibles à d'autres organismes.

Aussi, sans le système national de dépôt de renseignements, les intervenants n'ont actuellement aucune manière de savoir quels organismes détiennent quels renseignements à propos d'une personne. Rappelons que sous le régime de la LRSSS, les acteurs assujettis comprennent tant des organismes qui relèvent de la sphère privée, comme les cliniques médicales, les cliniques de physiothérapie ou les pharmacies communautaires, que de la sphère publique, comme les centres hospitaliers ou les laboratoires. L'objectif de la LRSSS est justement de permettre la circulation des renseignements de santé et de services sociaux entre ces organismes en fonction du parcours de soins d'une personne.

¹⁰⁹⁹ Voir *Id.*, art. 3 pour la définition du terme « intervenant ».

¹¹⁰⁰ En principe, c'est le système national de dépôt des renseignements prévu par la LGSSS qui permettra à Santé Québec de faire circuler les renseignements de santé et de services sociaux au sein des établissements à l'échelle provinciale.

¹¹⁰¹ Outre les systèmes mis en place en lien avec la LPCRS, il n'y a aucun processus technologique formel qui permet à tous les organismes de communiquer les renseignements d'une personne entre eux.

¹¹⁰² LRSSS, art. 90 al. 1, par. 3 et 5.



Or, de l'avis de la Commission, la circulation sécuritaire de ces renseignements conformément à la LRSSS est impossible sans la mise en place des outils, des procédures et des infrastructures technologiques qui permettent de réaliser les différentes opérations nécessaires à l'atteinte des objectifs de la LRSSS.

En somme, en vertu de la LRSSS, un organisme du secteur de la santé et des services sociaux se retrouve à assumer plusieurs responsabilités importantes comme :

- la protection des renseignements de santé et de services sociaux qu'il détient¹¹⁰³;
- la communication des renseignements de santé et de services sociaux demandés par un intervenant du secteur¹¹⁰⁴.

Or malgré ces responsabilités névralgiques, les outils, les procédures et les infrastructures technologiques qui lui permettraient d'assumer pleinement ces responsabilités ne sont pas encore disponibles. En l'absence des solutions technologiques lui permettant de vérifier l'identité des intervenants qui souhaitent obtenir l'accès à des renseignements de santé et de services sociaux ainsi que leur lien clinique avec la personne concernée, un organisme ne peut pas, selon la Commission, prétendre respecter ses obligations de manière efficiente. **Pour la Commission, en l'absence des outils et des infrastructures technologiques requises ainsi que de procédures quant à la communication des renseignements de santé et de services sociaux, chaque moment qui passe augmente les risques d'incidents de confidentialité.** De tels incidents pourraient venir éroder la confiance du public.

À cet égard, notons qu'un organisme du secteur qui retiendrait un renseignement de santé et de services sociaux suivant une demande légitime d'un intervenant pourrait être accusé de commettre une infraction et pourrait, du même coup, être passible d'une amende¹¹⁰⁵. Ce même organisme qui communiquerait un renseignement au mauvais destinataire, par exemple à un imposteur, se retrouverait dans la même situation¹¹⁰⁶.

3.2.1.2. Enjeux relatifs à l'application des droits de restriction et de refus des personnes concernées

Comme mentionné précédemment, les personnes concernées par des renseignements de santé et de services sociaux bénéficient du droit d'en restreindre l'accès à un intervenant particulier ou à une catégorie d'intervenants¹¹⁰⁷. Elles ont également le droit de refuser qu'un tel renseignement, présent ou à venir, soit accessible à certains proches ou encore, dans certains cas, à des chercheurs¹¹⁰⁸. Comme prévu par règlement¹¹⁰⁹, ces droits s'exercent par l'envoi, selon le cas, d'un avis de restriction ou d'un avis de refus écrit à l'organisme détenant les renseignements visés. Cet avis précise les personnes touchées par l'avis concerné et contient, notamment, une description des renseignements visés.

L'application de ces droits de restriction ou de refus implique vraisemblablement de créer des règles ou des alertes électroniques permettant de bloquer, conformément aux avis reçus, l'accès de certains

¹¹⁰³ *Id.*, art. 99.

¹¹⁰⁴ *Id.*, art. 38, 39 et 69.

¹¹⁰⁵ *Id.*, art. 159 par. 2.

¹¹⁰⁶ *Id.*, art. 160 par. 1.

¹¹⁰⁷ *Id.*, art. 7.

¹¹⁰⁸ *Id.*, art. 8.

¹¹⁰⁹ *Règlement d'application de certaines dispositions de la Loi sur les renseignements de santé et de services sociaux*, RLRQ, c. R-22.1, r. 1, art. 3 à 6.



intervenants ou chercheurs à certains renseignements, ou encore d'indiquer aux responsables des organismes de santé et de services sociaux que des renseignements ne peuvent être communiqués aux proches de la personne concernée. **Pour la Commission, le respect de ces droits de restriction et de refus pourrait donc être difficile, voire impossible, en l'absence d'une infrastructure technologique appropriée.**

3.2.2. L'absence de journalisation de l'accès aux renseignements entrave la transparence envers les personnes concernées

La Commission est préoccupée par le fait que près de deux ans après l'entrée en vigueur de la LRSSS, les organismes du secteur de la santé et des services sociaux n'ont toujours pas l'obligation de journaliser l'accès aux renseignements de santé et de services sociaux.

Les dossiers médicaux d'une personne bénéficient d'un haut niveau d'attente raisonnable en matière de protection de la vie privée. En effet, « ces dossiers sont susceptibles de contenir des renseignements très sensibles qui concernent la personne et qui sont particulièrement en mesure de révéler ses traits de personnalité, son mode de vie, ses pensées, etc.¹¹¹⁰ ».

L'ouverture à une plus grande circulation des renseignements de santé et de services sociaux devait par conséquent, en principe, s'accompagner d'une plus grande transparence envers les personnes concernées. C'est pourquoi la LRSSS prévoit pour celles-ci¹¹¹¹ :

- un droit d'accès à leurs renseignements de santé et de services sociaux;
- un droit d'être informées du nom de toute personne ou de tout groupement qui a accédé à un tel renseignement, l'a utilisé ou l'a communiqué, de même que de la date et de l'heure de cette opération.

Comme le mentionnait la Commission dans son mémoire sur la LRSSS, l'un des piliers de la relation de confiance entre un usager et un professionnel de la santé et des services sociaux repose ainsi sur l'assurance que les renseignements qu'il accepte de lui confier demeurent confidentiels¹¹¹². C'est pourquoi le droit au secret professionnel est garanti par la Charte¹¹¹³. Il permet à une personne de s'ouvrir complètement au professionnel afin qu'il puisse lui fournir les meilleurs soins possibles, sachant que le partage de ses renseignements dépendra de son autorisation ou de l'application de la Loi.

La Commission a d'ailleurs exprimé plusieurs réserves quant à la portée de la LRSSS et à l'étendue de son application¹¹¹⁴. À plusieurs égards, la Commission recommandait de mieux circonscrire ou de limiter de façon plus précise les conditions d'application de la LRSSS¹¹¹⁵.

¹¹¹⁰ Yvon DUPLESSIS et Jean HÉTU, *L'accès à l'information et la protection des renseignements personnels - Santé et services sociaux*, MAJ 16/07/2014 (feuilles mobiles), volume 1, Brossard, Québec, Wolters Kluwer Québec Ltée, par. 4174.

¹¹¹¹ LRSSS, art. 17 et 18.

¹¹¹² COMMISSION D'ACCÈS À L'INFORMATION, préc., note 1071, p. 4.

¹¹¹³ Charte, art. 9.

¹¹¹⁴ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 1071, p. 8 à 12.

¹¹¹⁵ Voir notamment : *Id.*, p. 20 et 21, 23 à 26, 40 et 41 ainsi que 43 et 44.



Malheureusement, depuis l'entrée en vigueur de la LRSSS, la transparence envers les personnes concernées quant à la circulation de leurs renseignements a été reléguée au banc des principes théoriques.

D'une part, l'obligation des organismes du secteur de la santé et des services sociaux de journaliser¹¹¹⁶ tout accès, toute utilisation et toute communication¹¹¹⁷ de renseignements de santé et de services sociaux n'est toujours pas en vigueur. D'autre part, une disposition transitoire de la LRSSS¹¹¹⁸ limite l'obligation de ces organismes à inscrire les communications de renseignements de santé et de services sociaux dans un registre.

Autrement dit, ces organismes n'ont aucune obligation de journaliser les accès aux renseignements de santé et de services sociaux qu'ils détiennent ainsi que les utilisations qu'ils en font.

À ce jour, alors que la simplification de la circulation des renseignements de santé et de services sociaux entre les intervenants et les organismes de ce secteur est pleinement en vigueur, les outils visant à assurer la transparence de cette circulation pourtant prévue par le législateur ne sont pas, dans les faits, en place. **En conséquence, le droit de savoir qui a accédé à un renseignement ou l'a utilisé pourrait donc être en grande partie illusoire.**

Or l'expérience passée a démontré toute l'importance de la surveillance des accès aux renseignements, notamment par leur journalisation et l'exploitation de cette journalisation. C'est précisément à ce niveau que de nombreux incidents de confidentialité ont été constatés dans les dernières années¹¹¹⁹.

¹¹¹⁶ C'est-à-dire de les documenter automatiquement, dans un registre numérique.

¹¹¹⁷ LRSSS, art. 103.

¹¹¹⁸ *Id.*, art. 265.

¹¹¹⁹ Voir notamment Hugo JONCAS, « Confidentialité des dossiers de patients | Des secrets médicaux bafoués », *La Presse* (11 mai 2023), en ligne : <<https://www.lapresse.ca/actualites/sante/2023-05-11/confidentialite-des-dossiers-de-patients/des-secrets-medicaux-bafoues.php>> (consulté le 31 mars 2026); VÉRIFICATEUR GÉNÉRAL DU QUÉBEC, « Protection des renseignements personnels numériques des usagers du réseau de la santé et des services sociaux - Audit de performance », dans *Rapport du Vérificateur général du Québec à l'Assemblée nationale pour l'année 2023-2024*, 2023, p. 66-115 aux pages 88-89, en ligne : <https://www.vgq.qc.ca/Fichiers/Publications/rapport-annuel/204/VGQ_nov2023_web.pdf>.



Dans un audit réalisé en 2023, le Vérificateur général du Québec illustre certains problèmes associés à l'absence de journalisation¹¹²⁰ :

« Dans les trois entités auditées, des activités dans des systèmes contenant des renseignements personnels d'utilisateurs ne sont pas journalisées. De plus, un autre système déployé dans le réseau par le MSSS ne permet pas de journaliser la gestion des droits d'accès. Ainsi, quelqu'un pourrait se voir octroyer ou même, dans certains cas, s'octroyer lui-même un droit d'accès temporaire sans traçabilité.

Par ailleurs, pour deux systèmes utilisés dans les établissements, dont l'un est géré par le MSSS, et pour lesquels il existe de la journalisation, celle-ci est altérable par des personnes dont les activités sont elles-mêmes journalisées, comme des administrateurs informatiques (hauts privilèges d'accès). Ces personnes seraient en mesure alors, par exemple, de faire disparaître les traces d'un accès non autorisé à des renseignements personnels d'utilisateurs. Selon le MSSS la désuétude technologique rend difficile l'instauration de contrôles permettant de conserver une version inaltérable de la journalisation. Comme il n'est pas prévu que ces systèmes seront remplacés avant plusieurs années, le risque associé à cette lacune subsistera. »

Dans la situation actuelle, l'exercice de la surveillance de ces accès par les organismes concernés pourrait être limité ou même compromis. La Commission voit difficilement comment les organismes du secteur de la santé et des services sociaux peuvent surveiller le respect des droits de refus d'accès ou des droits de restriction d'accès prévus par la LRSSS¹¹²¹ s'il n'y a pas un contrôle étendu des accès aux renseignements et de leurs utilisations.

Au surplus, comment la Commission pourrait-elle exercer une quelconque surveillance d'un système dont les accès ou les utilisations ne sont pas journalisés? Tant que s'appliquera la disposition transitoire évoquée plus haut, qui limite l'obligation de journalisation, cette situation apparaissant problématique se poursuivra. La Commission craint que la solution temporaire perdure et fragilise le niveau de protection qui constituait la contrepartie essentielle aux importantes modifications législatives apportées par la LRSSS.

Cette situation préoccupe grandement la Commission, alors qu'elle est à même de constater que l'accès aux renseignements de santé et de services sociaux et leur utilisation sont déjà en cours, ce qui est particulièrement clair en matière de recherche¹¹²².

En somme, l'absence d'obligation pour les organismes de journaliser les accès aux renseignements de santé et de services sociaux et leurs utilisations est un écueil majeur à leur protection. Comme le constatait le Vérificateur général dans un audit de performance visant trois de ces organismes, la situation était déjà problématique avant l'entrée en vigueur de la LRSSS¹¹²³ :

¹¹²⁰ VÉRIFICATEUR GÉNÉRAL DU QUÉBEC, préc., note 1119 à la page 88.

¹¹²¹ LRSSS, art. 7 et 8.

¹¹²² Entre le 1^{er} juillet 2024 et le 28 février 2025, la Commission a reçu 564 ententes de recherche en vertu de la LRSSS. Ce nombre s'est accru alors qu'elle en a reçu 1 202 de plus entre le 28 février 2025 et le 28 février 2026, pour un total de 1 766 entre l'entrée en vigueur de la Loi et cette date.

¹¹²³ VÉRIFICATEUR GÉNÉRAL DU QUÉBEC, préc., note 1119 à la page 3.



Constats

1. *Le MSSS et les établissements audités ne contrôlent pas suffisamment les accès à des renseignements personnels numériques d'utilisateurs.*
2. *Des mesures de cybersécurité, reconnues comme nécessaires en matière de protection des renseignements personnels numériques, sont à améliorer.*
3. *Le MSSS et les établissements audités manquent de rigueur dans la gestion des risques et des incidents en lien avec la confidentialité des renseignements personnels numériques. [...]*

Si ces constats étaient déjà préoccupants, ils le sont encore plus depuis l'entrée en vigueur de la LRSSS. En effet, cette loi se distingue de l'ancien régime puisqu'elle simplifie la circulation des renseignements de santé et de services sociaux. Cette réalité rend d'autant plus importante la surveillance des mesures de protection de ceux-ci.

La Commission est particulièrement préoccupée par le fait que le gouvernement pourrait attendre la mise en place du système national de dépôt de renseignements pour rendre obligatoire la journalisation des accès aux renseignements de santé et de services sociaux et de leurs utilisations. Or, un tel système pourrait encore prendre des années avant d'être mis en place.

3.2.1. La LRSSS soulève d'ores et déjà certains importants enjeux d'interprétation

Puisqu'elle constitue du droit nouveau, la LRSSS présente certains enjeux d'interprétation. Il va de soi que le temps devrait permettre de résoudre plusieurs d'entre eux par des décisions des tribunaux administratifs et de droit commun. La Commission souhaite malgré tout en soulever certains pour lesquels une intervention législative devrait être envisagée dès maintenant en raison de leur importance.

3.2.1.1. La portée de la LRSSS

Préciser adéquatement la portée de la LRSSS est primordial : elle permet notamment aux intervenants et aux organismes du secteur de la santé et des services sociaux de connaître leurs responsabilités et leurs obligations relatives à l'application de la Loi.

De l'avis de la Commission, parmi les organismes assujettis à la Loi, un cas notamment présente un problème d'interprétation significatif, soit celui de la personne ou du groupement qui exploite un cabinet privé de professionnel¹¹²⁴. Il faut se référer à la LGSSS¹¹²⁵ ou à la *Loi sur les services de santé et les services sociaux pour les Inuit et les Naskapis*¹¹²⁶ pour la définition de ces termes :

LGSSS

Pour l'application de la présente loi, on entend par « cabinet privé de professionnel » l'entreprise au sein de laquelle un ou plusieurs médecins, dentistes ou autres professionnels, individuellement ou en groupe, pratiquent habituellement leur profession à

¹¹²⁴ LRSSS, art. 4 paragr. 2 et annexe II paragr. 1.

¹¹²⁵ LGSSS, art. 481 al. 2.

¹¹²⁶ *Loi sur les services de santé et les services sociaux pour les Inuit et les Naskapis*, RLRQ, c. S-4.2, art. 95 al. 2 [ci-après LSSSS pour les Inuit et les Naskapis].



titre privé et à leur seul compte, sans fournir à leur clientèle, directement ou indirectement, des services d'hébergement et sans lui offrir des traitements médicaux spécialisés.

LRSSS pour les Inuit et les Naskapis

On entend par cabinet privé de professionnel un cabinet de consultation ou bureau, situé ailleurs que dans une installation maintenue par un établissement, où un ou plusieurs médecins, dentistes ou autres professionnels, individuellement ou en groupe, pratiquent habituellement leur profession à titre privé et à leur seul compte, sans fournir à leur clientèle, directement ou indirectement, des services d'hébergement.

Cette situation peut soulever certaines interrogations. Une conclusion envisageable serait de limiter le terme « professionnel » aux professions réglementées au sens du *Code des professions*¹¹²⁷. Or, cette position ne peut être retenue. D'une part, le terme « profession » dans son sens courant est plus large : le *Grand dictionnaire terminologique* de l'Office québécois de la langue française retient la définition « personne qui exerce régulièrement une profession, un métier, par opposition à un amateur¹¹²⁸ ». D'autre part, les intervenants au sens de la LRSSS n'exercent pas nécessairement des professions réglementées¹¹²⁹. Pour restreindre la portée du cabinet privé de professionnel aux professions réglementées, il aurait fallu que le législateur apporte cette précision directement dans la LRSSS¹¹³⁰.

Dans ce contexte, la circonscription des professions susceptibles de fournir des services du domaine de la santé et des services sociaux, sans autres critères, est un exercice difficile : les personnes visées, selon la définition donnée à ces termes, pourraient être nombreuses. Il suffit de penser à la quantité de professions liées au domaine de la santé et des services sociaux qui sont susceptibles d'exercer dans des lieux que l'on pourrait qualifier d'un « cabinet privé de professionnel », dont les suivantes¹¹³¹ :

▪ Pharmaciens;	▪ Diététistes-nutritionnistes;	▪ Naturopathes;
▪ Dentistes;	▪ Infirmières;	▪ Podologues;
▪ Physiothérapeutes;	▪ Kinésiologues;	▪ Audioprothésistes;
▪ Acuponcteurs;	▪ Orthophonistes;	▪ Opticiens;
▪ Ergothérapeutes;	▪ Orthoptistes;	▪ Chiropraticiens;
▪ Massothérapeutes;	▪ Psychoéducateurs;	▪ Psychothérapeutes;
▪ Psychologues;	▪ Sexologues;	▪ Sophrologues;
▪ Audiologistes;	▪ Travailleurs sociaux;	▪ Denturologistes;
▪ Biochimistes;	▪ Techniciens en orthèse-	▪ Optométristes.
▪ Criminologues;	prothèse;	

Des cas potentiellement litigieux pourraient être soulevés. À titre d'exemples :

- Faut-il considérer que la chirurgie plastique ayant un objectif purement esthétique relève des services du domaine de la santé et des services sociaux? A priori, les médecins qui la pratiquent détiennent les mêmes renseignements que tout organisme susceptible de procéder à des interventions chirurgicales pour des fins autres qu'esthétiques.
- Si la chirurgie esthétique relève du domaine de la santé et des services sociaux, faut-il considérer que le tatouage est également un service qui relève de ce domaine?

¹¹²⁷ *Code des professions*, préc., note 49.

¹¹²⁸ OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « professionnel, professionnelle », *Grand dictionnaire terminologique*, en ligne : <<https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/1299373/professionnel>> (consulté le 31 mars 2026).

¹¹²⁹ LRSSS, art. 3, 38 et 39.

¹¹³⁰ Soit au premier paragraphe de l'annexe II de cette loi.

¹¹³¹ Attention : par cette énumération, la Commission n'affirme pas que ces professions sont toutes assujetties à la LRSSS.



- Les conseillers en orientation offrent-ils des services du domaine de la santé et des services sociaux, étant des « professionnels de la relation d'aide, de l'orientation et du développement de carrière qui pratiquent dans le domaine de la santé mentale et des relations humaines¹¹³² »?
- En l'absence d'un traitement psychologique, est-ce qu'un coach en préparation mentale pour sportifs ou un coach de vie qui accompagne une famille dans des difficultés interpersonnelles offrent des services du domaine de la santé et des services sociaux?

En ce sens, la Commission s'interroge : quelles sont les balises à considérer à cet égard? Est-ce que toute intervention physique ou psychologique constitue un service du domaine de la santé et des services sociaux?

Ces questions sont particulièrement importantes. Les personnes exploitant des organismes qui pourraient être visés par la LRSSS doivent être en mesure de déterminer facilement si cette loi s'applique à leurs domaines d'activité ou non.

3.2.1.2. La monétisation des renseignements de santé et des services sociaux

Le législateur a choisi d'inscrire dans l'objet de la LRSSS que l'optimisation de l'utilisation et de la communication des renseignements de santé et de services sociaux devaient s'effectuer « à l'exclusion de leur vente ou de toute autre forme d'aliénation¹¹³³ ».

La Commission estime qu'il aurait été préférable d'interdire explicitement la vente ou l'aliénation des renseignements de santé et de services sociaux ou de circonscrire cette vente ou cette aliénation. En effet, le choix du législateur soulève certaines questions.

La LRSSS permet une circulation accrue des renseignements de santé et de services sociaux détenus par un organisme de ce secteur par des cas d'utilisation et de communication qu'elle prévoit expressément. Toute autre utilisation ou communication est conditionnelle à l'obtention du consentement exprès de la personne concernée¹¹³⁴. La Commission comprend donc qu'une personne pourrait donner un consentement libre et éclairé à un organisme du secteur de la santé et des services sociaux afin que celui-ci puisse vendre ou autrement aliéner un renseignement de santé et de services sociaux la concernant.

Or, la LRSSS établit une infraction pour quiconque « vend ou autrement aliène un renseignement détenu par un organisme ou dont il a obtenu communication d'un organisme, à moins, dans ce dernier cas, qu'il ne soit la personne concernée par ce renseignement¹¹³⁵ ». La Commission comprend de cette disposition qu'un organisme ne pourrait, même avec le consentement de la personne concernée, vendre ou aliéner un renseignement de santé et de services sociaux. D'ailleurs, les échanges des parlementaires lors de l'étude détaillée de cette disposition démontrent qu'ils souhaitaient interdire ces pratiques sous toutes leurs formes¹¹³⁶.

¹¹³² ORDRE DES CONSEILLERS ET CONSEILLÈRES D'ORIENTATION DU QUÉBEC, « Ordre des conseillers et conseillères d'orientation du Québec - OCCOQ », en ligne : <<https://www.orientation.qc.ca/>> (consulté le 31 mars 2026).

¹¹³³ LRSSS, art. 1.

¹¹³⁴ *Id.*, art. 5.

¹¹³⁵ *Id.*, art. 160 par. 3.

¹¹³⁶ Voir vers l'intervention de la députée Michelle Setlakwe : ASSEMBLÉE NATIONALE DU QUÉBEC, « Étude détaillée du projet de loi n° 3 – Loi sur les renseignements de santé et de services sociaux modifiant diverses dispositions législatives », dans *Journal des débats de la Commission des finances publiques*, 47-9, 2023, en ligne : <<https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/cfp-43-1/journal-debats/CFP-230215.html>> (vers 15 h 10).



La Commission est favorable à ce que les organismes du secteur de la santé et des services sociaux ne puissent, en aucune circonstance, vendre ou autrement aliéner des renseignements de santé et de services sociaux. Mais à défaut d'interdire formellement de telles pratiques dans la LRSSS, la Commission constate que les dispositions actuelles peuvent soulever certains questionnements à cet égard.

3.2.1.3. Le consentement en matière de recherche

La LRSSS prévoit que le consentement à l'utilisation ou à la communication d'un renseignement de santé et de services sociaux détenu par un organisme de ce secteur doit être manifeste, libre, éclairé et donné à des fins spécifiques¹¹³⁷. Il est prévu qu'en matière de recherche, le consentement peut viser des « thématiques de recherche, des catégories d'activités de recherche ou des catégories de chercheurs »¹¹³⁸. La Commission constate que ce nouveau concept peut entrer en contradiction avec le critère voulant que le consentement doive être « donné à des fins spécifiques »¹¹³⁹, c'est-à-dire avoir un objet précis et circonscrit.

Également, la Commission se questionne sur la durée de la validité des consentements ainsi donnés. La jurisprudence a toujours exigé une limite dans le temps. Par ailleurs, les lignes directrices de la Commission portant sur les critères de validité du consentement traitent aussi du fait que le consentement doit être temporaire comme étant un des critères de validité du consentement¹¹⁴⁰.

En pratique, pensons aux banques de renseignements qui sont constituées dans le but d'alimenter les recherches futures. La Commission est d'avis que celles-ci soulèvent plusieurs questionnements relativement au consentement. Par exemple, quelles sont les limites de ces banques? La constitution d'une banque pour la recherche sur le cancer pourrait impliquer la conservation des renseignements de santé et de services sociaux pour toujours si l'on conclut que les fins pour lesquelles ces renseignements sont recueillis ne seront jamais atteintes.

Bien qu'elle comprenne toute l'importance de la recherche en matière de santé et de services sociaux, la Commission rappelle que l'utilisation des renseignements des citoyens québécois doit être adéquatement circonscrite.

3.2.1.4. L'absence d'une disposition transitoire concernant les mandats ou les contrats conclus par les organismes du secteur de la santé et des services sociaux issus de la sphère privée

La LRSSS prévoit une disposition transitoire visant les mandats ou les contrats de service ou d'entreprise conclus avant l'entrée en vigueur de la LRSSS par les organismes du secteur de la santé et des services sociaux issus de la sphère publique. En bref, lorsqu'ils prévoient une communication de renseignements de santé et de services sociaux, ces mandats et ces contrats doivent être conclus conformément au régime de la LRSSS au plus tard deux ans après son entrée en vigueur, soit le 1^{er} juillet 2026¹¹⁴¹.

¹¹³⁷ LRSSS, art. 6 al. 1.

¹¹³⁸ *Id.*

¹¹³⁹ *Id.*, art. 6 al. 1.

¹¹⁴⁰ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 486, p. 20.

¹¹⁴¹ À moins d'expirer avant cette date, un mandat ou un contrat de service conclu en vertu de l'article 67.2 de la Loi sur l'accès ou de l'article 27.1 de la LSSSS peut demeurer valide jusqu'à la date qui suit de deux ans celle de l'entrée en vigueur de l'article 77 de la LRSSS, soit le 1^{er} juillet 2024 : LRSSS, art. 261 al. 2.



En revanche, aucune disposition analogue n'existe pour les mandats et les contrats de service ou d'entreprise conclus par les organismes assujettis à la LRSSS issus de la sphère privée, anciennement assujettis uniquement à la Loi sur le privé. Par conséquent, la Commission constate qu'une interprétation possible de cette situation est qu'un mandat ou un contrat conclu avant l'entrée en vigueur de la LRSSS, tel un contrat prévoyant l'hébergement de renseignements de santé et de services sociaux, pourrait demeurer assujetti à la Loi sur le privé indéfiniment en l'absence de modification législative.



3.3. Recommandations

Malgré l'entrée en vigueur relativement récente de la LRSSS, la Commission estime que le gouvernement doit déjà entreprendre une réflexion pour répondre à certains des enjeux soulevés précédemment. Notamment, des actions concrètes sont requises en lien avec la mise en place des systèmes numériques permettant l'application de certaines dispositions de la Loi, et certaines modifications à cette loi devraient être envisagées pour en clarifier l'interprétation.

3.3.1. Accélérer la mise en place d'outils et rendre la journalisation complète obligatoire

Selon la Commission, en théorie, les mesures de protection prévues par la LRSSS semblent adéquates. En revanche, pour être concrètes et efficaces, elles sont fortement tributaires de l'implantation de solutions technologiques supportant leur mise en œuvre. Il semble qu'il aurait été profitable et judicieux que ces solutions technologiques soient mises en place préalablement à la réforme pour assurer la protection des renseignements de santé et de services sociaux concernés. Or, à ce jour, ces solutions sont toujours attendues, ce qui laisse craindre pour le respect des mesures de protection prévues par la LRSSS.

Dans ce contexte, l'insuffisance des technologies actuellement disponibles aux organismes du secteur de la santé et des services sociaux fragilise la protection concrète accordée aux renseignements provenant de ce secteur. Cette situation apparaît problématique et introduit un risque pour les citoyens.

L'infrastructure technologique devrait permettre :

- d'assurer l'identification et l'authentification des intervenants;
- de mettre en place certaines mesures de protection permettant de vérifier qu'une personne est la patiente d'un intervenant;
- de communiquer d'une manière standardisée et sécurisée des renseignements de santé et de services sociaux et d'y permettre l'accès de la même manière par les intervenants autorisés;
- de journaliser les accès aux renseignements de santé et de services sociaux et les utilisations de ceux-ci;
- de savoir qui détient des renseignements de santé et de services sociaux sur une personne et quels domaines ou sujets sont concernés par ces renseignements;
- d'appliquer dûment les restrictions et les refus d'accès exprimés par les personnes concernées.

La Commission insiste particulièrement sur l'importance d'assurer dès maintenant une journalisation complète des accès aux renseignements de santé et de services sociaux et de leurs utilisations. Il s'agit d'un levier essentiel permettant de garantir la transparence envers les personnes concernées en ce qui a trait à la circulation de leurs renseignements, corollaire essentiel des possibilités accrues de circulation prévues par la LRSSS.



Recommandation 65

Rendre applicables les protections prévues à la LRSSS en accélérant la mise en place des outils, des procédures et des infrastructures technologiques requis afin, notamment, d'assurer l'identification et l'authentification des intervenants du secteur de la santé et des services sociaux.

Recommandation 66

Prendre les actions nécessaires afin qu'entre en vigueur l'article 103 de la LRSSS, qui prévoit l'obligation pour un organisme du secteur de la santé et des services sociaux de journaliser l'ensemble des accès aux renseignements de santé et de services sociaux qu'il détient ou de toute autre utilisation ou communication de ces renseignements.

3.3.2. Envisager des modifications législatives pour clarifier l'interprétation de la Loi

En ce qui a trait aux premiers enjeux d'interprétation se profilant en lien avec la LRSSS, la Commission estime que le législateur pourrait apporter certaines modifications afin de permettre de clarifier la Loi.

Premièrement, la notion de « cabinet privé de professionnel » devrait être mieux circonscrite, et des critères supplémentaires devraient être ajoutés à la LRSSS à ce sujet de manière à faciliter l'interprétation de son champ d'application.

Deuxièmement, la Commission invite le législateur à formuler une interdiction claire relative à toute possibilité de monétisation des renseignements par les organismes assujettis à la LRSSS ou par leur intermédiaire. Une telle interdiction devrait empêcher toute forme de participation de ces organismes à la vente ou à l'aliénation d'un renseignement de santé et de services sociaux.

Troisièmement, la Commission suggère de mieux baliser les consentements élargis en matière de recherche, compte tenu des conséquences pratiques de cette nouvelle disposition.

Quatrièmement, il serait souhaitable que la LRSSS prévoie, comme elle le fait pour les organismes publics du secteur de la santé et des services sociaux, des mesures transitoires visant certains contrats des organismes de santé et de services sociaux issus de la sphère privée. Ces contrats ont été conclus avant l'adoption de la LRSSS, suivant donc le régime de la Loi sur le privé, et demeurent en vigueur sans avoir été adaptés au nouveau régime. Ces mesures transitoires viseraient à ce que les mandats et les contrats de service ou d'entreprise concernés respectent, éventuellement, les dispositions de la LRSSS en matière contractuelle. En effet, les protections accordées par la Loi sur le privé sont moins contraignantes que celles de la LRSSS, ce qui milite pour une action à cet égard.



Recommandation 67

Ajouter à la LRSSS des critères permettant de circonscrire la notion de « cabinet privé de professionnel » contenue au paragraphe 1° de l'annexe II de cette Loi afin de mieux définir son champ d'application.

Recommandation 68

Interdire formellement toute possibilité pour les organismes du secteur de la santé et des services sociaux, qu'ils soient publics ou privés, de participer à toute vente ou aliénation d'un renseignement de santé et de services sociaux.

Recommandation 69

Baliser davantage le consentement en matière de recherche dans le domaine de la santé et des services sociaux.

Recommandation 70

Prévoir à la LRSSS une disposition transitoire, inspirée de celle du deuxième alinéa de l'article 261, visant à assurer que les mandats et les contrats de service ou d'entreprise conclus en vertu de la Loi sur le privé avant l'entrée en vigueur de la LRSSS viennent à échéance au terme d'une période de transition déterminée.

CHAPITRE 4

4. La Commission d'accès à l'information



Introduction

Dans une société libre et démocratique, il est essentiel de veiller attentivement au respect du droit à l'information et du droit à la vie privée des citoyens, garantis par la Charte et précisés par des lois quasi constitutionnelles. Au Québec, la Commission joue fièrement ce rôle depuis maintenant plus de 40 ans. Ainsi, depuis sa création, elle agit comme gardienne de ces droits afin de donner vie aux législations que le Québec a adoptées, à travers les années, en matière d'accès à l'information et de protection des renseignements personnels. Elle cumule des fonctions d'adjudication à l'égard des recours liés à l'exercice des droits conférés par les lois, de surveillance du respect par les organisations de leurs obligations et de promotion de ces droits et de ces obligations. La Commission a acquis une expertise indéniable et est reconnue comme une institution spécialisée et indépendante, d'importance névralgique.

La mission de la Commission est d'autant plus importante aujourd'hui, alors que l'activité économique repose de plus en plus sur l'exploitation des renseignements personnels des citoyens. **Dans cette ère de bouleversements, la Commission et les droits qu'elle protège par ses fonctions constituent, plus que jamais, un rempart protecteur pour assurer la solidité de la démocratie et préserver la confiance de la population dans ses institutions.** Rouage important de notre système fondé sur l'équilibre des pouvoirs, la Commission assure le respect des règles applicables en matière d'accès aux documents des organismes publics et de protection des renseignements personnels par l'État et les entreprises.



Les avancées technologiques ont accru les attentes à l'égard de la Commission. On lui en demande sans cesse davantage, vu l'importance des enjeux en cause. La diversité de ses charges et l'accroissement du nombre de situations qui nécessitent son intervention représentent un défi colossal.

Dans ce contexte, il importe que la Commission dispose de tous les moyens qui lui sont nécessaires pour s'acquitter pleinement de l'ensemble de ses fonctions.

Bien qu'elle fasse le maximum avec les ressources actuellement à sa disposition, le nombre croissant de situations où elle est appelée à intervenir rendent indispensable l'augmentation de sa capacité d'agir. La Commission ne manque pas d'idées et aspire à en faire bien davantage.

Dans le présent chapitre, la Commission :

- brosse le portrait de l'état actuel de ses ressources financières et humaines et illustre l'urgence de les revoir à la hausse;
- aborde le renforcement de son indépendance administrative, essentielle à son rôle de gardienne des droits;



- analyse les possibilités d'appel des décisions de sa section juridictionnelle en lien avec l'esprit de célérité et de simplicité propre à la justice administrative;
- traite de la portée des manquements passibles de sanctions administratives pécuniaires;

discute d'accompagnement des entreprises, à la demande du ministre responsable de l'Accès à l'information et de la Protection des renseignements personnels, en dressant le bilan de ses activités en la matière depuis l'adoption de la Loi 25.

4.1. La capacité d'agir de la Commission

4.1.1. Les ressources financières et humaines disponibles

Sommaire

Les ressources financières et humaines de la Commission sont insuffisantes étant donné l'importance de ses mandats et de l'expansion de ses responsabilités ces dernières années. En 2021-2022, avant l'adoption de la Loi 25, elle comptait sur un budget annuel de 8,3 millions de dollars et un effectif autorisé de 73 équivalents temps complet (ETC). En 2026-2027, son budget s'élève à 12,2 millions de dollars, et son effectif autorisé, à 92 ETC.

Bien que les ressources de la Commission aient augmenté avec l'adoption de la Loi 25, le rehaussement octroyé n'a pas été à la hauteur de l'expansion de ses fonctions. De surcroît, aucune nouvelle somme ou ressource ne lui a été accordée en lien avec ses nouvelles responsabilités prévues à la LRSSS et à d'autres lois touchant la protection des renseignements personnels.

4.1.1.1. Contexte

L'importance des rôles d'adjudication, de surveillance et de promotion de la Commission exige des moyens à la hauteur afin de lui permettre de contribuer pleinement à la protection du public. Au fil de son histoire, la Commission a souvent dû composer avec des ressources limitées¹¹⁴², mais avec le contexte actuel et de nouvelles responsabilités, cet enjeu s'aggrave.

Bien qu'elle ait posé de nombreux gestes ces dernières années, dans un souci d'optimiser ses pratiques et de faire des choix stratégiques, et qu'elle livre des services dont la rigueur est saluée, la créativité et la résilience dont la Commission a jusqu'ici fait preuve ne suffisent plus. En effet, elle est confrontée à des responsabilités considérablement accrues tout en faisant face à des restrictions budgétaires limitant sa capacité d'agir. Les réformes des dernières années ont enrichi l'éventail de ses pouvoirs, autant d'outils

¹¹⁴² Voir par exemple diverses mentions de cette situation dans les documents suivants : COMMISSION D'ACCÈS À L'INFORMATION, *Rapport annuel 1986-1987*, Les Publications du Québec, 1987, p. 20; Rapport quinquennal 2002, p. 145-146; COMMISSION D'ACCÈS À L'INFORMATION, *Rapport annuel 2005-2006*, 2006, p. 9; COMMISSION D'ACCÈS À L'INFORMATION, préc., note 152, p. 83-84.



pouvant donner vie aux principes qui les sous-tendent. Cependant, sans ressources adéquates, elle n'est pas en mesure de faire pleinement usage de ces pouvoirs.

Notamment, l'audace dont a fait preuve le Québec dans ses actions législatives récentes en matière de protection des renseignements personnels risque de se limiter à l'énonciation de principes : la loi affirme et suppose qu'un organisme de contrôle veille au grain, mais on ne lui en donne pas pleinement les moyens.

4.1.1.2. Situation actuelle

Les fonctions confiées à la Commission sont variées et nombreuses, et l'amènent à réaliser une foule d'activités ciblant des publics diversifiés. Cette section en donne un aperçu, puis fait état de l'expansion de ses responsabilités légales. Il est question de l'historique récent de ses ressources et de ses efforts constants pour livrer les meilleurs services possibles malgré ses enjeux de financement et d'effectifs.

4.1.1.2.1. La Commission et la portée de ses activités

La Commission est divisée en deux sections : la section juridictionnelle et la section de surveillance¹¹⁴³. Elle est donc à la fois un tribunal administratif et un organisme de surveillance veillant à l'application de la Loi sur l'accès, de la Loi sur le privé et de la LRSSS, lesquelles couvrent tant le secteur public que le secteur privé. Elle voit aussi à la promotion et au respect des droits des citoyens prévus par ces lois¹¹⁴⁴.

4.1.1.2.1.1. Les fonctions de la Commission

La Commission doit ainsi s'acquitter de nombreux mandats, dont les suivants :

- Décider notamment des demandes de révision et d'examen de mécontentement qui lui sont soumises;
- Surveiller l'application des lois ci-dessus, notamment en utilisant ses pouvoirs d'enquête pénale, d'enquête administrative et d'inspection;
- Rendre des ordonnances;
- Promouvoir les droits et les obligations prévus par ces lois;
- Examiner les ententes de communication de renseignements personnels, notamment à des fins d'étude, de recherche ou de production de statistiques;
- Émettre des avis sur les projets de législation ou de développement de systèmes d'information;
- Recevoir des avis concernant les incidents de confidentialité présentant un risque de préjudice sérieux;
- Recevoir des divulgations de systèmes et de banques biométriques.

La Commission se voit attribuer des fonctions supplémentaires dans diverses autres lois, par exemple la *Loi sur les agents d'évaluation du crédit*¹¹⁴⁵, la *Loi autorisant la communication de renseignements personnels aux familles d'enfants autochtones disparus ou décédés à la suite d'une admission en établissement*¹¹⁴⁶, la *Loi favorisant la transformation numérique de l'administration publique*¹¹⁴⁷, la *Loi concernant le cadre juridique des technologies de l'information*¹¹⁴⁸ ou la *Loi sur l'administration fiscale*¹¹⁴⁹.

¹¹⁴³ Loi sur l'accès, art. 103.

¹¹⁴⁴ *Id.*, art. 122.1 al. 2.

¹¹⁴⁵ *Loi sur les agents d'évaluation du crédit*, préc., note 86, art. 24 et 26.

¹¹⁴⁶ *Loi autorisant la communication de renseignements personnels aux familles d'enfants autochtones disparus ou décédés à la suite d'une admission en établissement*, RLRQ, c. C-37.4, art. 8 et 9.

¹¹⁴⁷ *Loi favorisant la transformation numérique de l'administration publique*, préc., note 828, art. 8 à 10.

¹¹⁴⁸ LCCJTI, art. 44 et 45.

¹¹⁴⁹ *Loi sur l'administration fiscale*, préc., note 80, art. 31, 31.1.0.1, 31.1.5 et section VIII.



Elle doit également considérer les règles en matière d'accès à l'information et de protection des renseignements personnels qui se retrouvent dans différentes lois sectorielles.

Les dernières années ont été marquées par plusieurs développements législatifs en matière de protection des renseignements personnels. S'ils sont largement positifs, ceux-ci ont néanmoins entraîné un accroissement sans précédent des responsabilités de la Commission.

4.1.1.2.1.2. *La Loi 25*

Adoptée en 2021 et entrée en vigueur progressivement entre 2021 et 2024, la Loi 25 a introduit certains nouveaux droits et une multitude de nouvelles obligations aux entreprises, aux organismes publics et aux partis politiques concernant notamment :

- la désignation d'un responsable de la protection des renseignements personnels au sein des organisations privées;
- la création, au sein des organismes publics, d'un comité sur l'accès à l'information et la protection des renseignements personnels;
- l'adoption de règles de gouvernance à l'égard de la protection des renseignements personnels;
- la réalisation d'EFVP pour les systèmes technologiques, les ententes de communication de renseignements personnels et la communication de tels renseignements à l'extérieur du Québec;
- le processus à suivre pour les ententes de communication de renseignements personnels sans le consentement des personnes concernées, remplaçant les processus d'autorisation en matière de recherche et de communication de renseignements personnels entre organismes publics;
- une transparence accrue envers les personnes concernées par le biais de politiques de confidentialité rédigées en des termes simples et clairs, mais aussi de nouvelles informations à fournir lors de la collecte;
- la fourniture d'informations concernant toute décision fondée exclusivement sur un traitement automatisé de renseignements personnels et l'offre d'un droit de révision aux personnes concernées;
- les critères de validité pour le consentement concernant le traitement des renseignements personnels, et des exceptions à l'obligation de l'obtenir;
- la configuration de paramètres de confidentialité les plus élevés par défaut et l'activation des technologies d'identification, de localisation et de profilage;
- la destruction ou l'anonymisation des renseignements personnels lorsque leurs finalités sont accomplies;
- la gestion des incidents de confidentialité, en ce qui a trait à la prise de mesures raisonnables pour diminuer les risques en cas d'incident et en éviter de nouveaux, à la transmission d'un avis à la Commission et aux personnes concernées si l'incident présente un risque de préjudice sérieux et à la tenue d'un registre;
- la divulgation obligatoire des banques de caractéristiques ou de mesures biométriques à la Commission au moins 60 jours avant leur mise en service.

La Loi 25 a aussi conféré de nouveaux droits aux personnes concernées, notamment le droit d'exiger dans certaines circonstances la cessation de la diffusion d'un renseignement personnel ou la désindexation d'un hyperlien permettant d'y accéder, le droit d'accéder aux renseignements personnels d'un proche pour motif de deuil et le droit à la portabilité des renseignements personnels.

Divers ajustements aux pouvoirs et aux fonctions de la Commission ont été apportés par la Loi 25. Entre autres, elle peut désormais imposer des sanctions administratives pécuniaires en vertu d'un tout nouveau régime à cet effet; en matière pénale, le montant maximal des amendes a considérablement augmenté.



Elle a également une fonction de sensibilisation plus explicite et une nouvelle fonction d'élaboration de lignes directrices pour faciliter l'application des lois.

Comme en témoignent les paragraphes qui précèdent, la Loi 25 a constitué une réforme majeure en imposant de nombreux changements pour les organisations, mais également, corrélativement, pour la Commission.

4.1.1.2.1.3. La LRSSS

La LRSSS, abordée en détail dans le chapitre 3 du présent rapport, a été adoptée en mars 2023 et est en vigueur depuis le 1^{er} juillet 2024. Elle n'a pas remplacé la Loi sur l'accès ni la Loi sur le privé, mais s'est plutôt superposée à celles-ci pour les organismes qu'elle concerne. Ces derniers doivent appliquer la LRSSS à l'égard des renseignements de santé et de services sociaux, mais également la Loi sur l'accès ou la Loi sur le privé pour les autres renseignements personnels qu'ils détiennent, selon leur secteur (public ou privé).

La LRSSS constitue donc un régime supplémentaire entraînant lui aussi des incidences considérables pour la Commission en élargissant ses responsabilités. Cette loi a ainsi représenté un changement fondamental de philosophie et d'approche concernant les renseignements de santé et de services sociaux, instaurant à la fois un régime de protection particulier et des mesures permettant leur circulation accrue, par exemple pour l'offre de soins ou la recherche. Ce nouveau paradigme requiert une vigilance importante de la part de la Commission. De plus, la LRSSS a élargi la portée de ce que constitue un organisme du secteur de la santé et des services sociaux en y englobant des organismes issus de la sphère privée. Dans les faits, la Commission doit aujourd'hui surveiller la collecte, l'utilisation, la communication, la conservation ainsi que la destruction ou l'anonymisation des renseignements de santé et de services sociaux au sein d'un vaste réseau comptant un nombre colossal d'employés. Avant l'entrée en vigueur de la LRSSS, elle n'était pas explicitement chargée de cette surveillance en ce qui a trait aux dossiers d'usagers des établissements assujettis à la LRSSS¹¹⁵⁰.

L'application de la Loi amène également la Commission à exercer une surveillance accrue des systèmes technologiques qui existent dans le réseau de la santé et des services sociaux, ainsi que de ceux qui devront être déployés pour assurer la conformité. On pense, entre autres, au Dossier santé numérique, un système de grande envergure contenant lui-même plusieurs composantes répondant à diverses fonctions, appelé à être déployé à terme dans l'ensemble des organismes du secteur de la santé et des services sociaux. Au surplus, la Commission devra surveiller, notamment :

- la mise en place des outils permettant la journalisation des communications de renseignements de santé et de services sociaux – à terme, cette journalisation s'étendra à l'accès à ces renseignements et à leur utilisation;
- l'utilisation, par les organismes du secteur de la santé et des services sociaux, de produits et services technologiques certifiés;
- les systèmes permettant l'accès à des renseignements de santé et de services sociaux.

La Commission prévoit que son implication à ce chapitre augmentera nécessairement au fil de l'avancement des chantiers technologiques liés à l'application de la LRSSS. Ces activités de surveillance s'ajoutent à celles qu'elle doit exercer en vertu de la Loi sur l'accès et la Loi sur le privé.

¹¹⁵⁰ LRSSS.



4.1.1.2.1.4. La Loi sur le ministère de l'Éducation, du Loisir et du Sport

En 2023, des modifications apportées à la *Loi sur le ministère de l'Éducation, du Loisir et du Sport*¹¹⁵¹ ont notamment chargé la Commission de surveiller l'application des dispositions relatives au système de dépôt et de communication de renseignements en éducation¹¹⁵². L'utilisation de ce système doit être rigoureusement encadrée. En effet, il est prévu qu'il conserve l'ensemble des renseignements que les organismes scolaires détiennent sur :

- les élèves et les parents depuis 2011, ce qui concerne 3 440 000 personnes;
- le personnel depuis 2016, ce qui concerne 535 000 personnes.

Ce système et ses composantes prévoient notamment l'utilisation de l'**IA** prédictive à des fins de prévention du décrochage scolaire, un cas d'usage exigeant beaucoup de vigilance par rapport à la protection des renseignements personnels.

4.1.1.2.1.5. La LGGRI

Depuis quelques années, la Commission s'est vu confier un rôle de surveillance accru en lien avec de grands projets numériques dans le secteur public, principalement par l'entremise de modifications à la LGGRI survenues entre autres :

- en 2021, en lien avec une volonté de valorisation et de mobilité des données numériques gouvernementales¹¹⁵³;
- en 2025, avec l'adoption d'une loi appuyant la mise en place d'une identité numérique nationale¹¹⁵⁴.

D'une part, en vertu de la LGGRI, un organisme public peut désormais être désigné par le gouvernement pour agir à titre de source officielle de données numériques gouvernementales¹¹⁵⁵. Cette source « recueille, utilise ou communique des données numériques gouvernementales ou recueille auprès de toute personne des renseignements, incluant des renseignements personnels, lorsque cela est nécessaire à une fin administrative ou de services publics ». L'organisme public ainsi désigné devient une plaque tournante en matière de gestion, de mobilité et de valorisation des données numériques gouvernementales. La Commission a pour fonction de recevoir, et donc d'analyser, des EFVP et des règles de gouvernance produites par chaque source officielle¹¹⁵⁶. Il s'agit de documents névralgiques, vu l'ampleur potentielle des flux de données en cause. Annuellement, une source officielle doit transmettre à la Commission un rapport d'activités concernant les renseignements personnels recueillis, utilisés ou communiqués¹¹⁵⁷.

¹¹⁵¹ *Loi modifiant principalement la Loi sur l'instruction publique et édictant la Loi sur l'Institut national d'excellence en éducation*, LQ 2023, c. 32, en ligne : https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2023/2023C32F.PDF.

¹¹⁵² *Loi sur le ministère de l'Éducation, du Loisir et du Sport*, préc., note 829, art. 6.18.

¹¹⁵³ *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*, LQ 2021, c. 22, en ligne : https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2021/2021C22F.PDF.

¹¹⁵⁴ *Loi concernant l'identité numérique nationale et modifiant d'autres dispositions*, LQ 2025, c. 26, en ligne : https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2025/2025C26F.PDF.

¹¹⁵⁵ LGGRI, art. 12.14.

¹¹⁵⁶ *Id.*, art. 12.16.

¹¹⁵⁷ *Id.*, art. 12.17.

D'autre part, les règles de la LGGRI sont conçues pour appuyer le développement de grands projets numériques gouvernementaux; elles servent déjà en vue du projet d'identité numérique nationale¹¹⁵⁸. De tels projets impliquent la collecte, l'utilisation, la communication et la conservation d'un très grand nombre de renseignements personnels. La surveillance proactive et assidue de ces projets par la Commission s'avère donc essentielle pour la protection du public.

4.1.1.2.1.6. La Loi électorale

La *Loi électorale* a été modifiée par la Loi 25 afin que les partis politiques provinciaux, les députés indépendants et les candidats aux élections provinciales soient soumis à certaines règles de protection des renseignements personnels¹¹⁵⁹. Celles-ci sont entrées en vigueur en 2023. En 2025, la Loi a de nouveau été modifiée pour que soit explicitement confiée à la Commission la fonction de surveiller l'application de ce régime particulier¹¹⁶⁰. Cette fonction sera officiellement en vigueur le 1^{er} juillet 2026.

4.1.1.2.1.7. La Loi sur l'Institut de la statistique du Québec

En 2021, puis en 2025, la *Loi sur l'Institut de la statistique du Québec* a été modifiée pour prévoir la possibilité que certains renseignements personnels ou certaines banques de renseignements personnels détenus par des organismes publics soient désignés par le gouvernement afin que l'Institut de la statistique du Québec puisse les détenir, les utiliser et les communiquer à des fins de recherche aux chercheurs liés à un organisme public¹¹⁶¹. L'objectif était de simplifier l'obtention de certains renseignements requis dans le cadre de travaux réalisés par l'Institut ou des chercheurs liés à des organismes publics, tout en assurant leur protection.

Ainsi, la Commission est impliquée de plusieurs manières :

- Elle est généralement consultée quant à toute désignation de renseignements personnels envisagée par le gouvernement en vertu de cette loi, et informée de toute désignation effective¹¹⁶².
- Elle reçoit copie de toute entente conclue entre l'Institut et un chercheur pour permettre à ce dernier d'accéder à des renseignements désignés¹¹⁶³, cette entente étant obligatoire¹¹⁶⁴.
- Elle doit approuver, tous les trois ans, les règles encadrant la gouvernance de l'Institut à l'égard des renseignements personnels désignés¹¹⁶⁵.
- Elle doit surveiller l'application de ces règles par l'ISQ¹¹⁶⁶.

¹¹⁵⁸ *Loi sur le ministère de la Cybersécurité et du Numérique*, RLRQ, c. M-17.1.1, art. 10.6.

¹¹⁵⁹ *Loi électorale*, RLRQ, c. E-3.3, art. 127.22 et 127.23.

¹¹⁶⁰ *Loi modifiant la Loi électorale principalement afin de préserver l'intégrité du processus électoral*, LQ 2025, c. 15, art. 26, en ligne : https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2025/2025C15F.PDF.

¹¹⁶¹ Cette possibilité a été introduite d'abord par la *Loi concernant principalement la mise en œuvre de certaines dispositions du discours sur le budget du 10 mars 2020*, LQ 2021, c. 15, art. 68 et suiv., en ligne : https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2021/2021C15F.PDF; le régime a été légèrement modifié par la *Loi concernant la mise en œuvre de certaines dispositions du discours sur le budget du 25 mars 2025 et modifiant d'autres dispositions*, LQ 2025, c. 32, art. 49 et suiv., en ligne : https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2025/2025C32F.PDF.

¹¹⁶² *Loi sur l'Institut de la statistique du Québec*, préc., note 110, art. 13.1 et 13.1.1.

¹¹⁶³ *Id.*, art. 13.11.

¹¹⁶⁴ *Id.*, art. 13.9.

¹¹⁶⁵ *Id.*, art. 30.3.

¹¹⁶⁶ *Id.*, art. 30.4.



4.1.1.2.1.8. La portée des activités de la Commission

En définitive, les fonctions de la Commission concernent donc, sans compter les particularités de plusieurs autres lois :

- l'ensemble des 9 millions de citoyens du Québec¹¹⁶⁷;
- près de 2 600 organismes publics visés par la Loi sur l'accès, soit :
 - environ 200 ministères et organismes gouvernementaux;
 - environ 1 900 organismes municipaux, intermunicipaux ou supramunicipaux;
 - environ 330 établissements scolaires, y compris les centres de services scolaires, les cégeps, les universités et les établissements privés subventionnés;
 - environ 75 organismes du secteur de la santé et des services sociaux, y compris notamment Santé Québec, des centres d'hébergement et de soins de longue durée et des centres de réadaptation;
 - les 46 ordres professionnels;
- l'ensemble des entreprises visées par la Loi sur le privé, soit celles qui font affaire au Québec et qui traitent des renseignements personnels, dont :
 - au minimum, sur le total de plus de 950 000 entreprises recensées au Québec, les quelque 278 000 d'entre elles qui emploient au moins une personne¹¹⁶⁸ traitant des renseignements personnels;
 - les nombreuses entreprises établies à l'extérieur du Québec qui y exercent néanmoins des activités couvertes par la Loi sur le privé;
- les personnes et entités assujetties, par le truchement de la *Loi électorale*, à certaines des dispositions de la Loi sur le privé, soit :
 - 21 partis politiques provinciaux autorisés¹¹⁶⁹, dont quatre auxquels sont affiliés 116 députés¹¹⁷⁰. À titre informatif, les partis autorisés ont présenté 866 candidats aux élections générales de 2022¹¹⁷¹;
 - 9 députés indépendants¹¹⁷²;
 - les candidats indépendants aux élections. À titre d'exemple, ils étaient 14 aux élections générales de 2022¹¹⁷³;

¹¹⁶⁷ INSTITUT DE LA STATISTIQUE DU QUÉBEC, « Population et composantes de l'accroissement démographique, par année, Québec, 1972-2026 » (18 mars 2026), en ligne : <<https://statistique.quebec.ca/fr/produit/tableau/population-composantes-accroissement-demographique-quebec>> (consulté le 2 avril 2026).

¹¹⁶⁸ INSTITUT DE LA STATISTIQUE DU QUÉBEC, « Nombre d'entreprises actives au Québec » (20 février 2024), en ligne : <<https://statistique.quebec.ca/fr/document/nombre-entreprises-actives-quebec>> (consulté le 2 avril 2026).

¹¹⁶⁹ « Partis politiques », *Élections Québec*, en ligne : <<https://www.electionsquebec.qc.ca/partis-et-autres-entites-politiques/partis-politiques/#provincial>> (consulté le 16 avril 2026).

¹¹⁷⁰ ASSEMBLÉE NATIONALE DU QUÉBEC, « Députés » (1 avril 2026), en ligne : <<https://www.assnat.qc.ca/fr/deputes/index.html>> (consulté le 16 avril 2026).

¹¹⁷¹ ÉLECTIONS QUÉBEC, « Élections générales de 2022 : 880 candidates et candidats sont dans la course! » (17 septembre 2022), en ligne : <<https://www.electionsquebec.qc.ca/communiques/elections-generales-de-2022-880-candidates-et-candidats-sont-dans-la-course/>> (consulté le 16 avril 2026).

¹¹⁷² À la date où s'achève la préparation de ce rapport, l'une de ces députées est affiliée à un parti politique provincial autorisé, mais celui-ci ne constitue pas un groupe parlementaire au sein de l'Assemblée nationale.

¹¹⁷³ ÉLECTIONS QUÉBEC, préc., note 1171.



- l'ensemble des organismes de santé et de services sociaux et des intervenants visés par la LRSSS, représentant par exemple :
 - 1 590 installations détenant un permis d'opération permettant d'offrir des services de santé et de services sociaux¹¹⁷⁴, gérées par 127 établissements¹¹⁷⁵;
 - quelque 328 000 employés œuvrant pour Santé Québec¹¹⁷⁶;
 - environ 1 600 résidences privées pour aînés détenant un certificat de conformité¹¹⁷⁷;
 - plus de 11 500 ressources intermédiaires et ressources de type familial¹¹⁷⁸;
 - des milliers de cliniques privées offrant des services de santé et de services sociaux, comme des cabinets de dentistes, de physiothérapeutes ou d'orthophonistes.

4.1.1.2.2. Le volume de dossiers reçus et traités par la Commission

Les chiffres suivants donnent un aperçu du volume de dossiers que la Commission reçoit et traite chaque année, lesquels ne représentent qu'une partie des activités qu'elle accomplit¹¹⁷⁹ :

Volume de dossiers reçus et traités en 2025-2026 pour certaines catégories d'activités de la Commission

Type de dossier	Volume reçu en 2025-2026	Volume traité en 2025-2026
Recours à la section juridictionnelle	4 214 ¹¹⁸⁰	3 188 ¹¹⁸¹
Plaintes	970	572
Avis d'incident de confidentialité	579	504
Divulgations de biométrie	84	70
Ententes de recherche	1 301	1 327 ¹¹⁸²

¹¹⁷⁴ MINISTÈRE DE LA SANTÉ ET DES SERVICES SOCIAUX, « Installations : Lieux physiques » (14 avril 2026), en ligne : <<https://m02.pub.msss.rtss.qc.ca/M02ListeInstall.asp>> (consulté le 14 avril 2026).

¹¹⁷⁵ MINISTÈRE DE LA SANTÉ ET DES SERVICES SOCIAUX, « Établissements : Entités légales » (14 avril 2026), en ligne : <<https://m02.pub.msss.rtss.qc.ca/M02ListeEtab.asp>> (consulté le 14 avril 2026). Il est important de noter que ces établissements sont majoritairement des établissements privés ou des établissements de Santé Québec.

¹¹⁷⁶ SANTÉ QUÉBEC, *Rapport annuel de gestion 2024-2025*, 2025, p. 2, en ligne : <<https://sante.quebec/inc/documents/sante-quebec-rapport-annuel.pdf>>.

¹¹⁷⁷ Ce chiffre est extrait en date du 14 avril 2026 du registre suivant : MINISTÈRE DE LA SANTÉ ET DES SERVICES SOCIAUX, « Registre des résidences pour personnes âgées », en ligne : <<http://k10.pub.msss.rtss.qc.ca/K10accueil.asp>> (consulté le 14 avril 2026).

¹¹⁷⁸ MINISTÈRE DE LA SANTÉ ET DES SERVICES SOCIAUX, *Étude des crédits 2025-2026 - Réponses aux questions particulières du deuxième groupe d'opposition*, 2025, en ligne : <https://www.assnat.qc.ca/Media/Process.aspx?Mediald=ANQ.Vigie.BII.DocumentGenerique_210853>, réponse MSSS-2RP-142.

¹¹⁷⁹ Par exemple, les activités de promotion; à cet effet, pour un aperçu, voir la section 4.4

¹¹⁸⁰ Il s'agit d'une estimation, la compilation finale n'étant pas achevée à la date de finalisation de ce rapport. Ce volume inclut environ 550 demandes d'autorisation de ne pas tenir compte qui sont liées entre elles.

¹¹⁸¹ Il s'agit d'une estimation, la compilation finale n'étant pas achevée à la date de finalisation de ce rapport.

¹¹⁸² Il faut noter qu'au cours d'un exercice financier, la Commission traite des ententes reçues vers la fin de l'exercice financier précédent.



Les dossiers reçus par la Commission ont cru significativement dans les dernières années, notamment par l'effet de la Loi 25. Entre 2021-2022 et 2025-2026, on peut par exemple noter les hausses présentées dans le tableau suivant.

Croissance entre 2021-2022 et 2025-2026 de certains types de dossiers reçus par la Commission

Indicateur	Progression entre 2021-2022 et 2025-2026
Avis d'incidents de confidentialité	+ 642 %
Divulgations de biométrie	+ 147 %
Plaintes	+ 477 %
Ententes de recherche	+ 1 431 %
Recours à la section juridictionnelle	+ 89 % ¹¹⁸³

4.1.1.2.3. L'état des ressources de la Commission

Pour 2026-2027, la Commission peut compter sur 92 ETC¹¹⁸⁴ et un budget annuel de 12,2 millions de dollars afin de s'acquitter de l'ensemble de ses fonctions¹¹⁸⁵. Les paragraphes suivants présentent certains éléments d'historique importants par rapport à ces ressources.

En 2021-2022, la Commission a compté sur un budget de 8,3 millions de dollars et un effectif autorisé de 73 ETC¹¹⁸⁶. À l'aube de cet exercice financier, en mars 2021, elle a réalisé dans la foulée de la Loi 25 une évaluation approfondie de sa situation, en tenant compte de diverses variables : sa capacité de traitement des demandes, le nombre de dossiers en attente, la hausse prévisible du nombre de nouvelles demandes en lien avec la réforme, le niveau de service visé et les nouvelles fonctions lui étant attribuées.

Cette évaluation a amené la Commission à demander, en octobre 2021, un financement additionnel récurrent de 13 millions de dollars par année, correspondant à une hausse de 113 ETC, afin notamment :

- d'accroître ses activités de prévention et de sensibilisation en matière de conformité des pratiques;
- de développer son expertise technologique et ses activités de veille des enjeux émergents dans une société numérique et un contexte de mondialisation;
- d'adapter ses activités en fonction de la Loi 25 par l'élaboration de nouveaux processus et la révision des processus existants, de même que par le développement d'un grand nombre d'outils et de mesures d'accompagnement;

¹¹⁸³ Il s'agit d'une estimation, la compilation finale des demandes reçues en 2025-2026 n'étant pas achevée à la date de finalisation de ce rapport.

¹¹⁸⁴ Cette unité de mesure utilisée pour faciliter les comparaisons d'effectifs correspond à la rémunération annuelle d'un employé à temps plein pour une durée de 1826,3 heures.

¹¹⁸⁵ GOUVERNEMENT DU QUÉBEC, *Crédits et dépenses des portefeuilles 2026-2027*, Budget de dépenses 2026-2027, volume 3, 2026, p. 4-1, en ligne : <https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/secretariat-du-conseil-du-tresor/publications-adm/budgets/2026-2027/3_credits_depenses_portefeuilles.pdf>.

¹¹⁸⁶ COMMISSION D'ACCÈS À L'INFORMATION, *Rapport annuel de gestion 2021-2022*, 2022, p. 74 et 80, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_RAAG_2021-2022.pdf>.



- de réduire les délais de traitement des demandes adressées aux deux sections de la Commission, en particulier dans le contexte de leur tendance à la hausse et de la prévisibilité d'une nouvelle augmentation dans le contexte de la réforme;
- de mener à bien divers projets de transformation numérique et ainsi de proposer des services plus accessibles et d'améliorer ses outils de travail.

Le gouvernement a invité la Commission à revoir cette demande à la baisse, invoquant notamment le contexte économique. En décembre 2021, elle a donc formulé une demande révisée visant plutôt l'ajout récurrent de 9,1 millions de dollars au budget annuel, correspondant à une hausse de 79 ETC. Pour abaisser le montant demandé, la Commission s'est ainsi concentrée sur les besoins les plus pressants en lien avec la mise en œuvre des nouveautés apportées par la Loi 25. Elle notait néanmoins que cette demande révisée ne permettrait pas, entre autres :

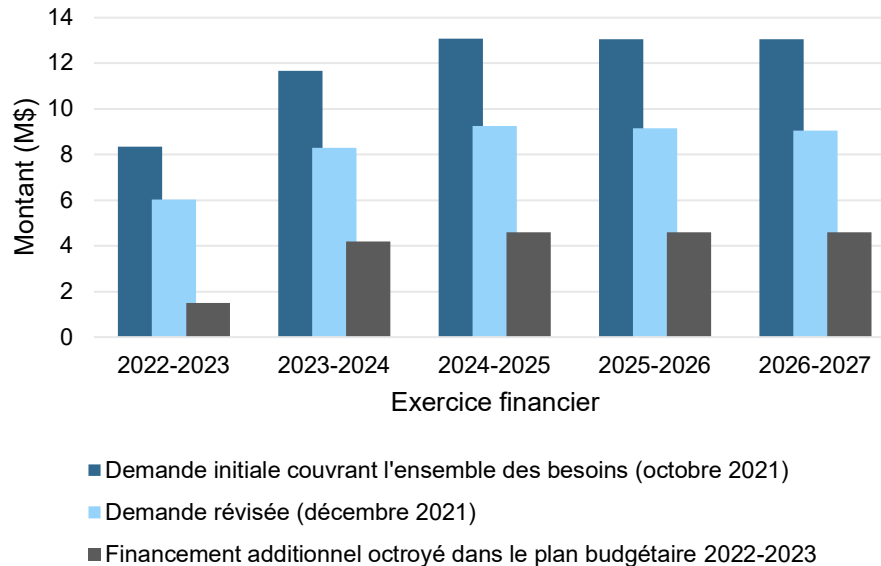
- d'ajouter certains postes en vue d'améliorer les délais de la section juridictionnelle de la Commission;
- de revoir la structure organisationnelle, avec pour effet de maintenir une surcharge pour les gestionnaires en place;
- d'augmenter significativement la capacité de la Commission à offrir de l'accompagnement aux organisations;
- d'augmenter significativement le nombre de postes liés à l'expertise technologique de la Commission.

Dans le plan budgétaire de 2022-2023¹¹⁸⁷, le gouvernement a finalement octroyé à la Commission un rehaussement budgétaire correspondant, à terme, à une augmentation récurrente de 4,6 millions de dollars de son budget annuel et à l'autorisation de pourvoir 40 ETC supplémentaires.

Pour synthétiser, le graphique suivant compare le financement additionnel initialement demandé par la Commission en 2021, celui demandé en 2022 à la suite d'un ajustement suggéré par le gouvernement, et celui octroyé dans le plan budgétaire 2022-2023. Comme on le constate, les crédits supplémentaires obtenus à l'époque correspondent environ au tiers de la demande initiale et à la moitié de la demande révisée.

¹¹⁸⁷ MINISTÈRE DES FINANCES DU QUÉBEC, *Budget 2022-2023 - Plan budgétaire*, 2022, p. G.50, en ligne : https://www.budget.finances.gouv.qc.ca/budget/2022-2023/documents/Budget2223_PlanBudgetaire.pdf.

Financement additionnel annuel demandé et obtenu par rapport à l'année 2021-2022¹¹⁸⁸



Il importe de souligner que le financement additionnel demandé par la Commission en 2021, puis octroyé en 2022-2023, ne tient pas compte des autres lois adoptées ou modifiées à la suite de la Loi 25, malgré leur incidence marquée sur ses fonctions, évoquée dans la section 4.1.1.2.1. En particulier, l'adoption de la LRSSS a ajouté une troisième loi à celles dont la Commission doit surveiller l'application, avec des effets majeurs sur l'ampleur des activités qu'elle doit mener, sur la revue de ses processus au sein de ses deux sections, juridictionnelle et de surveillance, et sur les activités de promotion à mettre en œuvre pour faire connaître ce nouveau cadre législatif.

Dans son mémoire sur le projet de loi ayant mené à la LRSSS, la Commission avait soulevé la nécessité de tenir compte de cette nouvelle loi et de ses effets dans la détermination de son budget¹¹⁸⁹. D'autres intervenants avaient souligné cette préoccupation, comme le Barreau du Québec¹¹⁹⁰.

En définitive, aucune ressource supplémentaire n'a été allouée à la Commission pour l'application de la LRSSS ni pour celle des autres lois ayant étendu ses fonctions, en sus de la Loi 25.

Notons qu'à l'aube de l'année financière 2025-2026, la Commission comptait sur un effectif autorisé total de 113 ETC. Or des mesures de restriction budgétaire instaurées dans la fonction publique dès l'automne 2024 se sont accompagnées, au cours de cet exercice, d'une réduction de 19 % de l'effectif autorisé de la Commission en mai 2025, pour une cible de 94 au 31 mars 2026. En fin de compte, au 31 mars 2027, la Commission devra respecter une nouvelle cible de 92 ETC. Conséquemment, son

¹¹⁸⁸ Il est important de noter que les chiffres présentés pour 2026-2027 ne tiennent pas compte des mesures de restriction budgétaires.

¹¹⁸⁹ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 1071, p. 72.

¹¹⁹⁰ « En revanche, nous ne pouvons cacher nos préoccupations réelles quant au niveau de financement requis pour s'assurer que cela puisse se réaliser sur le terrain. Il faut qu'un budget suffisant soit octroyé par le gouvernement pour permettre à la CAI de remplir son mandat. » : BARREAU DU QUÉBEC, *Commentaires et observations du Barreau du Québec - Projet de loi n° 3 — Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives*, 2023, p. 7-8, en ligne : <<https://www.barreau.qc.ca/media/kgodmtpc/memoire-pl-3.pdf>>.

budget de rémunération a également été réduit de 750 000 \$. Malgré toute l'ampleur des évolutions législatives citées précédemment, son effectif autorisé a augmenté, au net, de 19 ETC entre 2021-2022 et 2026-2027, et son budget, de 3,9 millions de dollars annuellement.

En synthèse, si des ressources additionnelles octroyées en lien avec la Loi 25 ont pu contribuer, dans une certaine mesure, à soutenir les actions de la Commission, elles sont demeurées largement insuffisantes par rapport au poids de ses nouvelles responsabilités. Dans l'éventualité de nouvelles compressions, il sera nécessaire de redéfinir la mission confiée à la Commission.

4.1.1.2.4. Les efforts de la Commission pour s'acquitter au mieux de ses mandats

Malgré la situation de ses ressources financières et humaines, la Commission a multiplié les efforts afin d'optimiser ses services. Elle a atténué ses contraintes, a accru son efficience et a simplifié l'accès à ses services aux citoyens, aux entreprises privées et aux organismes publics. Dès le début de l'année 2025, elle a procédé à des évaluations organisationnelle et technologique exhaustives, de manière à notamment optimiser sa capacité à répondre aux nombreux nouveaux mandats qui lui sont confiés.

Dans la foulée de ces évaluations, la Commission a amorcé une révision complète de ses méthodes de travail. Elle a également lancé diverses initiatives pour favoriser l'accès à la justice et rendre ses services plus efficaces. Par exemple :

- elle a institué un formulaire unique¹¹⁹¹. Il s'agit d'un point d'entrée centralisé et dynamique permettant de soumettre une demande à la Commission. Le formulaire s'adapte aux réponses fournies par l'utilisateur, un citoyen ou une organisation par exemple, pour l'orienter vers le bon endroit, à travers une seule interface. Le formulaire unique simplifie et facilite l'accès aux services de la Commission.
- elle a mis en place un processus de gestion hâtive à la section juridictionnelle, présenté plus en détail dans la section 1.2.3.3.1.3, contribuant à diminuer le délai de traitement des dossiers.

En outre, comme en fait état la section 4.4, la Commission a poursuivi le développement et la mise à jour d'informations vulgarisées, de guides et d'outils pour mieux soutenir les entreprises québécoises, à la mesure de ses capacités. De plus, elle a établi des partenariats avec divers regroupements du secteur privé afin d'améliorer la promotion en lien avec la Loi sur le privé. Cette approche de partenariat se reflète également dans des liens que la Commission souhaite établir progressivement avec des acteurs du milieu de la recherche. Par exemple, elle a récemment participé au lancement d'une chaire de recherche du Canada. Elle s'affiche aussi dans les liens qu'elle entretient entre autres avec l'Association des professionnels en accès à l'information et en protection des renseignements personnels (AAPPI) pour la mise en œuvre de la Loi sur l'accès.

En matière d'application de la loi et de diffusion d'orientations, la Commission a également misé sur la collaboration, affichant sa volonté d'intensifier et de formaliser des partenariats avec d'autres autorités de protection des renseignements personnels, notamment avec ses homologues de la Colombie-Britannique, de l'Alberta et de l'Ontario, de même qu'avec le Commissariat à la protection de la vie privée du Canada. Cette approche lui permet d'accroître sa capacité à assurer que les renseignements personnels des citoyens sont adéquatement protégés, de contribuer à une meilleure concertation dans l'application des lois et d'offrir une plus grande prévisibilité aux entreprises. Ces collaborations lui donnent l'occasion d'exprimer avec ses homologues des messages conjoints et convergents, ce qui en accentue la portée et l'impact. Dans le cadre de ces activités, la Commission agit comme ambassadrice assurant le

¹¹⁹¹ COMMISSION D'ACCÈS À L'INFORMATION, « Comment pouvons-nous vous aider? », en ligne : <<https://formulaire.cai.gouv.qc.ca/>> (consulté le 2 avril 2026).

rayonnement du Québec et de ses législations, en particulier en matière de protection des renseignements personnels, qui constituent une source d'inspiration pour d'autres juridictions.

4.1.1.3. Enjeux

Bien que la Commission rivalise d'initiative et de résilience pour s'acquitter de sa mission le mieux et le plus largement possible, l'insuffisance de ses ressources financières et humaines reste majeure et freine sa capacité. Ses efforts d'optimisation des dernières années ne suffisent plus. Dans ce contexte, l'écart entre les textes de loi et leur mise en application complète tend à se creuser, entraînant des conséquences directes pour les citoyens et l'économie du Québec.

4.1.1.3.1. L'écart entre les textes de loi et leur mise en application complète se creuse

La concrétisation des réformes touchant la protection des renseignements personnels est en grande partie conditionnelle à la capacité de la Commission d'assurer les activités juridictionnelles, de surveillance et de promotion qui en découlent. À l'heure actuelle, elle ne dispose pas de ressources conséquentes avec l'ensemble de ces responsabilités, notamment en lien avec la réalité de l'environnement numérique contemporain.

Premièrement, en matière d'application de la LRSSS, la Commission n'a d'autre choix que de souligner la possibilité que sans moyens supplémentaires, elle soit confrontée à des choix déchirants. Comme il est impensable de sacrifier la qualité de ses interventions, elle pourrait devoir se résoudre à en limiter la quantité. Ses ressources actuelles limitent ainsi les actions qu'elle peut mener pour informer la population, les intervenants et les organismes du secteur de la santé et des services sociaux, ou encore ses activités de surveillance pouvant mener à des recommandations et à des ordonnances.

Les activités de sa section juridictionnelle sont aussi affectées. Alors qu'un usager pouvait auparavant aussi s'adresser à la Cour supérieure, à la Cour du Québec ou au Tribunal administratif du Québec pour contester la décision d'un établissement de santé en matière d'accès aux renseignements contenus dans son dossier, la Commission constitue désormais le seul forum vers lequel il peut se tourner en pareil cas. L'augmentation des demandes qui découlent de l'entrée en vigueur de la LRSSS laisse également anticiper des cas plus nombreux et plus complexes que les membres de la Commission devront trancher.

Deuxièmement, suivant les changements législatifs évoqués à la section 4.1.1.2.1, près d'une dizaine de lois impliquent désormais l'obligation de transmettre des règles de gouvernance, des ententes, des évaluations ou des avis à la Commission. L'attente exprimée par ces législations est que, en tant qu'autorité de surveillance, elle examine ces documents et utilise ses pouvoirs de surveillance lorsque certaines pratiques lui semblent le justifier. Compte tenu de l'ampleur des enjeux en cause en matière de protection des renseignements personnels, de la complexité des grands projets gouvernementaux qui lui sont soumis et du volume de la documentation à examiner, comme l'illustre en partie la section 4.1.1.2.2, l'étude de l'ensemble de ces dossiers en profondeur et dans de courts délais¹¹⁹² constitue un défi de taille pour la Commission.

¹¹⁹² Par exemple, diverses dispositions prévoient la conclusion d'ententes de communication de renseignements personnels sans le consentement des personnes concernées entre organismes ou entre organismes et chercheurs; celles-ci sont transmises à la Commission et entrent en vigueur 30 jours après leur réception, ce qui laisse une courte fenêtre temporelle pour exercer tout pouvoir de surveillance éventuellement requis par la situation : Loi sur l'accès, art. 64, 67.2.3, 68; Loi sur le privé, art. 21.0.2; les ententes similaires établies en vertu de la LRSSS sont transmises à la Commission, mais aucun délai d'entrée en vigueur n'est



Troisièmement, en tant qu'autorité de surveillance, la Commission doit pouvoir maintenir un niveau d'expertise élevé en matière technologique, puisque la protection des renseignements personnels et les enjeux du numérique sont indissociables. La biométrie, la vidéosurveillance, la géolocalisation, le profilage, la cybersécurité, l'IA, les technologies quantiques et les objets connectés sont autant d'enjeux qui auront des effets majeurs sur les citoyens et la protection de leurs renseignements personnels. Ils requièrent que la Commission s'y penche de façon approfondie, mais des travaux de recherche et d'analyse incontournables sont ralentis en raison d'un manque criant de ressources. Cette situation peut également influencer sur l'ampleur de l'apport que peut fournir la Commission quant au rayonnement du Québec, notamment dans ses collaborations à l'échelle pancanadienne. La Commission devrait être en mesure d'y contribuer à la hauteur de l'importance du Québec dans la fédération canadienne.

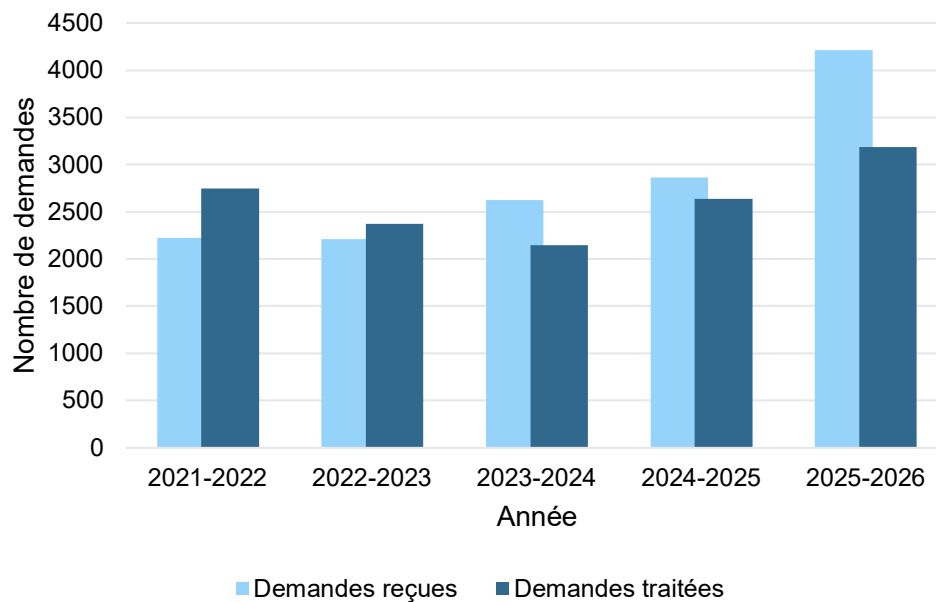
Cette question d'expertise a aussi d'autres ramifications. Le rôle-conseil attendu d'une autorité spécialisée comme la Commission est ainsi de plus en plus difficile à concilier avec les ressources qui lui sont allouées, alors que de nombreux enjeux technologiques et géopolitiques nécessitent plus que jamais une vigilance accrue de sa part. Pour ne prendre qu'un exemple, la progression de la part des inférences algorithmiques dans les activités des organisations, évoquée dans la section 2.1.3, peut entraîner des conséquences particulièrement concrètes dans des secteurs comme la finance et l'assurance ou lorsque ces inférences appuient des décisions de l'administration publique, notamment en matière d'aide de dernier recours ou de répression du crime. Dans ce contexte incertain, mais également très mouvementé, les Québécois doivent pouvoir compter sur une autorité de contrôle disposant de l'expertise nécessaire pour s'attaquer aux enjeux.

Quatrièmement, au Québec, chaque citoyen peut demander l'accès à des documents détenus par un organisme public, ou encore aux renseignements personnels qui le concernent détenus par une organisation publique ou privée. D'autres droits peuvent aussi être exercés auprès des organisations¹¹⁹³. La section juridictionnelle de la Commission est là pour entendre leurs recours. Toutefois, le nombre de ces recours a connu une hausse sans précédent au cours des dernières années, comme l'illustre le graphique suivant.

prévu, impliquant un examen nécessairement rétrospectif; autre exemple, les banques de caractéristiques et de mesures biométriques doivent être divulguées à la Commission 60 jours avant leur mise en service, un autre délai relativement court compte tenu du nombre de telles divulgations reçues annuellement : LCCJTI, art. 45.

¹¹⁹³ Comme le droit à la rectification, le droit à la portabilité ou, dans le secteur privé, le droit à la cessation de diffusion d'un renseignement personnel ou à la désindexation d'un hyperlien y étant rattaché.

Évolution du nombre de demandes reçues et traitées par la section juridictionnelle entre 2021-2022 et 2025-2026¹¹⁹⁴



Si la Commission met tout en œuvre et innove, comme mentionné précédemment, pour gérer adéquatement cet afflux de dossiers et parvenir le plus rapidement possible à offrir une solution aux litiges qui lui sont soumis, il y a une limite au fait d'accomplir plus avec moins. La progression des dossiers reçus alors que les ressources ne sont pas ajustées en conséquence peut avoir pour effet de restreindre l'exercice des droits des citoyens.

4.1.1.3.2. Le manque de ressources de la Commission entraîne des conséquences sur l'économie

En raison des limites de son budget et de ses effectifs, la Commission est aujourd'hui forcée de prioriser ses priorités : elle se voit contrainte, progressivement, de faire des choix de plus en plus délicats.

Cette situation limite grandement ses actions et entraîne donc des conséquences directes pour l'économie.

Par exemple, afin de contribuer au maintien d'un environnement d'affaires favorable et sécuritaire au Québec, la Commission agit au mieux pour accompagner les entreprises au respect de leurs obligations. Elle intervient quotidiennement en sensibilisation et en prévention. Mais comme mentionné à la section 4.4, la Commission ne peut accélérer la cadence.

Pourtant, les besoins sont encore très grands, alors que les renseignements personnels sont devenus le ciment de presque toutes les activités économiques et un facteur majeur dans le potentiel de développement d'une part non négligeable des entreprises et des organismes publics québécois. Les risques découlant d'une gestion inadéquate de ces renseignements sont d'ailleurs croissants dans le contexte économique et géopolitique actuel.

¹¹⁹⁴ Pour 2025-2026, il s'agit d'une estimation, la compilation finale n'étant pas achevée à la date de finalisation de ce rapport. Le nombre de demandes reçues inclut environ 550 demandes d'autorisation de ne pas tenir compte qui sont liées entre elles.



À titre illustratif, il ne se passe pratiquement plus une journée sans qu'on apprenne dans les nouvelles qu'une entreprise a fait l'objet d'un incident de confidentialité. Au-delà de l'atteinte même à leur vie privée à la suite d'un tel incident, les personnes concernées se voient souvent exposées à des risques accrus de fraude et de vol d'identité, qui peuvent entraîner des conséquences financières majeures. Par ailleurs, les risques liés à la sécurité des renseignements personnels dus à une non-conformité aux lois ou à un incident peuvent engendrer des coûts financiers et réputationnels élevés et accaparer des ressources considérables au sein des organisations. À terme, ils peuvent entraîner des effets défavorables sur la croissance économique de plusieurs secteurs d'activité ainsi que sur la création d'emplois, l'investissement, l'innovation et la compétitivité du Québec.

4.1.1.4. Recommandation

Les éléments relevés ci-haut par la Commission mènent à des constats importants pour la protection des droits à l'information et à la vie privée. Alors que la Commission se voit chargée de trancher des litiges en matière d'accès aux documents et d'exercice par les personnes concernées de droits liés aux renseignements personnels, ou encore de prévenir des infractions et des risques de mauvaise gestion des renseignements personnels des citoyens, ses ressources financières et humaines actuelles sont insuffisantes compte tenu des besoins de la société québécoise.

En mai 2022, l'Assemblée nationale, dans une motion adoptée à l'unanimité, a demandé au gouvernement « d'accorder des ressources suffisantes à la Commission d'accès à l'information du Québec pour mener à bien sa mission¹¹⁹⁵ ».

La Commission recommande aujourd'hui la même chose. Ses ressources devraient entre autres lui offrir une certaine prévisibilité des moyens dont elle dispose pour accomplir pleinement sa mission.

Recommandation 71

Octroyer à la Commission le budget et les effectifs requis pour qu'elle remplisse pleinement et efficacement sa mission, compte tenu notamment de :

- l'importance des droits qu'elle protège;
- l'ampleur, de la variété et de l'expansion récente de ses fonctions;
- l'évolution rapide du contexte technologique.

¹¹⁹⁵ ASSEMBLÉE NATIONALE DU QUÉBEC, préc., note 8.



4.1.1. L'indépendance administrative

Sommaire

La Commission exerce d'importantes fonctions l'amenant à entendre des litiges impliquant le gouvernement et à surveiller les pratiques des pouvoirs publics. Or son budget est rattaché au portefeuille du ministre du Conseil exécutif. Conjointement avec ses effectifs autorisés, il est déterminé par le Conseil du trésor, relevant du pouvoir exécutif. Cette situation fragilise l'indépendance administrative de la Commission.

Afin de garantir cette indépendance et de la protéger de tout potentiel d'ingérence ou de représailles, la Commission recommande que son budget et son niveau d'effectifs autorisés relèvent du Bureau de l'Assemblée nationale du Québec.

4.1.1.1. Contexte

Les fonctions de tribunal administratif et d'organisme de surveillance de la Commission requièrent qu'elle puisse agir en toute indépendance. Cette caractéristique était déjà jugée incontournable dès les travaux de la Commission Paré, lesquels ont mené à l'adoption de la Loi sur l'accès¹¹⁹⁶ :

Notre tradition politique n'accepte pas que les pouvoirs publics soient à la fois juge et partie. L'organisme de contrôle et de surveillance de l'accès aux documents et de la protection des renseignements personnels, chargé d'arbitrer les conflits entre les citoyens et les administrations, devra présenter de rigoureuses garanties d'indépendance. Nommé par l'État, il sera cependant autonome.

Cette indépendance est par ailleurs reconnue sur la scène internationale comme étant un principe cardinal pour les autorités de contrôle, tant en matière d'accès aux documents¹¹⁹⁷ qu'en matière de protection des renseignements personnels¹¹⁹⁸.

L'indépendance de la Commission dépend de plusieurs éléments liés à la nomination de ses membres, mais aussi à son autonomie administrative. À cet égard, si des garanties existent dans le premier cas, la Commission craint que l'insuffisance et l'instabilité des ressources évoquées précédemment ne fragilisent son indépendance, et estime qu'il faut agir pour éviter ce risque.

¹¹⁹⁶ COMMISSION D'ÉTUDE SUR L'ACCÈS DU CITOYEN À L'INFORMATION GOUVERNEMENTALE ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, préc., note 1, p. 10.

¹¹⁹⁷ Voir notamment le huitième principe de la plus récente déclaration de principes de la Conférence internationale des commissaires à l'information en 2025 : CONFÉRENCE INTERNATIONALE DES COMMISSAIRES À L'INFORMATION, *The Berlin Principles on the Protection and Promotion of Access to Information Commissioners*, Berlin, 2025, en ligne : <<https://information-commissioners.org/wp-content/uploads/2025/08/THE-BERLIN-PRINCIPLES-ON-THE-PROTECTION-AND-PROMOTION-OF-ACCESS-TO-INFORMATION-COMMISSIONERS.pdf>>.

¹¹⁹⁸ Voir par exemple CONSEIL DE L'EUROPE, *Convention 108+ pour la protection des personnes à l'égard du traitement des données à caractère personnel*, 2018, en ligne : <<https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726>>, article 15, paragraphe 5.

4.1.1.2. Situation actuelle

Comme le soutenait la Commission Paré en 1981, la nomination des membres de la Commission par une majorité aux deux tiers de l'Assemblée nationale¹¹⁹⁹ restreint la probabilité qu'une désignation par le pouvoir exécutif soit source de conflit d'intérêts¹²⁰⁰. En effet, les membres sont appelés à réviser des décisions prises par des organismes publics et à donner des avis sur des projets gouvernementaux. Ce mécanisme d'approbation aux deux tiers des voix prévaut également pour toute destitution¹²⁰¹. Il distingue la Commission des autres tribunaux administratifs et révèle l'importance des deux grands volets de sa mission. Il constitue une garantie procédurale efficace assurant que les décisions des membres ne soient pas influencées par la crainte de voir leur mandat prendre fin abruptement.

Administrativement, la Commission se rapporte au ministre responsable de l'Accès à l'information et de la Protection des renseignements personnels. C'est par lui que transite sa reddition de comptes, alors qu'elle lui transmet par exemple son rapport annuel d'activités et de gestion¹²⁰² ou certaines informations qu'il demande¹²⁰³. Le ministre ne dispose d'aucun pouvoir décisionnel direct à l'égard de la Commission, mais peut lui soumettre des sujets qu'il souhaite voir aborder dans ses rapports ou divers projets pour avis¹²⁰⁴.

Aux plans du budget et de la gestion, la Commission est rattachée au ministère du Conseil exécutif. Ses crédits budgétaires sont octroyés par cette entité, après avoir été déterminés par le Conseil du trésor.

4.1.1.3. Enjeux

Même si l'indépendance décisionnelle de la Commission est reconnue, il subsiste des préoccupations quant à son indépendance administrative. Celle-ci concerne son financement, mais aussi son assujettissement à des mesures administratives générales pouvant être imposées par le gouvernement à l'ensemble de la fonction publique, comme des restrictions portant sur les heures supplémentaires, les déplacements ou encore l'embauche.

À l'heure actuelle, la Commission doit présenter ses demandes budgétaires à un membre du Conseil exécutif alors même qu'elle surveille les agissements du gouvernement. L'exercice d'octroyer les budgets à un organisme comme la Commission peut être complexe et délicat pour le gouvernement. Il doit le faire en prenant garde de ne pas donner l'apparence de vouloir museler ou affaiblir un organisme qui a notamment pour fonction de veiller à la transparence de l'État et au respect des règles de protection des renseignements personnels par les organismes publics. C'est d'ailleurs pour éviter ce genre de situation qu'il ne détermine pas le budget et les effectifs de certaines entités comme les personnes désignées, évoquées ci-dessous.

4.1.1.4. Recommandation

Du point de vue de la Commission, il importe que son budget et ses effectifs soient pérennisés et protégés des aléas des décisions exécutives, au service de son indépendance administrative et de son autonomie

¹¹⁹⁹ Loi sur l'accès, art. 104.

¹²⁰⁰ COMMISSION D'ÉTUDE SUR L'ACCÈS DU CITOYEN À L'INFORMATION GOUVERNEMENTALE ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, préc., note 1, p. 81-82.

¹²⁰¹ Loi sur l'accès, art. 107.

¹²⁰² *Id.*, art. 118.

¹²⁰³ *Id.*, art. 120.

¹²⁰⁴ *Id.*, art. 118, 174 et 179.

financière. Pour ce faire, elle préconise de faire en sorte qu'elle soit complètement rattachée à l'Assemblée nationale. Elle évoquait déjà cette piste dans son rapport quinquennal de 2002¹²⁰⁵.

Suivant ce modèle, la Commission ne serait plus soumise aux mesures administratives pouvant actuellement affecter son indépendance. En outre, elle préparerait elle-même ses prévisions budgétaires annuelles et les soumettrait au Bureau de l'Assemblée nationale en vue de leur approbation.

Cette modification rendrait le fonctionnement de la Commission comparable à celui d'autres importants organismes de protection des droits et de vérification de l'administration publique¹²⁰⁶ dont les dirigeants sont eux aussi nommés par un vote aux deux tiers de l'Assemblée nationale, comme :

- le Protecteur du citoyen;
- le Vérificateur général;
- le Directeur général des élections;
- le Commissaire au lobbyisme;
- le Commissaire à l'éthique et à la déontologie;
- le Commissaire à la langue française;
- le Commissaire au bien-être et aux droits des enfants.

Dans le reste du Canada, des homologues dotés d'une mission semblable à celle de la Commission sont également rattachés à l'organe législatif de leur territoire respectif. C'est le cas notamment pour les commissaires à l'information et à la vie privée de l'Ontario¹²⁰⁷, de la Colombie-Britannique¹²⁰⁸, du Manitoba¹²⁰⁹, du Nunavut¹²¹⁰ et, à la suite d'un changement récent, de la Nouvelle-Écosse¹²¹¹, qui sont des officiers du parlement.

Dans plusieurs provinces et territoires, le commissaire voit son budget étudié et approuvé (avec ou sans modifications) par un comité multipartite du parlement qui exerce un rôle analogue à celui du Bureau de

¹²⁰⁵ Rapport quinquennal 2002, p. 146-147.

¹²⁰⁶ Ces organismes sont collectivement appelés « personnes désignées par l'Assemblée nationale » et leurs crédits font l'objet d'un volume séparé dans le budget de dépenses annuel du gouvernement; voir par exemple, pour 2025-2026 : GOUVERNEMENT DU QUÉBEC, *Budget de dépenses 2025-2026 - Crédits, dépenses et plans annuels de gestion des dépenses de l'Assemblée nationale et des personnes désignées*, 2025, en ligne : <https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/secretariat-du-conseil-du-tresor/publications-adm/budgets/2025-2026/4_Credits_Assemblee_nationale.pdf>.

¹²⁰⁷ *Loi sur l'accès à l'information et la protection de la vie privée [Ontario]*, préc., note 176, art. 4(1).

¹²⁰⁸ FIPPA de la Colombie-Britannique, art. 37(2).

¹²⁰⁹ *Loi sur l'accès à l'information et la protection de la vie privée*, C.P.L.M., c. F175, art. 58.1(1.0.2), en ligne : <<https://www.canlii.org/fr/mb/legis/lois/cplm-c-f175/derniere/cplm-c-f175.html>>.

¹²¹⁰ *Loi sur l'accès à l'information et la protection de la vie privée [Nunavut]*, L.C.Nun., c. A-20, art. 61, en ligne : <<https://www.nunavutlegislation.ca/fr/consolidated-law/acces-linformation-et-la-protection-de-la-vie-privee-codification-officielle-de-la>>.

¹²¹¹ Le gouvernement a prévu une disposition en ce sens dans sa nouvelle loi sur l'accès aux documents et la protection des renseignements personnels, adoptée en septembre 2025 et qui entrera en vigueur en 2027 : *Freedom of Information and Protection of Privacy Act [Nouvelle-Écosse]*, SNS 2025, c. 5, art. 121, en ligne : <<https://www.nslegislature.ca/sites/default/files/legc/statutes/freedom%20of%20information%20and%20protection%20of%20privacy.pdf>>.



l'Assemblée nationale du Québec. Cette situation prévaut entre autres en Alberta¹²¹², en Ontario¹²¹³, en Saskatchewan¹²¹⁴, à l'Île-du-Prince-Édouard¹²¹⁵ et à Terre-Neuve-et-Labrador¹²¹⁶.

Recommandation 72

Garantir l'indépendance administrative de la Commission, notamment en rattachant son budget et ses effectifs au Bureau de l'Assemblée nationale.

¹²¹² *Access to Information Act [Alberta]*, préc., note 165, art. 46(1).

¹²¹³ *Loi sur l'accès à l'information et la protection de la vie privée [Ontario]*, préc., note 176, art. 8(1).

¹²¹⁴ *Freedom of Information and Protection of Privacy Act [Saskatchewan]*, SS 1990-91, c. F-22.01, art. 43 à 43.3, en ligne : <https://publications.saskatchewan.ca/api/v1/products/527/formats/694/download>.

¹²¹⁵ *Freedom of Information and Protection of Privacy Act [Île-du-Prince-Édouard]*, RSPEI 1988, c. F-15.01, art. 49, en ligne : https://www.princeedwardisland.ca/sites/default/files/legislation/f-15-01-freedom_of_information_and_protection_of_privacy_act.pdf.

¹²¹⁶ *Access to Information and Protection of Privacy Act [Terre-Neuve-et-Labrador]*, préc., note 64, art. 91.



4.2. L'appel des décisions de la section juridictionnelle

Sommaire

Les décisions de la section juridictionnelle de la Commission sont sujettes, dans certains cas, à un droit d'appel à la Cour du Québec précédant, pour un même dossier, un possible recours en contrôle judiciaire auprès de la Cour supérieure. Selon la Commission, ce premier droit d'appel complexifie le parcours d'un citoyen pour obtenir une décision finale suivant une demande d'exercice de ses droits où l'ensemble de ces recours seraient exercés. Cette situation entre en contradiction avec les principes de la justice administrative, comme la célérité.

La Commission recommande que les décisions émanant de sa section juridictionnelle soient uniquement contestables par un recours en contrôle judiciaire déposé auprès de la Cour supérieure.

4.2.1. Contexte et situation actuelle

Bien que les questions de fait tranchées par la section juridictionnelle de la Commission soient sans appel, ses décisions finales peuvent être portées en appel à la Cour du Québec sur des questions de droit ou de compétence¹²¹⁷. Malgré ce recours auprès de la Cour du Québec, le même dossier peut ensuite faire l'objet d'un recours en contrôle judiciaire auprès de la Cour supérieure. Pourtant, pour certains autres tribunaux administratifs, la contestation s'effectue directement par voie de contrôle judiciaire devant la Cour supérieure.

De l'avis de la Commission, cette situation nuit notamment à la simplicité et à la célérité du processus de recours pour les citoyens.

4.2.2. Enjeux

La Commission considère que le processus actuel de contestation de ses décisions est complexe. Il ne favorise pas une conclusion rapide pour le citoyen du processus de recours concernant l'exercice des

¹²¹⁷ Loi sur l'accès, art. 147; Loi sur le privé, art. 61 al. 1; LRSSS, art. 150.



divers droits que lui confèrent les lois, comme le droit d'accès aux documents administratifs ou à ses renseignements personnels, ou le droit à leur rectification.

Lorsque l'ensemble des recours discutés précédemment sont exercés, l'obtention d'une décision « finale » sur un dossier nécessite de nombreuses procédures judiciaires et accroît évidemment les délais et les démarches nécessaires au dénouement de l'affaire. Sommairement, dans ces cas, la solution du dossier aura typiquement nécessité¹²¹⁸ :

- une demande d'exercice d'un droit conféré par les lois sur l'accès aux documents et la protection des renseignements personnels formulée par un citoyen auprès d'une organisation;
- une décision du responsable de l'accès aux documents ou de la protection des renseignements personnels de l'organisation concernée;
- un recours déposé par le citoyen auprès de la Commission;
- une décision finale de la section juridictionnelle de la Commission portant sur la demande de révision;
- une déclaration d'appel déposée à la Cour du Québec sur la base d'une question de droit ou de compétence;
- une décision de la Cour du Québec concernant la demande d'appel;
- un pourvoi en contrôle judiciaire déposé à la Cour supérieure;
- une décision de la Cour supérieure concernant ce pourvoi en contrôle judiciaire.

Or l'un des objectifs de la création des tribunaux administratifs est de rendre justice de manière moins formaliste, plus rapide et moins coûteuse, et ce, pour une plus grande accessibilité¹²¹⁹. En droit administratif, les objectifs du législateur sont notamment de satisfaire un besoin d'efficacité avec le bénéfice d'une connaissance approfondie du contexte particulier dans lequel s'inscrivent les différends à trancher¹²²⁰. Les tribunaux administratifs sont donc une réponse à la volonté du législateur de recourir à des décideurs possédant une expertise spéciale dans certains domaines¹²²¹.

Conformément à cet esprit, certaines décisions finales du Tribunal administratif du travail ou du Tribunal administratif du Québec, par exemple, ne peuvent être contestées que par voie de contrôle judiciaire devant la Cour supérieure, sans étape d'appel à la Cour du Québec.

4.2.3. Recommandation

La Commission est d'avis que le mode de contestation des décisions finales de sa section juridictionnelle devrait être modifié afin de simplifier le processus actuellement en place. Ainsi, elle recommande le retrait des dispositions prévoyant le processus d'appel de ces décisions devant la Cour du Québec afin, notamment, de reconnaître pleinement l'expertise spécialisée de la Commission, y compris sur les questions de droit et de compétence dont elle est saisie. En permettant la contestation des décisions de la Commission uniquement par la voie du contrôle judiciaire de la Cour supérieure, la Commission est d'avis

¹²¹⁸ L'illustration présuppose un recours initial en révision introduit par le citoyen lui-même; par ailleurs, elle exclut les démarches subséquentes possibles, dans certains cas, auprès de la Cour d'appel du Québec et de la Cour suprême du Canada.

¹²¹⁹ Pierre ISSALYS et Denis LEMIEUX, *L'action gouvernementale. Précis de droit des institutions administratives*, 4^e éd., Cowansville, Éditions Yvon Blais, 2019, p. 468.

¹²²⁰ *Id.*

¹²²¹ Patrice GARANT, *Droit administratif*, 7^e éd., Cowansville, Éditions Yvon Blais, 2017, p. 112.



que l'objectif propre aux tribunaux administratifs de prévoir des démarches proportionnées, eu égard aux coûts et aux délais pour le citoyen, serait mieux atteint.

Cette proposition s'inscrit dans un esprit de célérité et de simplicité des recours pour le citoyen, considérant que cette modification permettrait d'obtenir plus rapidement, et au terme de démarches moins nombreuses, une réponse finale quant à sa demande d'exercice d'un de ses droits ainsi qu'à l'état du droit applicable.

Recommandation 73

Retirer de la Loi sur l'accès, de la Loi sur le privé et de la LRSSS les dispositions relatives à l'appel devant la Cour du Québec des décisions émanant de la section juridictionnelle de la Commission pour qu'elles soient directement soumises au contrôle judiciaire de la Cour supérieure.

4.3. Le caractère objectif des manquements passibles de sanctions administratives pécuniaires

Sommaire

Les sanctions administratives pécuniaires ont été ajoutées à la Loi sur le privé par la Loi 25 : elles constituent un outil supplémentaire pour en assurer le respect par les entreprises. Malgré le caractère récent de leur introduction, la Commission constate des enjeux en lien avec la portée des manquements pouvant faire l'objet de sanctions administratives pécuniaires.

La Commission recommande ainsi de revoir les dispositions concernées pour :

- retirer ce type de sanction lorsque la démonstration du manquement concerné repose sur des éléments de type subjectif;
- ajouter ce type de sanction pour certains manquements dont la démonstration peut être objective et qui ne sont pas actuellement visés.

4.3.1. Contexte

Depuis le 22 septembre 2023, la Commission a le pouvoir d'imposer des sanctions administratives pécuniaires en vertu de la Loi sur le privé¹²²². Ces sanctions permettent à la Commission de jouir d'un moyen supplémentaire pour assurer son rôle de surveillance et de contrôle du respect de certaines des obligations imposées par cette loi. Pour mieux exploiter le grand potentiel de cet outil d'intervention, la Commission suggère des ajustements à la portée des manquements visés.

¹²²² Loi sur le privé, art. 90.1.



4.3.2. Situation actuelle

La Commission peut imposer une sanction administrative pécuniaire pour certains manquements à la Loi sur le privé, c'est-à-dire à toute personne qui :

- n'informe pas adéquatement les personnes concernées de la collecte de leurs renseignements personnels conformément aux articles 7 et 8 de la Loi¹²²³;
- recueille, utilise, communique, conserve ou détruit des renseignements personnels en contrevenant à la Loi¹²²⁴;
- ne déclare pas à la Commission ou aux personnes concernées, lorsqu'elle y est tenue, un incident de confidentialité¹²²⁵;
- ne prend pas les mesures de sécurité propres à assurer la protection des renseignements personnels¹²²⁶;
- n'informe pas la personne concernée qu'une décision à son égard a été fondée exclusivement sur un traitement automatisé de renseignements ou ne lui donne pas l'occasion de présenter ses observations à l'égard de cette décision¹²²⁷;
- si elle est un agent de renseignements personnels, se soustrait à ses obligations à ce titre prévues à la Loi sur le privé¹²²⁸.

Le montant maximal de ces sanctions atteint 50 000 \$ dans le cas d'une personne physique et, dans les autres cas, 10 000 000 \$ ou un montant correspondant à 2 % du chiffre d'affaires mondial de l'exercice financier précédent si ce dernier montant est plus élevé¹²²⁹.

Comme prévu à la Loi sur le privé¹²³⁰, la Commission a élaboré et rendu public un cadre général d'application des sanctions administratives pécuniaires¹²³¹ précisant :

- les objectifs poursuivis par ces sanctions;
- les critères devant guider la décision d'imposer une sanction lorsqu'un manquement est constaté et la détermination du montant de la sanction;
- les circonstances dans lesquelles le recours pénal est priorisé;
- les autres modalités relatives à l'imposition des sanctions. Par exemple, la Commission a prévu une catégorisation des sanctions et des montants encourus en fonction de l'ampleur du manquement, déterminée entre autres selon sa nature, sa gravité objective, sa durée et le nombre de personnes touchées.

¹²²³ *Id.*, art. 7, 8 et 90.1 par. 1.

¹²²⁴ *Id.*, art. 90.1 par. 2.

¹²²⁵ *Id.*, art. 90.1 par. 3.

¹²²⁶ *Id.*, art. 10 et 90.1 par. 4.

¹²²⁷ *Id.*, art. 12.1 et 90.1 par. 5.

¹²²⁸ *Id.*, art. 70, 70.1, 71, 72, 78, 79, 79.1 et 90.1 par. 6.

¹²²⁹ *Id.*, art. 90.12.

¹²³⁰ *Id.*, art. 90.2.

¹²³¹ COMMISSION D'ACCÈS À L'INFORMATION, *Cadre général d'application des sanctions administratives pécuniaires*, 2023, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_Cadre_Sanct_Pecun.pdf>.

4.3.3. Enjeux

Malgré l'implantation récente des sanctions administratives pécuniaires dans la Loi sur le privé, la Commission relève deux enjeux en lien avec l'application des dispositions qui les prévoient.

4.3.3.1. Certaines possibilités de sanctions administratives pécuniaires concernent des manquements reposant sur la démonstration d'éléments subjectifs

La Commission remarque que certains des manquements pouvant actuellement donner lieu à des sanctions administratives pécuniaires nécessitent la démonstration d'éléments constitutifs subjectifs.

Pourtant, la visée du recours à la sanction administrative pécuniaire est d'inciter à remédier aux manquements à la loi et de dissuader la répétition de ces manquements, et ce, de manière beaucoup plus rapide et souple qu'une poursuite pénale. Pour cette raison, ce type de sanction est d'ordinaire retenu pour des manquements qui se constatent objectivement, ce qui limite les débats associés : la preuve des éléments constitutifs de ces manquements devrait être relativement simple et reposer sur quelques éléments factuels seulement. L'enquête pouvant mener à l'imposition d'une sanction administrative pécuniaire est donc généralement rapide, puisqu'il suffit à l'autorité de constater, sur une base tangible, le respect ou non d'une obligation objective par l'entreprise visée. Idéalement, lors de ce type de processus, il devrait par conséquent y avoir peu de place à l'interprétation. De cette façon, une sanction administrative pécuniaire donne lieu à des effets directs : elle incite l'entreprise à prendre promptement les mesures requises pour remédier au manquement et elle en dissuade la répétition.

Au contraire, les cas nécessitant la démonstration d'éléments subjectifs demandent une appréciation approfondie s'appuyant sur une enquête plus complexe et dont les constats peuvent faire l'objet d'interprétation juridique et de débats contradictoires. Ainsi, compte tenu du libellé de certains paragraphes de la Loi sur le privé, il pourrait être difficile d'émettre des sanctions administratives pécuniaires quant à certains manquements lorsque certains éléments constitutifs de ceux-ci sont davantage subjectifs. Dans ces cas, l'objectif de souplesse et de rapidité de ce type de sanction risque de ne pas être atteint. Un exemple illustrant ce cas concerne les manquements en matière de nécessité. Une sanction administrative pécuniaire peut être imposée à une organisation qui « recueille, utilise, communique, conserve ou détruit des renseignements personnels en contravention à la loi ». Or, le respect du critère de nécessité est prévu à la loi notamment pour la collecte de renseignements personnels¹²³². L'évaluation de ce critère impose toutefois, ainsi que le rappelle la Commission dans la section 2.1.2, une analyse subjective au cas par cas.

Puisque les sanctions administratives pécuniaires semblent constituer un remède mal adapté à ce type de manquement, la Commission souligne que les éléments subjectifs actuellement retenus peuvent générer de l'incertitude pour les entreprises, au détriment de la sécurité juridique. En effet, compte tenu du caractère allégé de la procédure pour une sanction de ce type par rapport à une poursuite pénale, certains acteurs du secteur privé ont exprimé des craintes quant au fait que des sanctions d'un montant important puissent être imposées en lien avec des termes ou des critères portant à interprétation.

¹²³² Loi sur le privé, art. 90.1 al. 1 par. 2.



4.3.3.2. Des manquements dont la démonstration repose sur des éléments objectifs ne sont visés par aucune possibilité de sanction administrative pécuniaire

À l'opposé de la situation énoncée ci-haut, la Commission constate que certains manquements à la Loi sur le privé dont la démonstration pourrait s'effectuer objectivement ne peuvent actuellement faire l'objet de sanctions administratives pécuniaires. En voici quelques exemples :

- L'absence de publication du titre et des coordonnées du responsable de la protection des renseignements personnels sur le site Web de l'entreprise ou, si celle-ci ne dispose pas d'un site Web, son défaut de rendre ces informations accessibles par tout autre moyen approprié¹²³³.
- L'absence de publication, sur le site Web de l'entreprise, d'informations détaillées, en termes simples et clairs, au sujet des politiques et des pratiques encadrant sa gouvernance à l'égard des renseignements personnels, ou, dans le cas où elle n'a pas de site Web, le défaut de rendre ces informations accessibles par tout autre moyen approprié¹²³⁴.
- Le fait, pour une entreprise, de ne pas avoir procédé à une évaluation des facteurs relatifs à la vie privée dans le cadre d'un projet d'acquisition, de développement ou de refonte d'un système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels¹²³⁵.
- Le fait, pour une entreprise, de ne pas tenir de registre des incidents de confidentialité¹²³⁶.

4.3.4. Recommandation

La Commission estime que les dispositions de la Loi sur le privé prévoyant la possibilité de sanctions administratives pécuniaires devraient être revues de manière à mieux refléter leur but, soit que seuls les manquements de type objectif puissent être visés. Cet ajustement de la portée du régime de sanctions administratives pécuniaires devrait à la fois uniformiser les enquêtes administratives que doit mener la Commission et offrir plus de sécurité juridique aux entreprises.

Recommandation 74

Réviser les dispositions de la Loi sur le privé prévoyant la possibilité d'imposer des sanctions administratives pécuniaires pour :

- préciser que l'application de ces sanctions ne vise clairement que les manquements de type objectif;
- ajouter des manquements de type objectif qui ne sont pas actuellement visés.

¹²³³ *Id.*, art. 3.1 al. 3.

¹²³⁴ *Id.*, art. 3.2.

¹²³⁵ *Id.*, art. 3.3.

¹²³⁶ *Id.*, art. 3.8.



4.4. L'accompagnement des entreprises

Sommaire

La réforme des lois sur la protection des renseignements personnels a apporté de nombreux changements aux responsabilités des entreprises faisant affaire au Québec. Celles-ci ont exprimé le besoin d'être accompagnées dans la mise en œuvre de leurs nouvelles obligations. Soucieuse de sa mission de promotion, la Commission a mené plusieurs actions pour leur offrir de l'information et faciliter leur conformité à la Loi sur le privé, par exemple par :

- la refonte de son site Web pour le rendre plus complet et plus clair;
- la publication de lignes directrices en matière de consentement;
- la diffusion de 13 capsules vidéo sur la Loi sur le privé;
- l'adoption d'orientations communes avec ses homologues canadiens;
- la participation accrue à des événements publics et l'établissement de partenariats stratégiques;
- la sensibilisation des entreprises dans le cours des activités de surveillance.

4.4.1. Contexte

Dans la foulée du rehaussement des normes en matière de protection des renseignements personnels apporté par la Loi 25, les entreprises ont dû assumer de nouvelles responsabilités. Afin de tenir compte de ces obligations dans leurs opérations et de s'assurer de leur conformité au cadre légal qui leur est applicable, les entreprises ont signalé un besoin accru d'accompagnement.

À la demande du ministre responsable de l'Accès à l'information et de la Protection des renseignements personnels¹²³⁷, la Commission se penche sur ce thème dans le présent rapport. Elle revient sur les besoins exprimés par les entreprises, puis fait état de ses initiatives d'accompagnement dirigées vers le secteur privé depuis 2021.

¹²³⁷ Loi sur l'accès, art. 179.



4.4.2. Situation actuelle

La mise en application de la Loi sur le privé implique une responsabilisation accrue des entreprises en matière de protection des renseignements personnels qu'elles détiennent, laquelle exige assurément une montée en compétence de leurs responsables et de leur personnel. La réforme apportée par la Loi 25 constitue également une réponse à un contexte plus large de bouleversements technologiques qui traversent la société et le monde entrepreneurial, et qui imposent d'importantes adaptations des pratiques. Par exemple, l'adoption des nouvelles technologies dans les entreprises québécoises continue de croître, l'IA poursuivant notamment sa progression¹²³⁸. Cette conjoncture confronte les entreprises à certains défis en lien avec la conformité, notamment pour opérer et innover en toute confiance. Les besoins du secteur privé en matière d'accompagnement sont donc importants, comme l'ont révélé divers indicateurs ces dernières années.

Ainsi, dès les consultations particulières sur le projet de réforme en matière de protection des renseignements personnels, des regroupements d'entreprises ont souligné que l'ampleur des modifications envisagées nécessiterait une attention particulière à l'aide aux entreprises, notamment en raison des importantes sanctions prévues en cas de non-conformité. Ils indiquaient déjà que des guides de référence ou des lignes directrices devraient être produits pour faciliter l'application de la Loi, et ils attiraient l'attention sur la difficulté de mettre en œuvre la réforme pour les PME, dont les ressources et l'expertise sont limitées¹²³⁹.

Des sondages et diverses statistiques ont aussi illustré tant l'inquiétude que l'impréparation des entreprises en lien avec la réforme. Les données suivantes apportent un éclairage intéressant :

- Un sondage mené auprès d'une centaine d'organisations canadiennes ou étrangères¹²⁴⁰ par le cabinet Gowling WLG et IAB Canada en 2023 a révélé que 69 % des organisations souhaitaient des orientations plus claires quant à l'application de la Loi, que 67 % craignaient des sanctions en cas de manquement et que 52 % n'avaient pas les ressources nécessaires pour mettre en œuvre la réforme¹²⁴¹.
- La même année, une étude préliminaire du Groupe de recherche interdisciplinaire en cybersécurité de l'Université de Sherbrooke réalisée auprès de 100 PME et organismes à but non lucratif concluait que les PME estimaient, dans une proportion de 40 %, être « presque prêtes ou tout à fait prêtes » à

¹²³⁸ De 2022 à 2025, il faut noter que 21,6 % des entreprises québécoises ont réalisé « des investissements modérés à majeurs dans leur infrastructure numérique » : Pascasie NIKUZE, « Adoption et utilisation de l'intelligence artificielle par les entreprises au Québec en 2024 et en 2025. Portrait exploratoire », *Institut de la statistique du Québec* (28 novembre 2025), en ligne : <<https://statistique.quebec.ca/fr/produit/publication/adoption-et-utilisation-intelligence-artificielle-entreprises-au-quebec-2024-2025>> (consulté le 4 février 2026).

¹²³⁹ CONSEIL DU PATRONAT DU QUÉBEC, *Commentaires du CPQ - Projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, 2020, p. 5, en ligne : <http://www.assnat.qc.ca/Media/Process.aspx?MediaId=ANQ.Vigie.Bil.DocumentGenerique_161583>; FÉDÉRATION DES CHAMBRES DE COMMERCE DU QUÉBEC, *Projet de loi 64 - Loi modernisant des dispositions législatives en matière de protection des renseignements personnels. Mémoire présenté à la Commission des institutions*, 2020, p. 2, 5 et 6, en ligne : <http://www.assnat.qc.ca/Media/Process.aspx?MediaId=ANQ.Vigie.Bil.DocumentGenerique_161393>.

¹²⁴⁰ La majorité employaient au moins 100 personnes au Québec : GOWLING WLG et IAB CANADA, *Rapport du sondage sur la Loi 25 : les organisations sont-elles prêtes pour la nouvelle loi québécoise sur la protection de la vie privée?*, 2023, p. 5, en ligne : <<https://brandconnect.gowlingwlg.com/m/68e2153029089a3a/original/Rapport-du-sondage-sur-la-Loi-25-les-organisations-sont-elles-pret-es-pour-la-nouvelle-loi-quebecoise-sur-la-protection-de-la-vie-privee.pdf>> (consulté le 14 septembre 2023).

¹²⁴¹ *Id.*, p. 7-8.



appliquer les dispositions de la Loi 25 entrées en vigueur en septembre 2022¹²⁴². Or, sur la base des pratiques réelles analysées, les chercheurs indiquaient que seuls 3 % des organisations avaient accompli toutes les étapes requises pour se conformer aux nouvelles mesures¹²⁴³. Pour la majorité des dispositions, entrant en vigueur en septembre 2023, 33 % des organisations estimaient être prêtes, mais aucune ne l'était entièrement dans les faits¹²⁴⁴. Dans l'ensemble, une proportion de 40 % des organisations indiquait avoir « une réelle intention de se conformer à la Loi 25 dans les prochaines années¹²⁴⁵ ».

- Le fournisseur de solutions logicielles québécois Devolutions, dans son portrait de la sécurité informatique dans les PME en 2024-2025¹²⁴⁶, montrait que 47 % des entreprises sondées se disaient prêtes à respecter l'ensemble des nouvelles exigences de la Loi. Les défis évoqués par le reste des entreprises sont surtout le manque de ressources internes (47 %) et la complexité des exigences légales (6 %). Devolutions concluait que les freins étaient davantage structurels ou organisationnels que financiers.
- Une recherche menée en 2024 par une étudiante à la maîtrise de l'Université de Montréal¹²⁴⁷ a montré que 40 % des 94 entreprises interrogées ne diffusaient pas encore leur politique de confidentialité, et qu'une proportion substantielle d'entre elles avaient des pratiques d'archivage inadéquates, par exemple sans aperçu global des renseignements détenus ni politique de gestion du cycle de vie des informations, ce qui compliquait leur destruction au moment opportun¹²⁴⁸.
- Seuls 30 % des entreprises sondées par le groupe NOVIPRO et la firme Léger en 2025 ont adopté une approche proactive à la conformité en matière de protection des renseignements personnels¹²⁴⁹, et 22 % d'entre elles se déclaraient totalement conformes.
- La convergence relative de ces données révèle une conformité hésitante et des incertitudes des entreprises quant à ce qu'elles doivent faire pour améliorer la situation.

La Fédération des chambres de commerce du Québec rapportait encore récemment que les nouvelles exigences en matière de protection des renseignements personnels font partie des préoccupations récurrentes de ses membres¹²⁵⁰. Plusieurs entreprises affirment avoir dû dépenser des montants importants en services de consultation pour atteindre la conformité.

Les questions que la Commission reçoit des entreprises par différents canaux et ses interactions avec des organisations lors des premières étapes de dossiers de surveillance l'ont menée à des constats similaires.

¹²⁴² Manon G. GUILMETTE et Daniel CHAMBERLAND-TREMBLAY, *Rapport préliminaire - Étude sur le niveau de préparation des PME à la Loi 25, Loi québécoise portant sur la protection des renseignements personnels*, Groupe de recherche interdisciplinaire en cybersécurité / Université de Sherbrooke, 2023, p. 2, en ligne : <https://gric.recherche.usherbrooke.ca/wp-content/uploads/2023/09/gric_rapport20230919_pme_loi25.pdf> (consulté le 25 septembre 2023).

¹²⁴³ *Id.*

¹²⁴⁴ *Id.*, p. 2.

¹²⁴⁵ *Id.*, p. 3.

¹²⁴⁶ DEVOLUTIONS, *Portrait de la sécurité informatique chez les PME québécoises*, 2025, p. 32-33, en ligne : <<https://cdn.devolutions.net/documents/survey-report/state-of-it-security-in-smbs-2024-2025-fr.pdf>>.

¹²⁴⁷ Louise TREMBLAY, *La gestion des documents semi-actifs dans les entreprises privées québécoises à l'aune de la Loi 25, qui vise à assurer la protection des renseignements personnels*, mémoire de maîtrise, Université de Montréal, 2025, en ligne : <<https://umontreal.scholaris.ca/bitstreams/b792ed90-710b-48e9-a796-1fec850470bd/download>>.

¹²⁴⁸ Philippe Jean POIRIER, « Loi 25 sur les données personnelles : une conformité... encore à parfaire pour les entreprises », *Isarta tendances* (3 février 2026), en ligne : <<https://isarta.com/infos/loi-25-sur-les-donnees-personnelles-une-conformite-encore-a-parfaire-pour-les-entreprises/>> (consulté le 4 février 2026).

¹²⁴⁹ GROUPE NOVIPRO et LÉGER, *Portrait TI - 9^e édition*, 2025, p. 43, en ligne : <<https://info.novipro.com/portrait-ti>>.

¹²⁵⁰ Karl RETTINO-PARAZELLI, « La loi 25 pèse lourd sur les épaules des entreprises », *Les Affaires* (19 mars 2025), en ligne : <https://www.lesaffaires.com/dossiers/pme-alleger-le-fardeau-administratif/la-loi-25-pese-lourd-sur-les-epaules-des-entreprises-edition_19_mars_2025/> (consulté le 4 février 2026).



Face aux importants besoins d'accompagnement des entreprises pour l'application de la Loi sur le privé, en particulier pour les PME, qui constituent la quasi-totalité des entreprises avec employés¹²⁵¹, la Commission s'est mise en action. La promotion de la protection des renseignements personnels relève de ses fonctions¹²⁵² et doit notamment être assurée par des activités de sensibilisation, selon ce qu'a précisé la Loi 25¹²⁵³.

4.4.3. Moyens mis en œuvre par la Commission

Au cours des dernières années, la Commission a déployé des moyens variés pour soutenir les entreprises, que ce soit par la fourniture d'informations générales, la participation à des événements ou l'établissement de partenariats. Dans le cadre de sa mission de surveillance, elle est également fréquemment appelée à sensibiliser les entreprises faisant l'objet de signalements afin de les aider à améliorer leurs pratiques : un volet peu visible, mais important de ses activités.

4.4.3.1. La fourniture d'informations générales

La Commission s'assure de fournir des informations générales de qualité aux entreprises, et ce, par l'entremise de plusieurs outils et canaux de communication lui permettant d'en rejoindre le plus grand nombre possible.

Elle mise d'abord un site Web qui a été complètement refondu dans la foulée de l'adoption de la Loi 25 afin d'y restructurer la présentation de l'information, d'y simplifier les textes et de les rendre plus facilement compréhensibles, d'y améliorer les aspects graphiques et de respecter les standards d'accessibilité modernes sur tout type d'appareil. Dès 2021, avant même le début de cette refonte, la Commission a entrepris de revoir l'ensemble de l'information s'adressant aux entreprises sur son site Web, et elle l'a mise à jour en fonction des nouvelles obligations de la Loi, suivant un découpage aligné sur les grands principes de protection des renseignements personnels plus intuitif et séquentiel.

La Commission complète sa présence numérique par une activité soutenue sur les médias sociaux, en particulier sur le réseau LinkedIn, prisé des entreprises. Ouvert en 2023, le compte de la Commission a connu une forte croissance, passant de 398 abonnés au 31 mars de cette année-là à 4 631 à la même date trois ans plus tard. Elle y publie régulièrement des informations relatives au respect de la loi et à ses activités, ce qui contribue à faire connaître la Loi sur le privé.

En parallèle, la Commission a ouvert un compte sur la plateforme YouTube. En 2024, elle y a diffusé une série de 13 capsules vidéo réalisées en collaboration avec l'AAPI¹²⁵⁴. Spécialement conçues pour aider les

¹²⁵¹ Les données de décembre 2023 de l'Institut de la statistique du Québec indiquent que ce sont 275 795 des 278 278 entreprises avec employés qui en comptent moins de 200, soit 99,1 % : INSTITUT DE LA STATISTIQUE DU QUÉBEC, *Nombre d'entreprises actives au Québec en décembre 2023 (données semestrielles)*, 2024, en ligne : <<https://statistique.quebec.ca/fr/fichier/nombre-entreprises-actives-quebec-decembre-2023-donnees-semestrielles.xlsx>>.

¹²⁵² Loi sur l'accès, art. 22.1 al. 2.

¹²⁵³ Loi 25, art. 44.

¹²⁵⁴ COMMISSION D'ACCÈS À L'INFORMATION, « Protéger les renseignements personnels : capsules vidéo », en ligne : <<https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privées/capsules-video>> (consulté le 19 janvier 2026).

entreprises et les organisations privées à comprendre l'essentiel de leurs obligations en matière de protection des renseignements personnels, ces capsules ont déjà cumulé plus de 30 000 visionnements.

En plus des textes informationnels qu'il contient, le site Web de la Commission permet aux entreprises d'accéder à plusieurs guides, fiches et outils en lien avec la protection des renseignements personnels. Sans être exhaustive, la liste suivante donne un aperçu de la variété des documents publiés après la réforme :

- Aide-mémoire sur les nouvelles responsabilités des entreprises, les pistes d'action et les bonnes pratiques¹²⁵⁵;
- Nouvelle version du guide d'accompagnement à la démarche d'évaluation des facteurs relatifs à la vie privée¹²⁵⁶;
- Modèle de rapport d'évaluation des facteurs relatifs à la vie privée¹²⁵⁷;
- Nouvelle version du guide sur les principes et obligations à respecter en matière de biométrie¹²⁵⁸;
- Nouvelle version du modèle de formulaire de consentement à la biométrie¹²⁵⁹;
- Guide sur la rédaction d'une politique de confidentialité par les entreprises¹²⁶⁰;
- Guide sur la prévention des incidents de confidentialité¹²⁶¹;
- Liste de contrôle sur la prévention des incidents de confidentialité pour les entreprises¹²⁶²;
- Fiche sur les bonnes pratiques pour les entreprises devant effectuer un repérage complet et sérieux des renseignements personnels à la suite d'une demande d'accès¹²⁶³;
- Constats sur les problématiques courantes en lien avec le recours aux horodateurs et aux pointeuses biométriques¹²⁶⁴;
- Cadre général d'application des sanctions administratives pécuniaires¹²⁶⁵.

Ces documents sont appelés à être présentés de plus en plus directement sous la forme de pages Web. Soulignons par exemple l'ajout récent d'une page d'information destinée aux entreprises concernant le recrutement de personnel¹²⁶⁶.

¹²⁵⁵ COMMISSION D'ACCÈS À L'INFORMATION, *Entreprises - Vers la conformité à la Loi sur le privé*, 2022, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_GU_Responsabilites_Entreprises.pdf>.

¹²⁵⁶ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 847.

¹²⁵⁷ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 848.

¹²⁵⁸ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 1007.

¹²⁵⁹ COMMISSION D'ACCÈS À L'INFORMATION, *Modèle de formulaire de consentement à la collecte, à l'utilisation et à la conservation de renseignements biométriques*, 2022, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_FO_Consent_Biometrie_Modele.docx>.

¹²⁶⁰ COMMISSION D'ACCÈS À L'INFORMATION, *Rédiger une politique de confidentialité - Guide explicatif pour les entreprises*, 2023, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_GU_POL_Confidentialite.pdf>.

¹²⁶¹ COMMISSION D'ACCÈS À L'INFORMATION, *Prévenir les incidents de confidentialité - Guide explicatif pour les entreprises*, 2026, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_GU_ENTR_Prevention_incidents.pdf>.

¹²⁶² COMMISSION D'ACCÈS À L'INFORMATION, *Prévenir les incidents de confidentialité - Liste de contrôle pour les entreprises*, 2026, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_FIC_ENTR_Prevention_incidents.pdf>.

¹²⁶³ COMMISSION D'ACCÈS À L'INFORMATION, *Repérage complet et sérieux des renseignements personnels en entreprise - Bonnes pratiques pour les entreprises visées par une demande d'accès*, 2025, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_FIC_ENTR_Reperage_RP.pdf>.

¹²⁶⁴ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 1023.

¹²⁶⁵ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 1231.

¹²⁶⁶ COMMISSION D'ACCÈS À L'INFORMATION, « Recrutement de personnel et respect de la vie privée » (2025), en ligne : <<https://www.cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/operation-recrutement-emploi>> (consulté le 22 janvier 2026).



De plus, la Commission a travaillé à simplifier l'accès à certains de ces services en introduisant un formulaire unique pour transiger avec elle¹²⁶⁷.

4.4.3.2. Les lignes directrices

En vertu d'une nouvelle fonction que lui a confiée la Loi 25¹²⁶⁸, la Commission peut élaborer des lignes directrices visant à faciliter l'application de la Loi sur le privé.

Elle a diffusé en 2023 ses premières lignes directrices, portant sur les critères de validité du consentement¹²⁶⁹ et visant à clarifier, par des orientations et des exemples, la manière dont les lois doivent être appliquées concrètement par les organisations. Elles mettent aussi en lumière les meilleures pratiques concernant le consentement. Élaborées sur une période d'un an, ces lignes directrices ont fait l'objet d'améliorations substantielles à la suite d'une consultation publique. La Commission a en effet jugé capital de consulter divers groupes, dont des regroupements d'entreprises, pour s'assurer de prendre en compte la perspective du secteur privé et ses besoins.

4.4.3.3. Les orientations communes avec des homologues

La Commission fournit des orientations aux entreprises par le biais de prises de position communes avec d'autres autorités homologues, chargées de protection des renseignements personnels. Ces entreprises mettent en commun leur expertise et énoncent ainsi des orientations concordantes, au bénéfice notamment de celles qui font affaire dans plusieurs États.

Au cours des dernières années, principalement de concert avec ses homologues du reste du Canada, la Commission a ainsi encouragé les organisations à :

- éviter les interfaces truquées¹²⁷⁰;
- planifier diligemment la communication de renseignements de santé et de services sociaux aux autorités lorsqu'une situation de violence conjugale le justifie¹²⁷¹;
- assurer une meilleure protection des jeunes lorsqu'elles fournissent des technologies éducatives¹²⁷²;
- mettre en place des mesures permettant de protéger les jeunes en ligne¹²⁷³;

¹²⁶⁷ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 1191.

¹²⁶⁸ Loi sur l'accès, art. 123, par. 9.

¹²⁶⁹ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 486.

¹²⁷⁰ COMMISSAIRES FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX À LA PROTECTION DE LA VIE PRIVÉE ET DES OMBUDS RESPONSABLES DE LA PROTECTION DE LA VIE PRIVÉE, « Repérer et atténuer les préjudices découlant des mécanismes de conception trompeuse relatifs à la protection de la vie privée », *Commissariat à la protection de la vie privée du Canada* (13 novembre 2024), en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-territoires/res_241010_ct/> (consulté le 14 novembre 2024).

¹²⁷¹ COMMISSAIRES ET OMBUDS FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX À LA PROTECTION DE LA VIE PRIVÉE, « La communication responsable de renseignements en situation de violence conjugale », *Commissariat à la protection de la vie privée du Canada* (octobre 2024), en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-territoires/res_241010_vc/> (consulté le 19 janvier 2026).

¹²⁷² COMMISSAIRES FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX (FPT) ET DES OMBUDS RESPONSABLES DE LA PROTECTION DE LA VIE PRIVÉE, « Protéger la vie privée des enfants et des jeunes au moyen de l'utilisation responsable de technologies éducatives dans les salles de classe », *Commissariat à la protection de la vie privée du Canada* (8 octobre 2025), en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-territoires/res_20251008_edtech/> (consulté le 19 janvier 2026).

¹²⁷³ COMMISSAIRES FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX À LA PROTECTION DE LA VIE PRIVÉE ET DES OMBUDS RESPONSABLES DE LA PROTECTION DE LA VIE PRIVÉE, « Document accompagnateur – Mettre l'intérêt supérieur des jeunes à l'avant-plan en matière de



- protéger la vie privée de leurs employés, notamment en évitant la surveillance disproportionnée¹²⁷⁴;
- respecter une série de principes pour une utilisation responsable de l'IA générative¹²⁷⁵;
- adopter des mesures proactives pour limiter ou éliminer les nombreux risques associés à l'IA générative, notamment la génération d'images préjudiciables comme des images intimes non consensuelles ou des contenus diffamatoires impliquant des personnes réelles¹²⁷⁶.

4.4.3.4. La participation à des événements publics

Afin de rejoindre autrement les entreprises, la Commission a accru sa participation à des événements publics, soit en y offrant des présentations ou en participant à des panels, soit en y animant des kiosques favorisant des occasions d'échange.

Depuis 2021-2022, la Commission a pris part à pas moins de 95 événements, rejoignant ainsi plus de 20 000 personnes. Par exemple, elle a tenu des kiosques au Forum Cybereco et au Forum INCYBER Canada, de même qu'au Salon de l'emploi et de la formation continue et au Forum RH PME, en 2025. Sa présidente, ses vice-présidentes et des membres de son personnel ont aussi offert diverses présentations et ont participé à des panels à l'occasion d'événements comme le Canada Privacy Symposium de l'International Association of Privacy Professionals, la Semaine numériQC¹²⁷⁷ et des tables rondes organisées par des partenaires universitaires, comme l'Obvia et l'Institut intelligence et données de l'Université Laval, en plus d'offrir des conférences aux membres de certains regroupements d'entreprises. Notons en particulier que la Commission a accru le rythme de sa participation à des événements à partir de 2025-2026.

4.4.3.5. L'établissement de partenariats

Dès le dépôt du projet de loi devenu la Loi 25, les entreprises ont exprimé leurs inquiétudes en lien avec la mise en œuvre de certaines nouvelles obligations, faisant entre autres référence à la lourdeur des évaluations des facteurs relatifs à la vie privée ou au processus d'avis relatifs aux incidents de confidentialité. Des regroupements d'entreprises ont interpellé la Commission et les autorités politiques à ce sujet.

Afin de mieux comprendre les préoccupations exprimées, après l'adoption de la Loi, la Commission a rencontré des regroupements à plusieurs reprises. Dans plusieurs cas, les discussions ont mené à l'établissement de partenariats avec des acteurs comme le Conseil du patronat, les conseils québécois et canadien du commerce de détail, la Fédération des chambres de commerce du Québec et la Fédération canadienne de l'entreprise indépendante. Ces partenariats se sont traduits jusqu'ici par la diffusion des

vie privée et d'accès aux renseignements personnels », *Commissariat à la protection de la vie privée du Canada* (octobre 2023), en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-territoires/bg_231005_01/> (consulté le 19 janvier 2026).

¹²⁷⁴ COMMISSAIRES ET OMBUDS FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX À LA PROTECTION DE LA VIE PRIVÉE, « La protection de la vie privée des employés sur les lieux de travail modernes », *Commissariat à la protection de la vie privée du Canada* (octobre 2023), en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-territoires/res_231005_02/> (consulté le 10 janvier 2025).

¹²⁷⁵ COMMISSAIRES FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX À LA PROTECTION DE LA VIE PRIVÉE ET DES OMBUDSMANS RESPONSABLES DE LA PROTECTION DE LA VIE PRIVÉE, préc., note 1035.

¹²⁷⁶ DIVERSES AUTORITÉS MEMBRES DE L'ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, « Déclaration commune sur la protection de la vie privée et les images générées par l'intelligence artificielle », *Commissariat à la protection de la vie privée du Canada* (23 février 2026), en ligne : <https://www.priv.gc.ca/fr/nouvelles-du-commissariat/discours-et-declarations/2026/s-d_20260223_ia/> (consulté le 31 mars 2026).

¹²⁷⁷ Cet événement est désormais devenu le Rendez-vous numérique.

orientations et d'outils de la Commission par l'entremise des réseaux étendus de ces regroupements d'entreprises, de même que par certains webinaires et des articles informatifs publiés dans leurs bulletins d'information.

En parallèle, pour miser sur l'échange avec les parties prenantes et augmenter la portée de sa sensibilisation, la Commission a conclu divers partenariats avec des acteurs comme l'Ordre des conseillers en ressources humaines agréés, la Société québécoise d'information juridique (SOQUIJ) et la Commission des droits de la personne et des droits de la jeunesse (CDPDJ).

4.4.3.6. La sensibilisation dans les dossiers de surveillance

Lorsqu'elle examine les pratiques d'une entreprise dans le cadre de l'analyse préliminaire d'une plainte, d'une activité d'inspection ou d'une démarche d'enquête, ou encore à la suite de la réception d'un avis ou d'une entente, la Commission est en contact avec l'organisation en question. Elle profite de cette occasion d'avoir des échanges directs avec elle pour sensibiliser ses responsables aux obligations légales relatives à la protection des renseignements personnels.

Dans une majorité de situations, sans que les démarches formelles doivent se poursuivre, les entreprises conviennent de modifier leurs pratiques pour se conformer à la Loi. Bien que moins visible, il s'agit là d'une forme importante et efficace d'accompagnement¹²⁷⁸.

Notamment à la suite de modifications apportées par la Loi 25¹²⁷⁹ et en raison de l'accessibilité croissante des technologies biométriques, la Commission reçoit annuellement plus d'une centaine de divulgations de recours à la biométrie par les entreprises. Celles-ci projettent souvent de mettre en place des systèmes de contrôle des accès ou de gestion des heures de travail, par exemple.

Comme les lois prévoient de nombreuses obligations applicables en matière de biométrie¹²⁸⁰, la Commission examine de près ces avis reçus afin d'évaluer si les paramètres proposés semblent conformes au droit applicable. Par l'entremise de correspondances écrites et, souvent, d'échanges avec ses spécialistes, la Commission s'assure de sensibiliser les entreprises aux enjeux potentiels associés aux projets de biométrie lorsqu'elle en repère. Elle profite de ces conversations pour les informer des particularités du cadre légal et des orientations contenues dans ses décisions antérieures, ou encore de ses constats, en matière d'horodatage notamment¹²⁸¹.

Dans de nombreux cas, pour des considérations de protection de la vie privée, les entreprises reconsidèrent certains choix de paramétrage ou d'implantation des systèmes biométriques, ou choisissent finalement de ne pas aller de l'avant avec leur projet. Une intervention récente illustre bien la portée de cette sensibilisation effectuée par la Commission. Une grande entreprise comptant des milliers d'employés au Québec a avisé la Commission de l'implantation à venir d'un processus de validation de l'identité par reconnaissance faciale pour la vérification des antécédents. À la suite de la correspondance de la Commission l'informant de diverses

¹²⁷⁸ Dans ses rapports annuels 2020-2021 et 2021-2022, la Commission donnait certains exemples de ces interventions de sensibilisation : COMMISSION D'ACCÈS À L'INFORMATION, *Rapport annuel de gestion 2020-2021*, 2021, p. 43, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_RAAG_2020-2021.pdf>; COMMISSION D'ACCÈS À L'INFORMATION, préc., note 1186, p. 37-38.

¹²⁷⁹ Celles-ci ont porté sur les articles 44 et 45 de la LCCJTI.

¹²⁸⁰ Voir COMMISSION D'ACCÈS À L'INFORMATION, préc., note 1007.

¹²⁸¹ COMMISSION D'ACCÈS À L'INFORMATION, préc., note 1023.



considérations légales en lien avec ce projet, l'entreprise a réévalué la situation. Reconnaissante d'avoir été sensibilisée, elle a ultimement pris la décision de ne pas implanter ce nouveau processus. Étant donné le caractère éminemment sensible des renseignements biométriques, la vie privée de tous les candidats à de futurs emplois s'en trouve ainsi mieux protégée.

4.4.4. Conclusion

Malgré le travail accompli, d'importants défis subsistent pour tirer le maximum de bénéfices de la réforme apportée par la Loi 25, notamment en ce qui concerne la Loi sur le privé.

Ainsi, la Commission entend continuer d'explorer diverses pistes pour bonifier l'accompagnement des entreprises, comme :

- poursuivre la mise à jour de plusieurs documents publiés par la Commission à l'intention des entreprises;
- cibler les obligations dont la mise en œuvre pose des défis particuliers dans le secteur privé et évaluer le meilleur moyen de diffuser l'information pertinente pour assurer la conformité des pratiques;
- mettre en place un bulletin d'information afin de mettre en valeur de bonnes pratiques en matière de protection des renseignements personnels et des leçons tirées des décisions de sa section de surveillance;
- élaborer de nouvelles lignes directrices, pouvant porter par exemple sur l'usage des nouvelles technologies ou sur la communication de renseignements personnels à l'extérieur du Québec¹²⁸²;
- développer un outil d'auto-évaluation de conformité à la Loi sur le privé;
- évaluer la possibilité qu'un mécanisme de certification de la conformité des entreprises concernant certains pans de la Loi sur le privé soit développé;
- élaborer, en collaboration avec un ou plusieurs partenaires, une formation plus complète destinée aux PME;
- mettre en ligne de nouvelles capsules vidéo traitant de certains aspects plus précis du respect de la Loi;
- réaliser ou faire réaliser des inventaires ou des recherches permettant de mieux documenter la situation des entreprises et de répondre plus directement aux défis vécus sur le terrain.

Ces initiatives exigent plusieurs démarches, comme des analyses variées, la réalisation d'études et de sondages, l'établissement de liens avec les parties prenantes, la tenue occasionnelle de consultations, ainsi que la rédaction et la conception de tests éventuels auprès des utilisateurs. Ainsi, comme elle en fait état dans la section 4.1.1, la Commission doit composer avec des ressources actuelles qui lui imposent de prioriser ces initiatives et qui limitent la cadence à laquelle elle peut diffuser des outils. Sa fonction de promotion étant générale, elle doit tenir compte non seulement des centaines de milliers d'entreprises faisant affaire au Québec, mais également des neuf millions de citoyens, des quelque 2 600 organismes

¹²⁸² Les lignes directrices constituent un outil de choix auquel la Commission aimerait recourir davantage. Leur conception exige la collaboration de plusieurs experts à l'interne et à l'externe, dans une démarche qui requiert d'importants efforts. À titre illustratif, la Commission n'aurait pas été en mesure de mener de front la préparation d'autres lignes directrices et celle du présent rapport quinquennal, mobilisant déjà ses experts internes.



publics, des organismes du secteur de la santé et des services sociaux, des partis politiques et des chercheurs¹²⁸³. L'ensemble de ces groupes ont eux aussi de nouvelles obligations ou de nouveaux droits.

Compte tenu de ces éléments de contexte, la Commission continuera de privilégier la création de guides et de documents généraux ou sectoriels, dans l'objectif de rejoindre le plus grand nombre d'organisations possible, à un rythme compatible avec les ressources humaines et financières dont elle dispose.

Par ailleurs, la Commission doit noter que de nombreuses entreprises ont exprimé le besoin d'obtenir des réponses adaptées à leur contexte précis, voire des avis, dans un objectif de sécurité juridique, souhaitant ainsi bénéficier d'un service-conseil¹²⁸⁴. Bien qu'elle comprenne ce besoin et qu'elle reconnaisse que ce type de conseils serait certainement profitable aux entreprises, la Commission ne peut offrir un tel service. Tel que la loi est rédigée en ce moment, il pourrait en effet lui être impossible d'exercer ses fonctions de surveillance à l'égard des pratiques d'une entreprise à qui l'un de ses agents aurait préalablement fourni des conseils, celle-ci pouvant plaider avoir agi en suivant les recommandations de la Commission.

Pour terminer, à plusieurs occasions dans le présent rapport, la Commission rappelle combien les mesures adoptées dans la réforme du cadre de protection des renseignements personnels ont constitué un bond en avant. Elle invite même à les renforcer. En même temps, elle considère l'effet de ces avancées simultanément avec le besoin de s'assurer que la législation soit concrètement applicable par les entreprises. Ainsi, selon la Commission, l'application de plusieurs recommandations formulées dans le chapitre 2 de ce rapport contribuerait à alléger le fardeau perçu par les entreprises en lien avec l'application de la Loi sur le privé. Par exemple :

- dans la section 2.1.2, la Commission invite à reconsidérer l'approche procédurale de la protection des renseignements personnels qui caractérise actuellement la Loi sur le privé. Celle-ci impose aux entreprises de préparer une documentation abondante et de mener des réflexions complexes sur leurs activités impliquant des renseignements personnels. Des règles substantielles, plus claires, leur bénéficieraient. Il est ainsi plus aisé pour une entreprise de ne pas adopter une pratique lorsqu'elle est explicitement proscrite, avec l'assurance que ses concurrents se plient à la même règle.
- dans la section 2.1.7, la Commission explique que les situations déclenchant l'obligation de mener une évaluation des facteurs relatifs à la vie privée, procédure parmi celles jugées les plus lourdes par les entreprises, sont actuellement particulièrement fréquentes. Le resserrement de ces situations aiderait les entreprises à concentrer leurs efforts sur l'évaluation des projets les plus risqués ou dont l'ampleur est plus importante.

¹²⁸³ Voir la section 4.1.1.2.1.8.

¹²⁸⁴ Par exemple, l'homologue fédéral de la Commission en matière de vie privée offre des services de cet ordre : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Services-conseils aux entreprises » (27 octobre 2022), en ligne : <<https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/services-conseils-entreprises/>> (consulté le 17 avril 2026).

Table des recommandations du Rapport quinquennal 2026

L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS

Recommandation 1

Modifier les critères d'assujettissement à la Loi sur l'accès afin qu'elle soit applicable à toutes les organisations qui gravitent dans la sphère d'activités de l'État, d'un organisme public ou d'une municipalité, par exemple en s'assurant qu'elle vise les organisations dont :

- le fonds social est détenu en totalité ou en partie par l'État ou par un organisme public;
- le financement est en grande partie assumé par l'État ou par un organisme public, en adoptant un seuil de financement ou en visant des activités spécifiques qui sont ainsi financées;
- les activités correspondent à un service ou à une mission dont la responsabilité incombe à l'État, à un organisme public ou à une municipalité.

Recommandation 2

Effectuer, dans le cadre d'une réforme de la Loi sur l'accès, une révision globale de l'ensemble des dérogations à la Loi sur l'accès ou des régimes particuliers y suppléant adoptés par le législateur, notamment dans l'objectif :

- d'éliminer les dérogations et les régimes particuliers s'ils ne sont pas justifiés et nécessaires dans une optique d'intérêt public;
- de retirer du corpus législatif les dérogations similaires reprises dans plusieurs lois sectorielles en les remplaçant par une restriction générale directement prévue à la Loi sur l'accès;
- d'instaurer des normes, comme des critères, processus et outils, pour limiter et encadrer l'introduction de nouvelles dérogations ou de nouveaux régimes particuliers dans le futur.

Recommandation 3

Revoir dès que possible l'ensemble des régimes particuliers applicables en matière d'accès à l'information environnementale pour simplifier l'accès et maximiser la transparence, notamment en faisant rapidement entrer en vigueur les dispositions concernant la mise en place du registre public d'information environnementale introduit à la *Loi sur la qualité de l'environnement*.



Recommandation 4

Revoir l'ensemble des restrictions au droit d'accès pour en préciser la portée et en circonscrire l'utilisation, entre autres en :

- utilisant des termes moins subjectifs et englobants;
- s'assurant que les refus qui relèvent de la discrétion d'une personne autre que le responsable de l'accès de l'organisme public doivent eux aussi être motivés;
- prévoyant pour chaque restriction des conditions d'application et, le cas échéant, des situations où elles ne peuvent être invoquées;
- réunissant les restrictions visant à protéger les mêmes intérêts légitimes;
- revoyant la durée d'application des restrictions de manière à la réduire, lorsqu'elle est déjà prévue, ou à la limiter pour éviter l'application permanente de certaines restrictions.

Recommandation 5

Modifier la Loi sur l'accès de manière à étendre l'obligation de démontrer l'existence d'un préjudice à des intérêts légitimes afin qu'elle concerne l'ensemble des restrictions, qu'elles soient de nature facultative ou obligatoire.

Recommandation 6

Limiter le nombre de restrictions obligatoires au droit d'accès et les réserver aux seules situations visant à protéger un intérêt qui requiert une confidentialité quasi totale, en toutes circonstances.

Recommandation 7

Introduire à la Loi sur l'accès une disposition d'application générale établissant la primauté de l'intérêt public sur l'ensemble des restrictions au droit d'accès, laquelle :

- oblige un organisme public à donner accès à un renseignement lorsque l'intérêt public l'emporte clairement sur le préjudice potentiel lié à sa divulgation;
- contient une liste non exhaustive de facteurs à considérer dans l'évaluation de l'intérêt public.

Recommandation 8

Modifier le libellé de l'article 87 de la Loi sur l'accès afin de codifier clairement que les restrictions obligatoires au droit d'accès aux documents deviennent facultatives lorsqu'une personne demande l'accès à ses renseignements personnels.

Recommandation 9

Obliger les organismes publics à consulter de manière systématique les tiers concernés lorsqu'ils sont susceptibles d'invoquer les restrictions prévues aux articles 23 et 24 de la Loi sur l'accès.

Recommandation 10

Obliger les organismes publics à identifier le ou les tiers concerné(s) dans leur décision ou, lorsqu'il y a un enjeu de confidentialité associé à cette identification, les obliger à communiquer à la Commission, en cas de demande de révision, les coordonnées des tiers concernés dans un délai fixé par la Loi, accompagnées des motifs justifiant que leur identité soit traitée de façon confidentielle.



Recommandation 11

Modifier la Loi sur l'accès, et, par concordance, la Loi sur le privé et la LRSSS, afin que :

- le délai pour transmettre une décision en réponse à une demande d'accès aux documents ou aux renseignements personnels et motiver un refus sur la base d'une restriction facultative au droit d'accès soit de rigueur et emporte déchéance;
- le délai pour qu'une organisation puisse de mander de ne pas tenir compte d'une demande soit de rigueur et emporte déchéance.

Recommandation 12

Modifier la Loi sur l'accès et, par concordance, la Loi sur le privé et la LRSSS, pour permettre à la Commission d'interdire à une personne démontrant une utilisation abusive et répétée de son droit d'accès de formuler une demande d'accès auprès d'une organisation donnée sans l'autorisation de la présidence de la Commission et selon les conditions que celle-ci détermine.

Recommandation 13

Mandater un groupe de travail spécial, incluant notamment la Commission, des organismes publics et des représentants de la société civile, afin d'étudier l'opportunité de réviser les délais de traitement des demandes d'accès en tenant compte de l'équilibre devant être établi entre les attentes des demandeurs à l'information et la réalité opérationnelle des organismes publics dans le traitement effectif des demandes.

Recommandation 14

Prévoir à la Loi sur l'accès :

- un seuil minimal en matière d'allocation des ressources humaines et financières devant être dédiées aux tâches du responsable à l'accès aux documents;
- des obligations de formation initiale et continue du responsable de l'accès aux documents et du personnel qui le soutient, visant notamment des éléments de sensibilisation à l'importance du droit à l'accès et au devoir d'assistance envers le demandeur d'accès;
- des précisions quant au rôle et aux fonctions, en matière d'accès aux documents, du comité sur l'accès à l'information et la protection des renseignements personnels.

Recommandation 15

Modifier l'article 50 de la Loi sur l'accès afin que les décisions rendues par les responsables de l'accès :

- précisent le nombre et la nature des documents auquel l'accès est refusé, sous réserve que ces informations révèlent des informations sujettes à des restrictions obligatoires à l'accès;
- précisent le motif de refus pour chaque document ou partie de document auquel l'accès est refusé;
- précisent les alinéas ou les paragraphes des articles invoqués pour motiver le refus;
- associent des motifs de refus précis à chaque catégorie de documents demandés.

Recommandation 16

Assurer une uniformité en matière de gestion de l'information à l'échelle de l'administration publique par la modernisation de la *Loi sur les archives* ou, à défaut, par des modifications au cadre législatif en accès aux documents.



Recommandation 17

Intégrer à la Loi sur l'accès une disposition générale obligeant les organismes publics à documenter le processus menant à leurs décisions et à leurs actions importantes.

Recommandation 18

Étendre la portée du Règlement sur la diffusion afin qu'il vise tous les organismes publics assujettis à la Loi sur l'accès.

Recommandation 19

Créer un portail centralisé réunissant tous les documents diffusés par les organismes publics en vertu du Règlement sur la diffusion, mis à jour en continu et interrogeable par des fonctions de recherche.

Recommandation 20

Modifier le Règlement sur la diffusion de manière à uniformiser les pratiques de diffusion automatique, par exemple en :

- standardisant les formats de diffusion des documents et la structure de la section Web sur la diffusion de l'information;
- imposant l'utilisation d'un pictogramme et d'un libellé communs sur la page d'accueil du site Web des organismes publics pour rendre visible la section sur la diffusion de l'information;
- obligeant les organismes publics à tenir à jour, par l'entremise de cette section, une liste de tous les documents diffusés;
- exigeant que les hyperliens pointant vers des sites Web externes mènent directement vers les documents concernés plutôt que vers des sections génériques.

Recommandation 21

Étendre la liste de documents à diffuser automatiquement contenue au Règlement sur la diffusion en y ajoutant des catégories de documents telles que les suivantes :

- Rapports de sondage.
- Rapports d'évaluation des programmes.
- Documents et rapports produits en lien avec des consultations publiques.
- Liste de comités ministériels, interministériels, de concertation, consultatifs ou de même nature, de même que leur composition.
- Agenda des ministres, y compris leurs rencontres avec des acteurs non gouvernementaux.
- Partie accessible des dossiers soumis au Conseil des ministres.
- Avis, recommandations et analyses, après que la décision qu'ils appuient a été officiellement prise.

Recommandation 22

Retirer le critère subjectif de « l'intérêt pour l'information du public » du Règlement sur la diffusion en lien avec les études et les rapports de recherche ou de statistiques.

Recommandation 23

Exiger des organismes qu'ils évaluent périodiquement les autres documents qui devraient faire l'objet d'une diffusion proactive, par exemple en tenant compte du nombre de demandes d'accès les ayant visés.



Recommandation 24

Poursuivre les efforts visant la transparence des systèmes d'IA utilisés dans le secteur public en codifiant dans une loi ou un règlement, par exemple dans le Règlement sur la diffusion, les informations devant être diffusées sur chaque système envisagé ou déployé par un organisme public et en garantissant la tenue d'un registre centralisé des algorithmes.

Recommandation 25

Énoncer, dans le Règlement sur la diffusion, le principe de la « transparence dès la conception et par défaut », notamment en introduisant une obligation d'adopter un plan de diffusion proactive.

Recommandation 26

Renforcer, par voie législative ou réglementaire, la reddition de comptes en matière d'accès à l'information afin de la rendre :

- plus complète, en s'assurant qu'elle vise un maximum d'organismes publics;
- plus uniforme et plus précise, en s'assurant que les données à compiler par chaque organisme sont granulaires et produites suivant des normes prescrites qui facilitent leur exploitation et en fixant une période de référence commune;
- centralisée et transparente, en prévoyant que les données des organismes soient réunies dans une base de données unique, accessible, pouvant être interrogée par le public et dont la gestion serait confiée à la Commission.

LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Recommandation 27

Intégrer aux lois sur la protection des renseignements personnels un mécanisme permettant aux personnes concernées de formuler des indications de consentement automatisées, tout en prévoyant :

- une liste de protocoles permettant d'émettre de telles indications, comprise dans un règlement;
- le refus de consentir comme paramétrage par défaut de telles indications, si elles ne sont pas manuellement configurées par les personnes concernées;
- l'impossibilité que les éditeurs puissent redemander à la personne concernée de consentir si des indications ont déjà été données.

Recommandation 28

Obliger les organisations à résumer d'une façon simple et claire les faits saillants de leurs politiques de confidentialité, par exemple sous forme graphique, selon des modalités qui seraient déterminées par règlement.

Recommandation 29

Modifier les lois sur la protection des renseignements personnels afin que les organisations doivent fournir « juste à temps » les informations pertinentes à la prise de décision en matière de traitement de renseignements personnels, c'est-à-dire de manière contemporaine au choix.



Recommandation 30

Expliciter dans les lois que le critère de nécessité doit être évalué et respecté, non seulement pour la fin initiale pour laquelle la collecte est envisagée, mais également pour toute autre opération impliquant des renseignements personnels à travers leur cycle de vie.

Recommandation 31

Codifier expressément le test de nécessité dans les lois sur la protection des renseignements personnels.

Recommandation 32

Encadrer, par voie législative ou réglementaire, les renseignements pouvant être considérés nécessaires ou non dans le cadre de pratiques courantes et ayant des répercussions importantes dans la vie des citoyens, comme la collecte de renseignements personnels avant la location d'un logement ou la vidéosurveillance.

Recommandation 33

Intégrer explicitement les inférences faites par profilage au sein de la définition de renseignement personnel dans la Loi sur l'accès et la Loi sur le privé ainsi que dans la définition de renseignement de santé et de services sociaux prévue à la LRSSS.

Recommandation 34

Élargir la portée de la notion de renseignement personnel dans les lois québécoises, par exemple :

- en remplaçant le critère d'identification par un critère plus englobant; ou
- en ajoutant des critères complémentaires à l'identification.

Recommandation 35

Préciser que la création et l'inférence de renseignements personnels sont assimilables à une collecte pour l'application des lois sur la protection des renseignements personnels.

Recommandation 36

Modifier les lois afin que les obligations d'information des organisations s'appliquent également à la création et à l'inférence de renseignements personnels.

Recommandation 37

Requérir le consentement du titulaire de l'autorité parentale ou du tuteur d'un mineur de moins de 14 ans pour que des inférences algorithmiques soient produites à son sujet, à moins que ces inférences soient manifestement à son bénéfice.

Recommandation 38

Modifier les lois sur la protection des renseignements personnels de manière à définir et à encadrer le moissonnage de renseignements personnels.

Recommandation 39

Prévoir un encadrement législatif pour l'ensemble des entreprises faisant le commerce de renseignements personnels, passant notamment par :



- l'extension, à tous les courtiers en données, des règles particulières de la Loi sur le privé applicables aux agents de renseignements personnels;
- l'introduction d'une obligation, pour les courtiers en données, de déclarer à la Commission toute activité de moissonnage;
- la mise en place d'un registre public des courtiers en données qui collectent des renseignements personnels concernant des Québécois, comportant notamment des informations sur les types de renseignements vendus, les coordonnées de leur siège social ou de leurs établissements au Québec ainsi qu'un lien vers un site Web qui détaille la manière d'exercer ses droits en matière de protection des renseignements personnels;
- la mise en place d'un guichet unique gouvernemental permettant à toute personne d'exercer ses droits simultanément auprès de tous les courtiers en données enregistrés.

Recommandation 40

Préciser l'encadrement législatif applicable en matière d'anonymisation afin que :

- le Règlement sur l'anonymisation s'applique à toutes les démarches d'anonymisation, peu importe le moment du cycle de vie du renseignement personnel auquel elles sont réalisées;
- l'autorité réglementaire puisse prévoir des règles s'appliquant aux renseignements une fois qu'ils ont été anonymisés, à travers tout leur cycle de vie subséquent, notamment en ce qui concerne la communication;
- l'autorité réglementaire puisse exclure la possibilité d'anonymiser certains types de renseignements personnels.

Recommandation 41

Clarifier l'arrimage du standard d'anonymisation entre le Règlement sur l'anonymisation et les lois et préciser, dans le Règlement, une méthode d'évaluation du risque ou une échelle de niveau de risque.

Recommandation 42

Ajouter une balise à la LRSSS pour restreindre l'utilisation possible des renseignements anonymisés, soit pour les seules fins d'intérêt public dans le cas des établissements du secteur public, et pour des fins sérieuses et légitimes dans le cas des établissements du secteur privé.

Recommandation 43

Prévoir :

- un pouvoir réglementaire permettant d'interdire en tout ou en partie la diffusion de renseignements anonymisés;
- une mention explicite, dans la Loi sur l'accès, que les renseignements anonymisés sont exclus de la portée du droit d'accès aux documents.

Recommandation 44

Mieux définir l'EFVP dans les lois pour qu'il y soit explicitement indiqué que cette évaluation :

- a pour objectif fondamental la protection des personnes concernées;
- doit porter en premier lieu sur leur droit à la vie privée, mais également sur leurs autres droits et libertés susceptibles d'être affectés par le traitement de leurs renseignements personnels;
- doit toujours comporter trois volets, à savoir :



- l'analyse de la conformité légale du projet;
- l'évaluation des risques soulevés par le projet à l'égard du droit à la vie privée et des autres droits et libertés des personnes concernées;
- la mise en place de mesures d'atténuation de ces risques.

Recommandation 45

Prévoir que l'EFVP s'accompagne d'une analyse d'impact algorithmique lorsqu'elle concerne un système d'IA visant la prise de décision automatisée concernant les personnes.

Recommandation 46

Préciser dans la Loi sur l'accès et la Loi sur le privé quelle entité est ultimement responsable de l'EFVP lorsque plusieurs parties sont impliquées, notamment :

- en indiquant qu'il s'agit de l'organisation ayant la détention juridique des renseignements personnels concernés;
- en encadrant la collaboration des parties pour la réalisation de l'EFVP.

Recommandation 47

Harmoniser la LRSSS, la Loi sur l'accès et la Loi sur le privé en ce qui concerne l'entité ultimement responsable de l'EFVP lorsque plusieurs parties sont impliquées.

Recommandation 48

Regrouper les dispositions concernant l'EFVP pour en simplifier l'application et en préciser les modalités par règlement.

Recommandation 49

Prévoir des circonstances dans lesquelles les organismes publics sont tenus de consulter, lors de l'étape d'évaluation des risques de la démarche d'EFVP, un comité représentatif des personnes concernées par un projet et de tenir compte de sa contribution.

Recommandation 50

Revoir la portée des situations dans lesquelles une EFVP est obligatoire, notamment :

- en y ajoutant des conditions d'application;
- en définissant les termes utilisés.

Recommandation 51

Prévoir un pouvoir réglementaire permettant au gouvernement d'établir une liste de situations :

- exigeant toujours une EFVP;
- exemptées d'EFVP.

Recommandation 52

Ajouter à la Loi sur l'accès, à la Loi sur le privé et à la LRSSS des manquements précis visant le fait de ne pas avoir réalisé une EFVP lorsqu'elle est requise.



Recommandation 53

Prévoir des circonstances où les organismes publics sont tenus de diffuser proactivement un condensé de l'EFVP menée.

Recommandation 54

Obliger les organisations à tenir un registre interne d'EFVP, en prescrivant le contenu de ce registre dans un règlement.

Recommandation 55

Interdire explicitement le recours aux interfaces truquées ayant un effet sur la protection des renseignements personnels.

Recommandation 56

Interdire explicitement le recours aux conceptions addictogènes sur les plateformes et sur les médias sociaux couramment fréquentés par des mineurs.

Recommandation 57

Concrétiser les recommandations mises de l'avant par la Commission en matière de protection des jeunes dans l'environnement numérique, notamment :

- en intégrant la notion d'intérêt supérieur des jeunes dans les lois sur la protection des renseignements personnels;
- en interdisant explicitement la collecte, l'utilisation ou la communication des renseignements personnels d'un mineur dans le but de faire de la publicité commerciale, d'influencer son comportement ou ses décisions dans un contexte commercial ou à toute autre fin présumément ou effectivement préjudiciable;
- en interdisant explicitement la vente de renseignements personnels d'un mineur;
- en imposant aux organisations un devoir particulier de protection envers les mineurs;
- en exigeant que l'évaluation de projets impliquant des renseignements personnels de mineurs tienne compte des effets potentiels sur l'ensemble de leurs droits fondamentaux;
- en encadrant davantage la conception des produits et services numériques utilisés par les mineurs.

Recommandation 58

Intégrer les dispositions concernant la biométrie prévues aux articles 44 à 45 de la LCCJTI aux lois générales sur la protection des renseignements personnels.

Recommandation 59

Organiser un vaste dialogue public sur le futur de la protection des renseignements personnels à l'ère numérique en impliquant des acteurs de tous horizons, par exemple par le biais d'une commission spéciale, en vue de parvenir à une nouvelle approche permettant de compléter le modèle actuel.

Recommandation 60

Poursuivre les initiatives de coopération nationale et internationale sur les questions liées au numérique et à la protection des renseignements personnels.



Recommandation 61

Considérer, au sein de la réflexion sur l'avenir de la protection des renseignements personnels, l'adoption d'interdictions ou d'autorisations plus explicites en matière de traitement de renseignements personnels.

Recommandation 62

Considérer, au sein de la réflexion sur l'avenir de la protection des renseignements personnels, l'adoption de nouveaux modèles de gouvernance des données permettant une gestion collective des renseignements personnels, en réponse aux limites du paradigme du contrôle individuel, et l'imposition de devoirs aux parties disposant d'un pouvoir dominant.

Recommandation 63

Considérer, au sein de la réflexion sur l'avenir de la protection des renseignements personnels, l'imposition de contrôles en amont concernant les technologies de l'information impliquant des renseignements personnels.

Recommandation 64

Considérer, au sein de la réflexion sur l'avenir de la protection des renseignements personnels, de viser explicitement dans les lois sur la protection des renseignements personnels toutes les étapes de conception et de production de technologies impliquant de tels renseignements.

LA LOI SUR LES RENSEIGNEMENTS DE SANTÉ ET DE SERVICES SOCIAUX

Recommandation 65

Rendre applicables les protections prévues à la LRSSS en accélérant la mise en place des outils, des procédures et des infrastructures technologiques requis afin, notamment, d'assurer l'identification et l'authentification des intervenants du secteur de la santé et des services sociaux.

Recommandation 66

Prendre les actions nécessaires afin qu'entre en vigueur l'article 103 de la LRSSS, qui prévoit l'obligation pour un organisme du secteur de la santé et des services sociaux de journaliser l'ensemble des accès aux renseignements de santé et de services sociaux qu'il détient ou de toute autre utilisation ou communication de ces renseignements.

Recommandation 67

Ajouter à la LRSSS des critères permettant de circonscrire la notion de « cabinet privé de professionnel » contenue au paragraphe 1^o de l'annexe II de cette Loi afin de mieux définir son champ d'application.

Recommandation 68

Interdire formellement toute possibilité pour les organismes du secteur de la santé et des services sociaux, qu'ils soient publics ou privés, de participer à toute vente ou aliénation d'un renseignement de santé et de services sociaux.



Recommandation 69

Baliser davantage le consentement en matière de recherche dans le domaine de la santé et des services sociaux.

Recommandation 70

Prévoir à la LRSSS une disposition transitoire, inspirée de celle du deuxième alinéa de l'article 261, visant à assurer que les mandats et les contrats de service ou d'entreprise conclus en vertu de la Loi sur le privé avant l'entrée en vigueur de la LRSSS viennent à échéance au terme d'une période de transition déterminée.

LA COMMISSION D'ACCÈS À L'INFORMATION

Recommandation 71

Octroyer à la Commission le budget et les effectifs requis pour qu'elle remplisse pleinement et efficacement sa mission, compte tenu notamment de :

- l'importance des droits qu'elle protège;
- l'ampleur, de la variété et de l'expansion récente de ses fonctions;
- l'évolution rapide du contexte technologique.

Recommandation 72

Garantir l'indépendance administrative de la Commission, notamment en rattachant son budget et ses effectifs au Bureau de l'Assemblée nationale.

Recommandation 73

Retirer de la Loi sur l'accès, de la Loi sur le privé et de la LRSSS les dispositions relatives à l'appel devant la Cour du Québec des décisions émanant de la section juridictionnelle de la Commission pour qu'elles soient directement soumises au contrôle judiciaire de la Cour supérieure.

Recommandation 74

Réviser les dispositions de la Loi sur le privé prévoyant la possibilité d'imposer des sanctions administratives pécuniaires pour :

- préciser que l'application de ces sanctions ne vise clairement que les manquements de type objectif;
- ajouter des manquements de type objectif qui ne sont pas actuellement visés.



Annexe 1 – Table des recommandations du Rapport quinquennal 2016

UN CARACTÈRE PRÉPONDÉRANT À RÉAFFIRMER

Recommandation 1 : Mettre sur pied une commission parlementaire visant à réaffirmer le statut prépondérant de la Loi sur l'accès et de la Loi sur le privé et à déterminer les dispositions législatives dérogatoires qui devraient être abrogées, maintenues ou modifiées.

Recommandation 2 : Soumettre l'adoption de toute nouvelle dérogation à la Loi sur l'accès et à la Loi sur le privé à un processus de consultation publique obligatoire permettant d'obtenir l'avis des citoyens, des groupes et des organismes concernés.

POUR UNE PLUS GRANDE TRANSPARENCE DES ORGANISMES PUBLICS

Recommandation 3 : Modifier la Loi sur l'accès afin qu'un plus grand nombre d'organismes y soient assujettis, notamment en s'inspirant des critères retenus par d'autres juridictions.

Recommandation 4 : Revoir l'ensemble des restrictions énoncées dans la Loi sur l'accès afin :

- D'en prescrire plus précisément la portée et d'en limiter la durée. Certaines restrictions pourraient également être assorties d'une liste de situations dans lesquelles elles ne peuvent être invoquées pour justifier un refus de communiquer une information;
- De prévoir des conditions d'application faisant référence à un risque de préjudice aux intérêts qu'elles visent à protéger et non à la seule nature ou à la provenance du document;
- De limiter le nombre de restrictions obligatoires aux seules situations visant à protéger un intérêt qui requiert une confidentialité quasi totale, en toutes circonstances;
- D'inclure une disposition applicable à l'ensemble des restrictions, prévoyant la primauté de l'intérêt public, de façon à obliger l'organisme à donner accès au renseignement lorsque l'intérêt public l'emporte clairement sur le préjudice susceptible de découler de sa divulgation. Cette disposition pourrait s'accompagner de l'obligation que soit prise en compte une liste non exhaustive de facteurs dans l'évaluation de l'intérêt public.

Recommandation 5 : Modifier la Loi sur l'accès pour préciser les obligations d'un organisme public concernant l'accès à des renseignements contenus dans un document informatisé, plus précisément dans une base de données.

Recommandation 6 : Inclure dans la loi une disposition générale obligeant les organismes publics à créer des documents dans le but d'étayer le processus décisionnel (réflexions, délibérations, mesures et décisions importantes), assortie de sanctions appropriées en cas de non-conformité.



Recommandation 7 : Modifier la Loi sur l'accès afin d'attribuer à la Commission une plus grande marge de manœuvre dans l'application de l'article 137.1 et prévoir que cette disposition ne peut être invoquée que dans les délais de 20 ou 30 jours prévus par la loi.

Recommandation 8 : Favoriser l'instauration d'une culture de transparence au sein des ordres professionnels, à l'égard des renseignements concernant les enquêtes des syndicats.

Recommandation 9 : À cette fin, remplacer les mots « dont la divulgation est susceptible de révéler le contenu d'une enquête ou d'avoir un effet sur une enquête à venir, en cours ou sujette à réouverture », au deuxième alinéa de l'article 108.3 du Code des professions, par des critères similaires à ceux prévus à l'article 28 de la Loi sur l'accès, applicables aux organismes publics chargés de détecter ou de réprimer le crime.

Recommandation 10 : Rétablir l'équilibre entre le droit au secret professionnel et le droit d'accès aux documents des organismes publics prévu à l'article 9 de la Loi sur l'accès en précisant la portée du secret professionnel dans le contexte de l'objectif de transparence visé par la Loi sur l'accès.

Recommandation 11 : Concilier le droit au secret professionnel avec le droit de la personne de recevoir communication des renseignements personnels détenus à son sujet par les organismes publics et les entreprises.

Recommandation 12 : Modifier la Loi afin que le secret professionnel ne puisse être invoqué par les organismes publics pour empêcher la divulgation du montant total des honoraires d'un avocat sauf dans le cas où cette divulgation est clairement susceptible de divulguer une information autrement protégée par le secret professionnel.

Recommandation 13 : À l'instar des lois des autres provinces canadiennes, moduler la protection des renseignements personnels dans le cadre des demandes d'accès afin de prévoir que ceux-ci peuvent être communiqués lorsque leur divulgation ne constitue pas une atteinte déraisonnable au droit à la vie privée des tiers.

Recommandation 14 : Préciser certains critères à considérer dans cette évaluation.

Recommandation 15 : Prévoir des situations où la divulgation est présumée être une atteinte déraisonnable et celles où elle ne l'est pas.

Recommandation 16 : Inclure la divulgation de renseignements aux proches parents d'une personne décédée pour des motifs de compassion parmi les éléments qui sont présumés ne pas constituer une atteinte déraisonnable à la vie privée.

Recommandation 17 : Prévoir un mécanisme de consultation et d'avis aux tiers, au besoin, et leur recours à la Commission.

Recommandation 18 : Afin que les renseignements personnels et les droits des personnes faisant l'objet de vérifications d'antécédents judiciaires et d'autres vérifications de même nature soient mieux protégés, la Commission invite le législateur et le gouvernement à adopter un cadre législatif ou réglementaire visant à :

- Limiter les circonstances permettant de telles vérifications et préciser les critères d'appréciation de l'infraction reliés à la nature des fonctions, de façon à uniformiser les pratiques dans les organismes responsables de ces vérifications;



- Limiter et encadrer l'utilisation de renseignements personnels qui ne se trouvent pas aux plumitifs aux fins de ces vérifications;
- Limiter l'utilisation des résultats de ces vérifications par l'organisme ou l'entreprise qui reçoit ces renseignements;
- Permettre l'accessibilité des personnes aux renseignements personnels les concernant, reliés à ces vérifications, afin de favoriser l'exercice du droit de rectification prévu dans la Loi sur l'accès.

Recommandation 19 : Clarifier et uniformiser les régimes d'accessibilité aux rapports d'enquête de harcèlement en milieu de travail, y compris en ce qui concerne la compétence de la Commission de rendre des décisions à ce sujet.

POUR UN RENFORCEMENT DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LES SECTEURS PUBLIC ET PRIVÉ

Recommandation 20 : Inclure une obligation de responsabilité des entreprises dans la Loi sur le privé.

Recommandation 21 : Modifier la Loi sur le privé afin qu'elle prévoie la désignation d'un responsable de l'accès et de la protection des renseignements personnels et la diffusion publique de son nom et de ses coordonnées.

Recommandation 22 : Modifier l'article 72 de la Loi sur le privé afin :

- D'obliger les agents de renseignements personnels à informer la Commission dans les 30 jours suivant le changement de leurs coordonnées;
- D'obliger les agents de renseignements personnels qui prévoient cesser leurs activités à en aviser la Commission par écrit.

Recommandation 23 : Modifier les articles 76 et 79 de cette même loi afin que les avis publics que doivent publier les agents de renseignements personnels et la Commission puissent être diffusés sur Internet.

Recommandation 24 : Retirer la notion de « dossier » de la Loi sur le privé et articuler les obligations des entreprises autour de la finalité de la collecte des renseignements personnels.

Recommandation 25 : Modifier l'article 8 de la Loi sur le privé afin de préciser :

- Le moment où l'information doit être donnée à la personne concernée (selon que l'information est colligée auprès d'elle ou d'un tiers, à son insu ou non);
- D'y inclure une obligation d'informer la personne des renseignements personnels qui seront recueillis et des moyens par lesquels ils seront recueillis;
- Que cette information doit être claire, compréhensible et accessible quel que soit le support utilisé pour recueillir les renseignements personnels.

Recommandation 26 : Modifier la Loi sur le privé afin qu'elle prévoie que les renseignements liés à l'exercice de fonctions dans une entreprise ne sont pas des renseignements personnels.

Recommandation 27 : Modifier la Loi sur l'accès et la Loi sur le privé pour :



- Prévoir que la communication de renseignements sensibles ou leur utilisation à d'autres fins qu'à celles de leur collecte ne soit possible qu'avec le consentement explicite de la personne concernée ou l'autorisation de la loi;
- Encadrer davantage la collecte et l'utilisation des renseignements personnels concernant les jeunes.

Recommandation 28 : Intégrer les critères du consentement prévus dans la Loi sur le privé à la Loi sur l'accès.

Recommandation 29 : Modifier la Loi sur l'accès et la Loi sur le privé pour y préciser les exigences liées à ces critères.

Recommandation 30 : Modifier la Loi sur l'accès et la Loi sur le privé pour qu'elles précisent que le consentement ne permet pas une collecte de renseignements personnels non nécessaires.

Recommandation 31 : Modifier l'article 14 de la Loi sur le privé afin qu'il précise que le consentement à la collecte qui y est mentionné est celui prévu à l'article 6 de cette loi, soit le consentement à ce qu'un renseignement soit recueilli auprès d'un tiers.

Recommandation 32 : Modifier la Loi sur l'accès et la Loi sur le privé de façon à ce que le consentement puisse être retiré en tout temps, sous réserve de restrictions prévues par la loi.

Recommandation 33 : Légiférer afin d'interdire la collecte, l'utilisation et la communication des renseignements génétiques à des fins autres que médicales, scientifiques ou judiciaires.

Recommandation 34 : Référer, dans la Loi sur l'accès et la Loi sur le privé, aux dispositions de la Loi concernant le cadre juridique des technologies de l'information concernant la biométrie.

Recommandation 35 : Ajouter une obligation selon laquelle la déclaration de création d'une banque de caractéristiques ou de mesures biométriques doit être déposée à la Commission soixante (60) jours avant sa mise en service.

Recommandation 36 : Obliger les organismes publics et les entreprises qui envisagent d'implanter un procédé permettant de saisir des caractéristiques ou des mesures biométriques à faire une évaluation préalable des risques et des impacts sur la vie privée et sur la protection des renseignements personnels avant la mise en activité du système et à en effectuer un suivi tout au long de son utilisation.

Recommandation 37 : Établir des mesures d'entreposage et de conservation des caractéristiques ou mesures biométriques propres à assurer leur confidentialité, notamment, lorsque la technologie le permet, en :

- imposant l'anonymisation irréversible des caractéristiques ou des mesures biométriques immédiatement après qu'elles aient été collectées (la conversion de l'image de la donnée biométrique brute en formule codée peut être utilisée à cette fin);
- exigeant la destruction de la caractéristique ou de la mesure originale brute une fois le processus d'anonymisation terminé;
- obligeant l'utilisation d'un support externe, individuel ou portable, pour la conservation des caractéristiques ou des mesures biométriques anonymisées, sous le contrôle de la personne concernée;
- prévoyant que la base de données soit locale plutôt que centralisée, lorsque sa création est absolument nécessaire.



Recommandation 38 : Modifier la Loi sur l'accès et la Loi sur le privé afin que l'obligation de déclarer à la Commission les incidents de sécurité portant sur des renseignements personnels y soit ajoutée et définir les conditions et les modalités de cette obligation de déclaration.

Recommandation 39 : Modifier la Loi sur l'accès et la Loi sur le privé afin que les organismes publics et les entreprises soient obligés de notifier les personnes concernées lors de la survenance d'un incident de sécurité portant sur des renseignements personnels.

Recommandation 40 : Modifier la Loi sur l'accès et la Loi sur le privé afin que [l]es pouvoirs d'intervention [de la Commission] en matière d'incidents de sécurité portant sur des renseignements personnels soient renforcés et qu'elles lui attribuent un pouvoir d'émettre des ordonnances visant à protéger les droits des personnes concernées, selon des critères similaires à ceux d'une ordonnance de sauvegarde, ainsi qu'un pouvoir d'ordonner la remise ou la destruction des renseignements personnels aux personnes qui sont en possession de ceux-ci sans droit.

Recommandation 41 : Modifier la Loi sur le privé afin d'y ajouter une disposition visant à obliger les entreprises à détruire les renseignements personnels une fois que les fins pour lesquelles ils ont été recueillis sont accomplies, sous réserve des obligations contenues dans d'autres lois.

Recommandation 42 : Modifier la Loi sur le privé afin que les entreprises soient obligées de conserver les renseignements ayant servi à prendre une décision concernant une personne pendant un an suivant cette décision, et ce, afin de préserver les droits d'accès de cette personne.

Recommandation 43 : Supprimer les mots « ou par un calendrier de conservation établi par règlement du gouvernement » à l'article 12 de la Loi sur le privé.

Recommandation 44 : Abroger le paragraphe 3° de l'article 90 de la Loi sur le privé.

Recommandation 45 : Modifier la Loi sur le privé afin qu'une disposition soit ajoutée à la section VI de cette loi quant au délai de conservation des renseignements personnels détenus par les agents de renseignements personnels.

Recommandation 46 : Modifier les articles 59 et 125 de la Loi sur l'accès et 18 et 21 de la Loi sur le privé afin que l'autorisation préalable de la Commission soit éliminée et prévoir, notamment :

- Que la demande du responsable de la recherche doit être faite par écrit auprès de l'organisme ou de l'entreprise qui détient les renseignements nécessaires à la réalisation de la recherche et identifier ces renseignements.
- Que l'organisme ou l'entreprise peut communiquer les renseignements personnels, sans obtenir le consentement des personnes concernées, seulement si les critères suivants sont satisfaits :
 - L'objectif de la recherche ne peut être atteint que si les renseignements sont communiqués sous une forme qui pourrait permettre d'identifier les personnes concernées;
 - Il est déraisonnable d'exiger du chercheur qu'il obtienne le consentement des personnes concernées;
 - La divulgation et l'utilisation des renseignements personnels par le chercheur dans le cadre de sa recherche ne sont pas préjudiciables aux personnes concernées par les renseignements et les bénéfices attendus de la recherche sont clairement dans l'intérêt public;
 - Les renseignements personnels seront utilisés d'une manière qui en assure la confidentialité.
- Qu'une entente doit être conclue entre le chercheur et l'organisme ou l'entreprise qui prévoit notamment que :



- Les mesures de sécurité adéquates seront mises en place de manière à ce que le caractère confidentiel des renseignements communiqués soit assuré en tout temps, et ce, peu importe leur support et quelle que soit la forme sous laquelle ils sont détenus;
 - Les renseignements personnels communiqués ne seront accessibles qu'aux personnes à qui ils sont nécessaires pour l'exécution de leurs fonctions et qui ont signé au préalable un engagement à la confidentialité;
 - Les renseignements permettant d'identifier les personnes devront être retirés à la première occasion raisonnable;
 - Les renseignements ne seront pas utilisés à des fins différentes de la communication prévue au protocole de recherche transmis avec la demande d'obtention des renseignements;
 - Les renseignements seront conservés séparément de tout autre fichier de renseignements non prévus au protocole de recherche, notamment de fichiers reçus dans le cadre d'autres recherches;
 - Les renseignements personnels ne seront pas communiqués, publiés ou autrement diffusés sous une forme permettant d'identifier les personnes concernées;
 - Les détails concernant l'information et le formulaire de consentement que le chercheur doit transmettre aux personnes soient prévus, dans le cas où la demande de communication a pour objet d'entrer en contact avec les personnes concernées;
 - L'organisme public ou l'entreprise et la Commission seront informés sans délai si les conditions prévues à l'entente n'auront pas été observées ainsi que de tout manquement aux mesures de sécurité et de tout événement susceptible de porter atteinte au caractère confidentiel des renseignements;
 - Les renseignements communiqués devront être détruits une fois la recherche complétée, et un avis de la destruction des renseignements devra être transmis à l'organisme public ou à l'entreprise.
- Que cette communication doit être inscrite au registre des communications de l'organisme public détenteur des renseignements et qu'une entreprise a l'obligation de diffuser des informations similaires sur son site Internet.

Recommandation 47 : Harmoniser les dispositions des lois sectorielles en conséquence.

Recommandation 48 : Modifier ces lois afin que les organisations pour lesquelles travaillent les chercheurs soient également responsables et imputables de la protection des renseignements personnels communiqués à des fins de recherche.

Recommandation 49 : Encadrer la constitution et l'utilisation des biobanques et des renseignements génétiques à des fins de recherche. Cet encadrement devrait inclure des règles visant à assurer la protection des renseignements personnels qu'elles contiennent, notamment quant au consentement des personnes concernées, à la confidentialité des données, à leur utilisation et à leur communication, notamment à l'extérieur du Québec, et à la transparence des informations au sujet de leur existence, de leur durée et de l'utilisation des renseignements qu'elles contiennent.

Recommandation 50 : Modifier l'article 67 de la Loi sur l'accès afin de préciser qu'il ne s'applique pas si la communication est prévue à l'article 68.

Recommandation 51 : Regrouper sous deux articles les communications prévues dans ces dispositions en intégrant l'article 68.1 dans les situations énumérées à l'article 68.

Recommandation 52 : Prévoir que les communications visées par ce nouvel article 68 doivent respecter les critères suivants :



- L'objectif de la communication ne peut être atteint que si les renseignements sont communiqués sous une forme permettant d'identifier la personne concernée et seuls les renseignements nécessaires sont communiqués;
- Il est déraisonnable d'exiger le consentement des personnes concernées ou d'envisager un autre moyen d'atteindre l'objectif de cette communication;
- Les risques d'atteinte à la vie privée découlant de l'utilisation des renseignements personnels sont minimisés et les bénéfices découlant de cette communication sont dans l'intérêt public ou surpassent nettement l'atteinte aux droits des personnes concernées résultant de cette communication;
- Une entente encadrant la communication des renseignements personnels est conclue et contient minimalement les éléments prévus actuellement par l'article 68, al. 2 de la Loi sur l'accès.

Recommandation 53 : Préciser, à l'article 70 de la Loi sur l'accès, que les communications prévues à l'article 68 de la Loi sur l'accès doivent être soumises à la Commission pour avis et que cette demande d'avis doit inclure :

- Une copie de l'entente;
- Un document précisant :
 - L'objectif de la communication de renseignements personnels;
 - La disposition de la Loi sur l'accès et celles d'une autre loi en vertu desquelles l'organisme considère être autorisé à communiquer les renseignements personnels sans le consentement des personnes concernées;
 - Les précisions permettant à la Commission d'évaluer l'application de cette disposition;
 - Les moyens pris par l'organisme pour informer les personnes concernées de cette communication (transparence du processus);
 - Les informations permettant à la Commission d'évaluer le respect des critères énoncés à l'article 68;
 - Pour les communications susceptibles d'avoir un impact important sur la vie privée des personnes concernées, inclure une évaluation des impacts sur la vie privée des personnes concernées qui comprend notamment les moyens pris par les organismes pour les atténuer. Ces situations visent notamment : les communications visant un nombre important de renseignements personnels, la communication de renseignements sensibles ou l'ensemble d'une banque de données aux fins de les comparer ou de les inclure dans une autre banque, notamment aux fins de prendre une décision concernant les personnes concernées.

Recommandation 54 : Prévoir que seuls les avis défavorables de la Commission doivent être motivés.

Recommandation 55 : Modifier les délais suivant lesquels la Commission doit donner son avis, afin qu'ils soient suspendus lorsque la demande est incomplète ou que des informations additionnelles sont requises. Prévoir également l'envoi d'un avis d'intention lorsque la Commission envisage d'émettre un avis défavorable et permettre aux parties à l'entente de faire valoir leur point de vue par écrit ou de modifier l'entente.

Recommandation 56 : Modifier la Loi sur l'accès et la Loi sur le privé afin que les organismes publics et les entreprises soient obligés de réaliser une analyse des impacts et des risques concernant la protection des renseignements personnels avant toute communication de renseignements personnels à l'extérieur du Québec.

Recommandation 57 : Modifier la Loi sur l'accès et la Loi sur le privé afin que les organismes publics et les entreprises soient obligés de conclure un contrat avec l'entité publique ou privée à laquelle les renseignements personnels seront communiqués ou confiés et d'y inclure les mesures requises pour que les impacts et les risques identifiés dans l'analyse soient atténués.



Recommandation 58 : Harmoniser les dispositions de la Loi sur l'accès et de la Loi sur le privé concernant la communication à l'extérieur du Québec avec l'article 26 de la LCCJT.

Recommandation 59 : S'assurer du respect de la protection des renseignements personnels lorsque le gouvernement du Canada ou du Québec négocie des partenariats ou des traités commerciaux ou autres avec d'autres juridictions.

Recommandation 60 : Relancer la réflexion sur la recherche de l'équilibre entre le respect de la vie privée et la collecte, l'utilisation et la diffusion de renseignements personnels à des fins généalogiques ou historiques et modifier la législation en tenant compte de l'ensemble du cadre juridique applicable.

LES DONNÉES OUVERTES

Recommandation 61 : Adopter le principe de l'ouverture par défaut des données détenues par les organismes publics, sous réserve de motifs légitimes justifiant que certaines données ne peuvent être diffusées, motifs qui doivent être connus du public.

Recommandation 62 : Faire connaître de manière plus précise la politique du gouvernement ou son plan d'action en matière de diffusion de données ouvertes, y compris les priorités de diffusion, et clarifier le cadre de gouvernance qu'il entend mettre en œuvre. Le principe de priorisation de données ouvertes favorisant la démocratie et la transparence devrait guider le Gouvernement du Québec dans son initiative en la matière.

Recommandation 63 : L'adoption d'une politique ou d'un plan d'action du gouvernement en matière de diffusion de données ouvertes devrait préciser si les banques de données contenant des renseignements personnels anonymisés ou des renseignements personnels à caractère public peuvent être diffusées tout en mentionnant les motifs à l'appui de cette décision.

Recommandation 64 : Restreindre clairement, dans la politique du gouvernement ou dans son plan d'action concernant les données ouvertes, la diffusion des renseignements personnels à caractère public considérant les dispositions actuellement en vigueur concernant les renseignements personnels à caractère public.

Recommandation 65 : Dans la mesure où le gouvernement souhaite diffuser, dans un format anonymisé, des jeux de données contenant des informations au sujet d'individus, que les licences d'utilisation soient adaptées en conséquence, notamment en interdisant expressément toute réutilisation qui vise à réidentifier une personne et en prévoyant une clause de suspension du droit de réutilisation, ainsi que la suppression ou le rapatriement des banques de données compromises.

Recommandation 66 : Si l'intention du gouvernement est de diffuser, dans un format anonymisé, des jeux de données contenant des informations au sujet d'individus, mettre sur pied un réseau d'experts en cette matière, dont pourraient bénéficier les organismes publics. Ce réseau d'experts pourrait :

- accompagner les organismes dans :
 - l'anonymisation de banques de données contenant des renseignements personnels, notamment par l'identification et la promotion des meilleures pratiques et des outils en cette matière;
 - l'évaluation de l'opportunité d'ouvrir une base de données, à la lumière d'une analyse du risque de réidentification;
 - l'évaluation continue de ce risque, si l'organisme choisit de la diffuser;



- les stratégies d'intervention rapide en cas de réidentification de renseignements ou de diffusion accidentelle de renseignements permettant d'identifier un individu;
- offrir de la formation à ce sujet;
- effectuer une veille sur la diffusion et sur les réutilisations des données ouvertes.

Recommandation 67 : Mettre en place les mesures nécessaires afin que les organismes intègrent ces préoccupations, dès la conception d'une banque de données, le cas échéant, notamment les modalités de son anonymisation éventuelle et de suivi de son utilisation (ex. : marquage des jeux de données).



Annexe 2 – Compilations de données en accès dans sept juridictions

Le tableau suivant appuie la section 1.4.5 du présent rapport.

Dimension	Canada (fédéral)	Ontario	Colombie-Britannique	Écosse	Royaume-Uni	Australie (fédéral)	Australie (État de Victoria)
Type de norme encadrant la production de statistiques	Loi ¹ , directive ²	Lois ³	Pratique administrative ⁴	Loi ⁵ , code de pratique ⁶ , demande du commissaire ⁷	Loi ⁸ , code de pratique ⁹	Lois ¹⁰ , règlement ¹¹ , lignes directrices ¹²	Loi ¹³
Organisme compilateur	Secrétariat du Conseil du Trésor	Commissaire à l'information et à la protection de la vie privée	Ministère des Services aux citoyens	Commissaire à l'information	Ministère du Conseil exécutif	Commissaire à l'information	Commissaire à l'information
Fréquence de soumission ou d'examen des données brutes	Annuelle	Annuelle	S. O. (<i>portail gouvernemental centralisé pour les demandes d'accès</i> ¹⁴)	Trimestrielle	Annuelle	Trimestrielle	Annuelle
Granularité des données brutes	Agrégées (<i>par organisme, par période</i>)	[Information non repérée]	Granulaires (<i>par demande</i>)	Agrégées (<i>par organisme, par période</i>)	Agrégées (<i>par organisme, par période</i>)	[Information non repérée]	[Information non repérée]
Mécanisme de soumission des données brutes	S. O. (<i>portail gouvernemental centralisé pour les demandes d'accès</i> ¹⁵)	Portail Web ¹⁶	S. O. (<i>portail gouvernemental centralisé pour les demandes d'accès</i>)	Portail Web ¹⁷	[Information non repérée]	Portail Web ¹⁸	Portail Web ¹⁹
Validation des données par l'organisme compilateur	[Information non repérée]	[Information non repérée]	[Information non repérée]	Non ²⁰	Oui ²¹	Non ²²	[Information non repérée]



Dimension	Canada (fédéral)	Ontario	Colombie-Britannique	Écosse	Royaume-Uni	Australie (fédéral)	Australie (État de Victoria)
Fréquence de diffusion publique des statistiques	Annuelle	Annuelle	Annuelle	Trimestrielle	Annuelle	Trimestrielle (tableau de bord) Annuelle (brutes)	Annuelle
Format de diffusion publique des statistiques	Rapport ²³ et tableaux ²⁴	Rapport ²⁵ et tableaux ²⁶	Rapport ²⁷ et tableaux ²⁸	Tableau de bord ²⁹ et tableaux ³⁰	Tableaux ³¹	Rapport ³² , tableau de bord ³³ et tableaux ³⁴	Rapport ³⁵
Granularité des données diffusées publiquement	Agrégées (par organisme, par période)	Agrégées (par organisme, par période)	Granulaires (par demande)	Agrégées (par organisme, par période)	Agrégées (par organisme, par période)	Agrégées (par organisme, par période)	S. O. (les données brutes ne sont plus diffusées) ³⁶

Références du tableau

¹ CANADA, *Loi sur l'accès à l'information*, L.R.C (1995), c. A-1, art. 70(1)(d), en ligne : <<https://laws-lois.justice.gc.ca/fra/lois/a-1/>>.

² SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, « Directive sur les demandes d'accès à l'information », *Canada.ca* (2022), par. 4.1.46, en ligne : <<https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=18310>>.

³ *Loi sur l'accès à l'information et la protection de la vie privée [Ontario]*, L.R.O. 1990, c. F-31, art. 34, en ligne : <<https://www.ontario.ca/fr/lois/loi/90f31>>; *Loi sur l'accès à l'information municipale et la protection de la vie privée [Ontario]*, L.R.O 1990, c. M-56, art. 26, en ligne : <<https://www.ontario.ca/lois/loi/90m56>>.

⁴ Plus précisément, la loi prévoit que le ministre responsable de la loi dépose annuellement un rapport sur son administration. Par usage, depuis de nombreuses années, ce rapport intègre des statistiques, mais le cadre légal est muet à ce sujet. Voir *Freedom of Information and Protection of Privacy Act [Colombie-Britannique]*, RSBC 1996, c. 165, art. 68 [ci-après FIPPA de la Colombie-Britannique], en ligne : <https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00_multi>.

⁵ *Freedom of Information Act 2002 [Écosse]*, 2002, asp 13., art. 60(2)f), en ligne : <<https://www.legislation.gov.uk/asp/2002/13/contents>>.

⁶ CONSEIL DES MINISTRES DE L'ÉCOSSE, *Scottish Minister's Code of Practice on the Discharge of Functions by Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004*, 2016, en ligne : <<https://www.gov.scot/binaries/content/documents/govscot/publications/advice-and-guidance/2016/12/foi-eir-section-60-code-of-practice/documents/foi-section-60-code-practice-pdf/foi-section-60-code-practice-pdf/govscot%3Adocument/FOI%2B-%2Bsection%2B60%2Bcode%2Bof%2Bpractice.pdf>>.

⁷ Le commissaire écossais procède par demandes récurrentes aux organismes. Le tableau suivant recense les statistiques qu'il requiert depuis 2022. SCOTTISH INFORMATION COMMISSIONER, *Statistics requested by Commissioner as of January 2022*, 2022, en ligne : <https://www.foi.scot/sites/default/files/2022-03/Statistics_requested_by_Commissioner_as_at_January_2022.xlsx>.



- ⁸ *Freedom of Information Act 2000 [Royaume-Uni]*, 2000, c. 36, art. 45, en ligne : <https://www.legislation.gov.uk/ukpga/2000/36/contents>.
- ⁹ CABINET OFFICE, *Freedom of Information Code of Practice*, 2018, sect. 8.5, en ligne : <https://www.gov.uk/government/publications/freedom-of-information-code-of-practice>.
- ¹⁰ *Australian Information Commissioner Act 2010*, art. 8(j), 30 et 31, en ligne : <https://www.legislation.gov.au/C2010A00052/latest/text>, traduction de l'auteur de la note. *Freedom of Information Act 1982 [Australie]*, art. 93, en ligne : <https://www.legislation.gov.au/C2004A02562/latest/text>.
- ¹¹ *Freedom of Information (Prescribed Authorities, Principal Offices and Annual Report) Regulations 2017 [Australie]*, art. 8, en ligne : <https://www.legislation.gov.au/F2017L01676/asmade>.
- ¹² OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, *FOI Guidelines issued by the Australian Information Commissioner under s 93A of the Freedom of Information Act 1982*, 2025, sect. 15, en ligne : https://www.oaic.gov.au/_data/assets/pdf_file/0020/250391/FOI-Guidelines-Compilation-October-2025.PDF.
- ¹³ *Freedom of Information Act 1982 [Victoria]*, 9859/1982, art. 64, en ligne : <https://www.legislation.vic.gov.au/in-force/acts/freedom-information-act-1982/113>.
- ¹⁴ MINISTÈRE DES SERVICES AUX CITOYENS DE LA COLOMBIE-BRITANNIQUE, « Request records from government », *Gov.bc.ca* (19 septembre 2024), en ligne : <https://www2.gov.bc.ca/gov/content/governments/about-the-bc-government/open-government/open-information/freedom-of-information> (consulté le 4 mars 2025).
- ¹⁵ SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, « Présenter une demande d'accès à l'information ou à vos renseignements personnels », *Canada.ca* (17 octobre 2024), en ligne : <https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/acces-information/presenter-demande.html> (consulté le 3 mars 2025).
- ¹⁶ COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, « Site Web de présentation des statistiques annuelles », en ligne : <https://statistics.ipc.on.ca/fr-CA/> (consulté le 4 mars 2025).
- ¹⁷ SCOTTISH INFORMATION COMMISSIONER, « FOI and EIRs statistics », en ligne : <https://www.foi.scot/statistics> (consulté le 9 avril 2026).
- ¹⁸ OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, préc., note 12, sect. 15.7.
- ¹⁹ « FOI Annual Report Electronic Data Collection », *Office of the Victorian Information Commissioner*, en ligne : <https://foiannualreport.smartmailpro.com/> (consulté le 5 mars 2025).
- ²⁰ « Please be aware that the data is submitted directly by public authorities. It is not checked or verified by the Commissioner and the Commissioner is not responsible for its quality or accuracy. Data is added to this page each quarter by the Commissioner's staff, taken directly from data submitted by authorities ». Voir SCOTTISH INFORMATION COMMISSIONER, préc., note 17.
- ²¹ « These statistics have been independently reviewed by the Office for Statistics Regulation (OSR). They comply with the standards of trustworthiness, quality and value in the Code of Practice for Statistics. » Voir CABINET OFFICE, « Freedom of Information statistics: annual 2023 », *GOV.UK* (avril 2024), en ligne : <https://www.gov.uk/government/statistics/freedom-of-information-statistics-annual-2023> (consulté le 5 mars 2025).
- ²² « Agencies and ministers are responsible for the reliability and quality of their data contained in the dashboard and questions about their data should be directed to them. » Voir OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, « Australian Government freedom of information statistics » (13 janvier 2025), en ligne : <https://www.oaic.gov.au/freedom-of-information/australian-government-freedom-of-information-statistics> (consulté le 14 janvier 2025).
- ²³ SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, « Rapport statistique sur l'accès à l'information et la protection des renseignements personnels pour 2023–2024 », *Canada.ca* (20 décembre 2024), en ligne : <https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/statistiques-airp/rapport-statistique-acces-information-protection-reseignements-personnels-2023-2024.html> (consulté le 3 mars 2025).
- ²⁴ SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, « Statistiques sur l'accès à l'information et la protection des renseignements personnels pour l'année - Portail du gouvernement ouvert », *Canada.ca*, en ligne : <https://ouvert.canada.ca/data/fr/dataset/236294e1-bc74-486f-ab97-42227bc8832> (consulté le 3 mars 2025).



- ²⁵ Voir par exemple COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, *Au-delà de l'imagination: planifier pour un avenir numérique - Rapport statistique 2023*, 2024, en ligne : <https://www.ipc.on.ca/sites/default/files/documents/ra-2023-rapport%20statistique_0.pdf>.
- ²⁶ COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, *IPC 2023 Annual Statistical Report Raw Data*, 2024, en ligne : <https://www.ipc.on.ca/sites/default/files/IPC_AR_2023-raw-data.zip>.
- ²⁷ Voir par exemple MINISTÈRE DES RELATIONS AVEC LES CITOYENS DE LA COLOMBIE-BRITANNIQUE, *Report on the administration of Freedom of Information and Protection of Privacy Act*, Colombie-Britannique, 2024, en ligne : <https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/initiatives-plans-strategies/open-government/open-information/annual_report_on_the_administration_of_foippa_fy_2023-24_002.pdf>.
- ²⁸ OPEN INFORMATION, « Freedom of Information (FOI) Statistics », *British Columbia Data Catalogue*, en ligne : <<https://catalogue.data.gov.bc.ca/dataset/freedom-of-information-foi-statistics>> (consulté le 4 mars 2025).
- ²⁹ SCOTTISH INFORMATION COMMISSIONER, préc., note 17.
- ³⁰ *Id.*
- ³¹ CABINET OFFICE, préc., note 21.
- ³² Voir par exemple OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, *Annual report 2023-24*, 2024, en ligne : <https://www.oaic.gov.au/__data/assets/pdf_file/0025/243592/OAIC_Annual-Report-2023-24_Digital.pdf>.
- ³³ OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, préc., note 22.
- ³⁴ « Freedom of information statistics », *Data.gov.au*, en ligne : <<https://data.gov.au/data/dataset/freedom-of-information-statistics>> (consulté le 28 octobre 2025).
- ³⁵ Voir par exemple OFFICE OF THE VICTORIAN INFORMATION COMMISSIONER, *OVIC 2023-24 Annual Report - Changes*, 2024, p. 105 et suiv., en ligne : <<https://ovic.vic.gov.au/wp-content/uploads/2024/10/OVIC-Annual-Report-2023-24.pdf>>.
- ³⁶ Les données brutes reçues par l'OVIC ne sont plus rendues disponibles, même si elles l'ont déjà été il y a une dizaine d'années. OFFICE OF THE FREEDOM OF INFORMATION COMMISSIONER, « Report on Operation of FOI Act - 2014-15 », *Victorian Government Data Directory* (1 octobre 2015), en ligne : <<https://discover.data.vic.gov.au/dataset/report-on-operation-of-foi-act-2014-15>> (consulté le 5 mars 2025).

Québec

525, boul. René-Lévesque Est
bur. 2.36
Québec (Québec) G1R 5S9

Montréal

2045, rue Stanley, bur. 900
Montréal (Québec) H3A 2V4



Commission d'accès
à l'information
du Québec

cai.gouv.qc.ca