



Commission
d'accès à l'information
du Québec

Version abrégée du rapport

Mieux protéger les renseignements personnels des jeunes à l'ère numérique



Août 2022

Ce document a pour but de donner une vue d'ensemble des principales réflexions et propositions contenues dans la version intégrale de ce rapport disponible sur le site internet de la Commission : <http://www.cai.gouv.qc.ca>

Le genre masculin désigne aussi bien les femmes que les hommes et n'est utilisé que pour alléger le texte.

La reproduction ou la traduction sont autorisées à la condition que la source soit indiquée.

Dépôt légal – 2022
Bibliothèque et Archives nationales du Québec
Bibliothèque et Archives Canada
ISBN : 978-2-550-92755-6 (version imprimée)
ISBN : 978-2-550-92754-9 (version PDF)

1. INTRODUCTION

La récente réforme des lois sur la protection des renseignements personnels¹ (la Loi 25) ajoute à la *Loi sur la protection des renseignements personnels dans le secteur privé*² une mesure de protection visant explicitement les jeunes : en deçà de 14 ans, le parent ou tuteur doit consentir à la collecte de renseignements auprès du mineur ou à leur utilisation ou communication à d'autres fins. De 14 à 17 ans, le mineur peut consentir lui-même, mais son parent ou tuteur peut continuer à le faire.

Dans son rapport *Mieux protéger les renseignements personnels des jeunes à l'ère numérique*, la Commission d'accès à l'information se penche sur la suffisance de cette mesure à la demande du ministre responsable de l'Accès à l'information et de la Protection des renseignements personnels. Comme la loi lui permet désormais de le faire³, le ministre a donné à la Commission le mandat d'examiner si des mesures supplémentaires devraient être envisagées dans la Loi sur le privé afin de protéger davantage les mineurs de moins de 14 ans dans le contexte d'une collecte ou d'une utilisation de leurs renseignements personnels à des fins commerciales ou à des fins de profilage commercial et de lui faire des recommandations à ce sujet.

Les travaux de la Commission ont porté en particulier sur l'environnement numérique, qui offre de nombreuses opportunités, mais aussi des risques importants pour les droits fondamentaux des jeunes, dont celui à la vie privée. À travers le monde, ces risques suscitent d'ailleurs des préoccupations grandissantes. Les initiatives appelant à renforcer la protection accordée aux jeunes dans le monde numérique, notamment en matière de vie privée, se multiplient. De nombreuses juridictions étudient actuellement des textes législatifs ou normatifs comportant des dispositions en ce sens. Dans la préparation de ce rapport, la Commission s'est notamment inspirée de ces travaux, mais aussi d'études menées auprès des jeunes et de leurs parents.

Au terme de sa réflexion, la Commission constate que la vulnérabilité des jeunes et l'asymétrie de pouvoirs très importante entre les entreprises et eux militent pour une protection légale renforcée. Elle estime que des mesures additionnelles sont requises pour protéger les jeunes notamment de l'exploitation commerciale.

Dans le prolongement de la réforme de la Loi sur le privé et dans le respect de l'esprit de la *Loi sur la protection du consommateur*⁴, qui interdit de faire de la publicité commerciale destinée aux enfants, la Commission recommande donc d'interdire la collecte, l'utilisation

¹ *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, L.Q. 2021, c. 25, ci-après la Loi 25.

² *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1, ci-après la Loi sur le privé.

³ *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1, art. 118.

⁴ *Loi sur la protection du consommateur*, RLRQ, c. P-40.1, ci-après la LPC.

et la communication de renseignements personnels concernant des mineurs à des fins de publicité ou de profilage commercial et à toute autre fin dont on sait ou dont il est raisonnable de penser qu'elle nuit aux mineurs. Elle recommande aussi de renforcer la responsabilité des entreprises qui tirent profit des renseignements personnels des mineurs et de clarifier certains aspects de la loi, tant au bénéfice des mineurs qu'à celui des entreprises, vu l'importance des sanctions auxquelles celles-ci pourront s'exposer dès 2023 en cas de manquement à la loi. Enfin, elle suggère d'accroître les efforts en matière d'éducation et de sensibilisation au numérique et au droit à la vie privée. Les recommandations complètes de la Commission sont présentées dans la section 6 à la page 16.

2. PRINCIPES ET CONCEPTS

Dans son rapport, la Commission s'appuie sur certains principes et concepts. Elle donne d'abord quelques précisions au sujet de ceux-ci.

Principes et droits reconnus internationalement

Tout comme beaucoup de documents internationaux et de recherches traitant de la protection des renseignements personnels des mineurs, le rapport de la Commission se fonde sur les principes et les droits énoncés dans la Convention relative aux droits de l'enfant de l'Organisation des Nations unies⁵, laquelle vise tous les moins de 18 ans. La Commission considère également l'Observation générale n° 25 du Comité des droits de l'enfant de l'ONU⁶, qui précise l'application de la Convention dans l'environnement numérique.

La Convention s'articule autour des principes suivants :

- **Non-discrimination** : Les droits de la Convention s'appliquent à tout enfant, sans distinction aucune. Dans l'environnement numérique, la discrimination peut par exemple survenir lors de l'utilisation d'informations obtenues de façon inéquitable dans un processus de décision automatisée visant un enfant;
- **Intérêt supérieur de l'enfant** : Les décisions prises à propos de l'enfant, que ce soit par son entourage ou par des acteurs externes, dont l'État, doivent prioriser le respect de ses droits et la satisfaction de ses besoins particuliers;
- **Droit à la vie, à la survie et au développement** : Tout enfant a le droit de vivre et de se développer pleinement, tant aux plans mental, émotionnel et cognitif que

⁵ 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>>, ci-après la Convention.

⁶ COMITÉ DES DROITS DE L'ENFANT DE L'ORGANISATION DES NATIONS UNIES, *Observation générale n° 25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique*, 2021, en ligne : <<https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsqkirKQZLK2M58RF%2f5F0vEG%2bcAAx34gC78FwvnmZXGFsdFXGQsWU46nx%2b5vAg3QbGXlnOwo3Oquj8nN7ltX6yUYoRpe7N%2b7Q6mEUIz2mfWi>> (consulté le 16 décembre 2021).

- social et culturel. Les États doivent prendre les mesures nécessaires pour réduire les risques auxquels les mineurs sont exposés dans l'environnement numérique;
- > **Participation** : L'opinion de l'enfant doit être prise en compte lorsque des décisions sont prises à son sujet;
 - > **Évolution des capacités** : Le besoin de protection de l'enfant diminue graduellement au fur et à mesure qu'il acquiert des connaissances et des compétences lui conférant une plus grande autonomie par rapport à la réalisation de ses droits. Les États devraient s'assurer que les services numériques respectent le stade de développement de l'enfant, qui fait varier la probabilité et la gravité des risques.

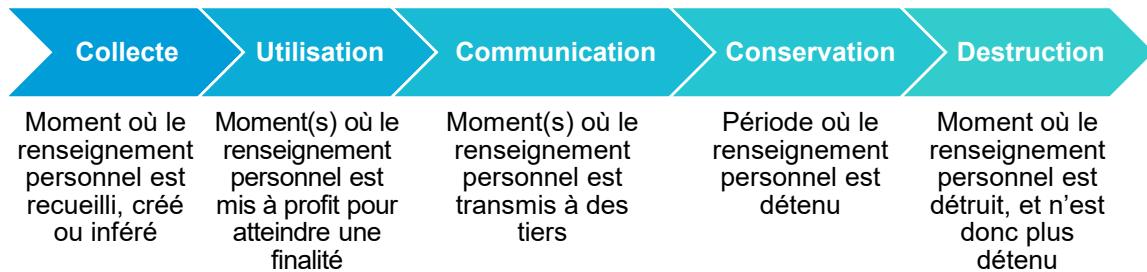
La Convention reconnaît également aux enfants de nombreux droits. Parmi ceux-ci, plusieurs entrent en ligne de compte lorsque les entreprises recueillent, utilisent, communiquent ou conservent des renseignements personnels à leur sujet :

- > Droit de s'exprimer et de penser librement;
- > Droit à la vie privée;
- > Droit à l'information;
- > Droit de jouer, de se relaxer et de participer pleinement à la vie culturelle et artistique;
- > Droit de ne pas être exploités économiquement ou de toute manière qui nuit à leur bien-être.

Plusieurs pratiques numériques actuelles comportent des risques pour ces droits.

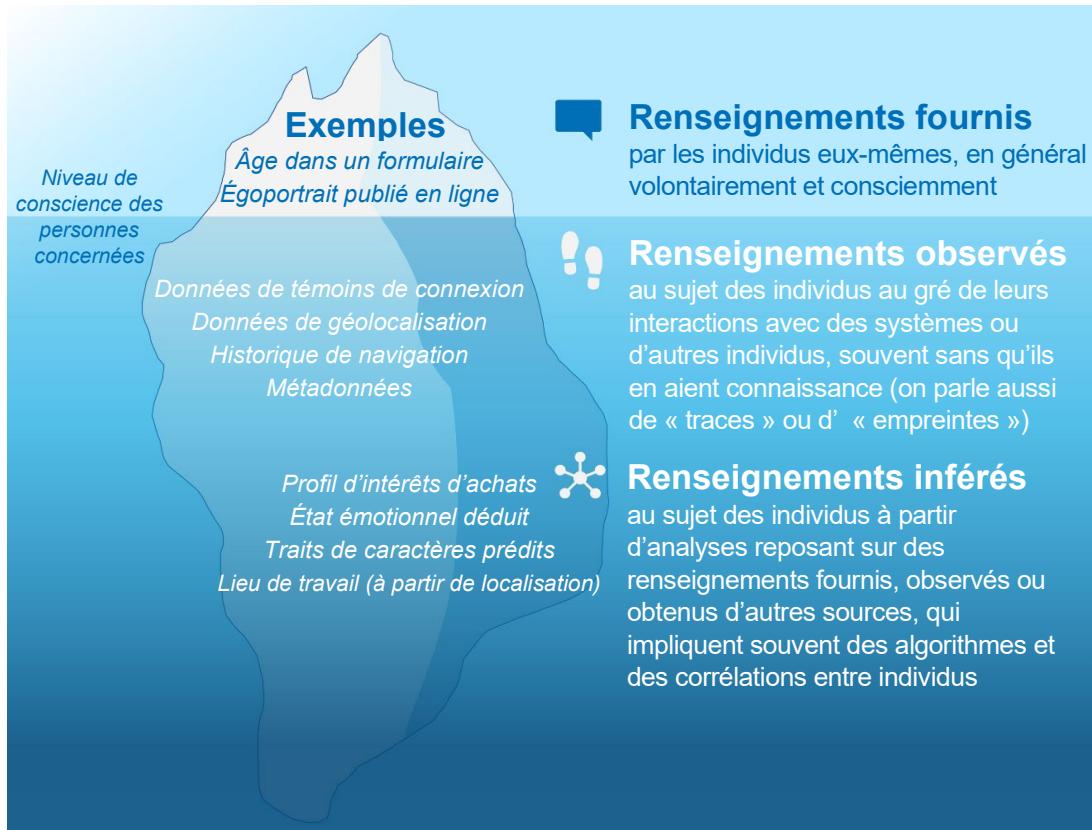
Cycle de vie et typologie des renseignements personnels

La Loi sur le privé prévoit des mesures visant à assurer la protection des renseignements personnels du moment où ils sont recueillis par l'entreprise jusqu'au moment où ils sont détruits. Ce cycle de vie compte cinq étapes :



Par ailleurs, à l'ère numérique, distinguer les renseignements personnels selon le mécanisme par lequel ils sont obtenus permet de raffiner la compréhension des enjeux. Sur la base de travaux de la juriste Simone van der Hof⁷, la Commission distingue trois catégories de renseignements personnels, qui désignent la façon dont ceux-ci sont obtenus par les entreprises. La métaphore de l'iceberg permet de représenter le tout :

⁷ Simone VAN DER HOF, « I Agree... or Do I? – A Rights-Based Analysis of the Law on Children's Consent in the Digital World », (2016) 34-2 *Wisconsin International Law Journal* 409-445.



Dimensions de la vie privée numérique

Le rapport de la Commission fait référence à trois « dimensions de la vie privée numérique » (interpersonnelle, institutionnelle et commerciale), tirées de recherches sur la protection des mineurs dans l'environnement numérique⁸. Celles-ci permettent d'éclairer différents enjeux vécus par les mineurs en matière de protection des renseignements personnels.

- > **La dimension interpersonnelle** concerne la gestion des renseignements personnels dans les relations du mineur avec d'autres **personnes**. Elle implique surtout des renseignements fournis par le mineur lui-même.
- > **La dimension institutionnelle** concerne la collecte et la gestion des renseignements personnels du mineur par les **organismes publics**. Les renseignements personnels qu'elle implique sont soit fournis par le mineur, soit observés – ses dossiers (scolaire, médical, etc.) en sont un exemple.
- > **La dimension commerciale** concerne la collecte, l'utilisation, la communication ou la conservation des renseignements personnels du mineur par des **entreprises**. L'essentiel des activités commerciales repose sur des

⁸ Mariya STOLOVA, Sonia LIVINGSTONE et Rishita NANDAGIRI, *Children's data and privacy online*, The London School of Economics and Political Science, 2021, en ligne : <<https://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf>>, notre traduction.

renseignements observés (par exemple, grâce à des métadonnées ou à des témoins de connexion) ou inférés (par exemple, par profilage).

Portée de l'analyse de la Commission

À partir des éléments présentés dans cette première partie, la Commission apporte enfin quelques précisions quant à la portée du mandat qui l'a guidée dans la rédaction du rapport :

- > L'analyse de la Commission considère **tous les jeunes de moins de 18 ans, incluant les 14 à 17 ans**. Sauf mention contraire, l'utilisation du terme « mineur » renvoie donc aux moins de 18 ans.
- > Puisque le numérique joue désormais un rôle prépondérant dans la vie des mineurs, la Commission se concentre sur la protection des renseignements personnels **dans cet environnement**.
- > Étant donné la demande du ministre, la dimension commerciale de la vie privée est au cœur du rapport. À diverses occasions, la Commission fait toutefois des liens avec sa **dimension interpersonnelle**.
- > Puisque toutes les étapes du cycle de vie des renseignements personnels comportent des risques particuliers, l'analyse de la Commission considère également **la communication et la conservation de renseignements**, en plus de la collecte et de l'utilisation.

3. CONTEXTE

En vue d'éclairer ses recommandations sur les mesures de protection des renseignements personnels des mineurs, la Commission explore les caractéristiques de l'environnement numérique dans lequel ils évoluent, les pratiques des entreprises, les attitudes et connaissances des mineurs et de leurs parents de même que les risques auxquels les mineurs sont exposés dans l'environnement numérique. Elle conclut que leur vulnérabilité particulière justifie une protection légale renforcée, à l'instar de celle que prévoit la LPC en matière de publicité commerciale visant les moins de 13 ans.

Environnement numérique et activités des entreprises

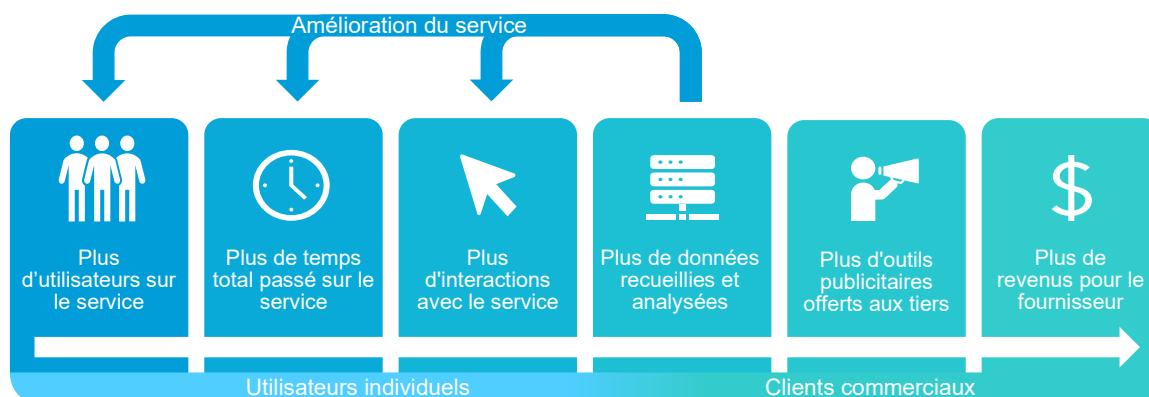
La Commission caractérise d'abord l'environnement numérique, incontournable dans la vie des jeunes. Elle constate que celui-ci génère des risques importants pour les mineurs. En effet, trois grandes tendances le traversent et cadrent les interactions dont il est le théâtre :

- > **La mise en données** (*datafication* en anglais) : le numérique permet la collecte de grandes quantités données au sujet des individus en vue de leur exploitation, dans de plus en plus de contextes et de plus en plus rapidement;

- > **L'hyperconnectivité** : les objets et les lieux s'intègrent désormais aux réseaux où interagissent les personnes et les organisations, ce qui accentue la mise en données et brouille les frontières entre les univers physique et numérique;
- > **La commercialisation** : l'environnement numérique est conçu et exploité surtout par des entreprises, lesquelles en dictent la conception et en établissent les fonctionnalités, généralement en suivant des impératifs commerciaux.

L'évolution rapide de cet environnement en constitue également une propriété transversale. L'effet combiné de ces forces sur la vie privée des mineurs et la réalisation de leurs droits est particulièrement important.

La Commission se penche ensuite sur les pratiques actuelles des entreprises qui fournissent des produits et des services numériques. Elle constate que le contexte économique dans lequel opèrent aujourd'hui les entreprises les pousse à recueillir sans cesse plus de renseignements personnels. Il est aussi à l'origine de modèles d'affaires problématiques pour la protection des renseignements personnels, notamment celui de la publicité comportementale, élément fondamental de l'économie dite « de l'attention », illustrée dans le schéma suivant :



Suivant ce schéma, les individus sont vus à la fois comme des consommateurs et comme des ressources qui produisent des données. Celles-ci peuvent être revalorisées pour attirer davantage d'utilisateurs sur les services et maximiser le temps qu'ils y passent, mais également exploitées à des fins publicitaires par des clients commerciaux. Cette chaîne de valeur encourage le recours à des stratégies toujours plus persuasives reposant entre autres sur des éléments de design et des algorithmes qui peuvent être raffinés et rendus plus puissants grâce aux renseignements personnels recueillis.

Par ailleurs, les modèles reposant sur la vente de renseignements personnels sont également source de préoccupations importantes.

Puisque les jeunes, qui constituent le tiers des utilisateurs d'Internet, représentent une clientèle particulièrement intéressante que l'on peut notamment fidéliser à long terme, ils n'échappent pas à ces pratiques et sont parfois spécifiquement visés. Pensons notamment aux jouets connectés et aux applications mobiles destinées aux jeunes ou populaires auprès d'eux qui recueillent, souvent à leur insu, une multitude de renseignements personnels, comme le démontrent certaines études.

Caractéristiques des mineurs et de leurs parents

Les comportements, les attitudes et les connaissances des mineurs et de leurs parents permettent de mieux comprendre de quelle façon les mineurs sont confrontés aux risques numériques et y réagissent. En particulier, les recherches indiquent que tous deux ont une littératie numérique limitée, exacerbée par le manque de transparence des pratiques des entreprises, qui les défavorise.

Les jeunes évaluent généralement les enjeux de vie privée par rapport à la dimension interpersonnelle (qui peut voir ce qu'ils publient en ligne) et non en fonction de ce que les entreprises recueillent à leur sujet et de la façon dont elles utilisent ces informations (dimension commerciale). Lorsqu'on leur présente plus en détail l'écosystème numérique dans lequel ils naviguent, ils expriment un inconfort et qualifient de troublantes et dérangeantes certaines pratiques en lien avec les algorithmes, le profilage, la géolocalisation ou la publicité ciblée. Enfin, leur perception du risque est aussi teintée par leur vision interpersonnelle de cet environnement, qui correspond au discours public limité à la dimension de la sécurité en ligne : cyberintimidation, prédatation sexuelle, cyberharcèlement ou piratage sont ainsi au cœur des préoccupations, puisqu'ils ont des conséquences plus claires sur leur sécurité, leur réputation ou leur dignité. Les mineurs se soucient aussi de ne pas être suivis par leurs parents.

Des constats similaires s'appliquent aux parents. Même s'ils comprennent les bases, en l'occurrence le compromis souvent demandé entre divulgation de renseignements personnels et fourniture d'un service numérique, les parents démontrent eux aussi une compréhension essentiellement interpersonnelle de la vie privée. Par exemple, ils s'en remettent à des stratégies de restriction de l'auditoire lorsqu'ils veulent protéger les renseignements personnels de leurs enfants qu'ils publient sur les réseaux sociaux. De même, ils ont peu conscience des renseignements observés et inférés. Leur perception du risque est aussi essentiellement liée à la sécurité en ligne.

Risques numériques pour les mineurs

La Commission retient pour les fins de son rapport la typologie CO:RE dite des « 4 C ». Celle-ci distingue des risques de contenu, de contact, de conduite et de contrat, lesquels s'articulent dans trois dimensions : agression, sexualité et valeurs. De plus, la typologie définit trois risques transversaux, soit les risques d'atteintes à la vie privée, d'inégalités et de discrimination et les risques pour la santé.

Tous ces éléments sont synthétisés dans le tableau ci-après, traduit et adapté de celui proposé par les chercheuses Sonia Livingstone et Mariya Stoilova⁹, qui recense également des exemples de risques pouvant être classés dans chaque cellule :

⁹ Sonia LIVINGSTONE et Mariya STOLOVA, « The 4Cs: Classifying Online Risk to Children », CO:RE Short Report Series on Key Topics 2021, p. 12, doi : 10.21241/SSOAR.71817. Tableau reproduit et traduit selon les termes de la licence CC BY 4.0 FR.

	Contenu	Contact	Conduite	Contrat
Agression	Information ou communication violente, « sanglante » (<i>gore</i>), explicite, raciste, haineuse ou extrémiste	Harcèlement, persécution, comportements haineux, surveillance excessive ou non désirée	Intimidation, communication ou activité de pairs haineuse ou hostile (ex. <i>trolling</i> , exclusion, humiliation)	Vol d'identité, fraude, hameçonnage, arnaques, piratage, chantage, risques de sécurité
Sexualité	Pornographie (préjudiciable ou illégale), sexualisation de la culture, normes oppressives liées à l'image corporelle	Harcèlement sexuel, leurre sexuel, sextorsion, pornographie juvénile	Harcèlement sexuel, messagerie de nature sexuelle non consensuelle, pressions sexuelles néfastes	Trafic à des fins d'exploitation sexuelle, diffusion payante de pornographie juvénile
Valeurs	Désinformation, marketing ou contenu généré par les utilisateurs inapproprié à l'âge	Manipulation ou persuasion idéologique, radicalisation, recrutement dans des mouvements extrémistes	Communautés d'utilisateurs potentiellement nuisibles (ex. automutilation, anti-vaccination, pression par les pairs négative)	Jeux d'argent, bulles de filtres, microciblage, interfaces truquées influant sur les croyances ou les achats
Risques transversaux	<ul style="list-style-type: none"> • Violations de la vie privée (interpersonnelle, institutionnelle, commerciale; normalisation de la surveillance) • Risques pour la santé mentale et physique (ex. mode de vie sédentaire, utilisation excessive de l'écran, isolement, anxiété) • Inégalités et discrimination (inclusion et exclusion, exploitation des vulnérabilités, biais algorithmiques/analyse prédictive) 			

La typologie CO:RE ne suppose pas que chaque risque ne se situe que dans une cellule du tableau; en effet, les risques sont de plus en plus liés. À ce sujet, il faut souligner le rôle important des fournisseurs de services numériques dans l'émergence des différentes catégories de risques, en raison de leur position dominante dans tous les aspects de la vie numérique. En plus de pouvoir être directement à l'origine de risques de contrat, ils gèrent par exemple les plateformes où les individus interagissent, ce qui peut générer des risques de contact et de conduite; ils hébergent aussi du contenu numérique en grande quantité, qu'il soit créé par des utilisateurs ou des organisations.

Dès lors, les choix opérés par les entreprises sur la base de leurs intérêts commerciaux ne sont pas neutres. Ils peuvent influencer de manière importante la

probabilité et la nature des risques de toutes sortes auxquels les mineurs sont exposés dans l'environnement numérique¹⁰.

La Commission observe que les renseignements personnels (fournis, observés et inférés) sont au cœur des modèles d'affaires des fournisseurs de services en ligne. Sans qu'elles soient des causes universelles, leur collecte, leur utilisation et leur communication peuvent néanmoins ouvrir la porte aux risques figurant dans le tableau présenté ci-dessus. Pour illustrer cette situation, la section 3.3.2 du rapport présente cinq scénarios fictifs dans lesquels des outils techniques ou des éléments de design utilisés par des entreprises génèrent des risques pour les mineurs.

Aussi, l'incertitude qui existe concernant les utilisations futures possibles des renseignements est également un facteur à considérer, tout comme la dimension sociale des préjudices potentiels. Ceux-ci peuvent ainsi concerter *un mineur* en particulier, mais aussi *les mineurs* comme groupe.

Raisons d'agir

Au terme de cette exploration des éléments de contexte, la Commission retient qu'il est impératif que les lois sur la protection des renseignements personnels prévoient des mesures particulières pour les mineurs. **Celles-ci doivent permettre de maximiser les opportunités qui s'offrent à eux dans l'environnement numérique tout en minimisant les risques auxquels ils sont exposés.**

Cette position s'explique principalement par la vulnérabilité des mineurs, qui, entre autres, naviguent dans un environnement numérique conçu avant tout pour des adultes, se concentrent sur la gestion interpersonnelle de la circulation de leurs renseignements personnels et ne peuvent exercer toute la vigilance souhaitée en raison de la complexité et de l'opacité des pratiques commerciales impliquant des renseignements personnels. D'autres facteurs de vulnérabilité souvent examinés en matière de protection du consommateur s'ajoutent : capacités de raisonnement différentes des adultes, sensibilité à la pression et à l'influence des pairs et difficulté à interpréter les intentions. En somme, les mineurs sont exposés à plus de situations potentiellement préjudiciables et sont également moins outillés que les adultes pour y faire face.

Dans la mesure où plusieurs pratiques commerciales exploitent ces facteurs de vulnérabilité, il existe une forte asymétrie de pouvoirs entre les entreprises et les mineurs. Ainsi, les entreprises, entre autres, contrôlent en bonne partie la conception de l'espace numérique et peuvent mobiliser des méthodes novatrices pour influencer les comportements ou les intentions des mineurs, celles-ci étant souvent propulsées par le grand volume de données auxquelles elles ont accès.

La Commission remarque qu'en d'autres matières, la société québécoise a mis en place des protections particulières (par ex. vente d'alcool et de tabac, accès aux films dont le

¹⁰ 5RIGHTS FOUNDATION, « Risky by design - Introduction », *Risky-By-Design* (2022), en ligne : <<https://www.riskyby.design/introduction>> (consulté le 28 février 2022).

contenu est restreint, etc.). Notamment, le Québec a fait le choix d'interdire la publicité commerciale s'adressant aux enfants de moins de 13 ans. Cette dernière mesure, inscrite dans la LPC, témoigne d'un véritable choix de société plaçant l'intérêt supérieur de l'enfant au-dessus des intérêts commerciaux. Dans la section 3.4.2, la Commission dresse plusieurs parallèles entre cette interdiction et la question examinée dans son rapport, rappelant que la protection des mineurs contre l'exploitation économique dans une économie numérique où leurs données sont utilisées à des fins commerciales reste plus que jamais importante.

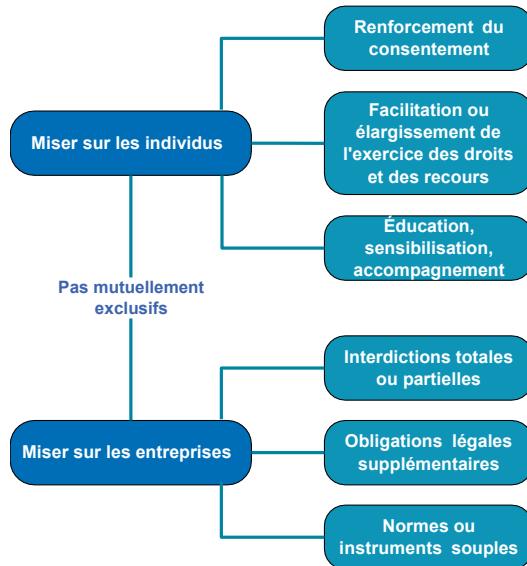
4. MOYENS POUR PROTÉGER LES MINEURS

Étant établi qu'il est nécessaire d'accorder une protection particulière aux mineurs par rapport à leurs renseignements personnels, la Commission évalue dans cette section les moyens d'y parvenir à partir de ses recommandations passées et de la documentation préparée par plusieurs organisations internationales ou nationales. En effet, depuis un peu plus d'une dizaine d'années, de plus en plus de travaux supra-gouvernementaux, gouvernementaux et non gouvernementaux dans différentes juridictions présentent des pistes d'action sur ce thème pour les décideurs.

Beaucoup de points de convergence se dégagent. La Commission constate que pour atteindre l'objectif de maximiser les opportunités offertes par l'environnement numérique tout en minimisant les risques qui s'y posent, il est possible d'agir essentiellement de deux façons – sans qu'elles soient mutuellement exclusives :

- > En misant sur les **individus** pour améliorer leur capacité d'agir et leurs connaissances (prévention) ou encore pour qu'ils puissent agir *a posteriori* (recours et droits). Précisons que ces mesures peuvent être matérialisées par des obligations incombant aux entreprises; elles confient néanmoins l'essentiel du fardeau de la protection aux individus;
- > En misant sur les **entreprises** pour renforcer leurs obligations de protection (prévention) afin de prévenir les préjudices pouvant affecter les mineurs.

La figure suivante résume les grandes catégories de mesures présentées dans la section 4 du rapport, qui constitue un étalonnage préalable aux recommandations de la Commission. Ces catégories sont dégagées des analyses de diverses organisations, des lois, des réglementations et des normes québécoises et internationales.



Outre ces mesures visant les individus et les entreprises, les travaux consultés proposent parfois aussi de mieux asseoir les lois sur la protection des renseignements personnels sur les principes de la Convention. Par exemple, l'intégration du principe d'intérêt supérieur de l'enfant à même ces lois permettrait non seulement de clarifier la pondération des intérêts dans certaines situations conflictuelles entre individus, mais donnerait également le ton aux organisations en ce qui concerne les décisions ayant un impact sur la protection des renseignements personnels des mineurs. Dans les sections 4.1.1 à 4.1.3 de son rapport, la Commission donne davantage de détails à propos de chaque mesure repérée dans la documentation consultée.

Dans la section 4.2, elle analyse la façon dont les 13 cadres législatifs suivants¹¹ concrétisent ces mesures :

#	Juridiction	Législation	Abréviation
1	Union européenne	Règlement général sur la protection des données	RGPD
2	Union européenne	Législation sur les services numériques	LSN
3	Union européenne	Législation sur l'intelligence artificielle	LIA
4	Royaume-Uni	Data Protection Act 2018	DPA18
5	États-Unis (fédéral)	Children's Online Privacy Protection Act	COPPA
6	États-Unis (fédéral)	Kids' Online Safety Act	KOSA
7	Californie	California Age-Appropriate Design Code Act	CAADCA
8	Colorado	Colorado Privacy Act	CPA
9	Washington (État)	Washington Privacy Act	WPA

¹¹ Les références complètes de ceux-ci se retrouvent au début de la section 4.2 du rapport complet.

#	Juridiction	Législation	Abréviation
10	Canada (fédéral)	<i>Loi de 2022 sur la mise en œuvre de la Charte du numérique</i> (projet de loi C-27)	C-27
11	Ontario	Livre blanc sur une éventuelle loi provinciale sur la protection des renseignements personnels dans le secteur privé	LBO
12	Inde	<i>Personal Data Protection Bill 2019</i>	PDPB
13	Brésil	<i>Lei Geral de Proteção de Dados Pessoais</i>	LGPD

Le tableau en page 13 constitue une synthèse de la section 4.2. Il vise à faciliter la comparaison des encadrements juridiques, mais n'est pas exhaustif. Le portrait brossé, issu d'une recherche approfondie, mais non d'une analyse juridique, est forcément réducteur des nuances applicables dans chaque juridiction, mais donne une indication sur l'étendue des mesures implantées ou envisagées dans chaque régime et l'interaction entre elles.

	Loi ou projet de loi												
Mesures	1	2	3	4	5	6	7	8	9	10	11	12	13
Consentement parental jusqu'à un âge X	13-16	RGPD	RGPD	13	13	COPPA	CERT CCPA	13	13	PART	13-16	18	18
Adaptation des informations données à l'âge de l'enfant													
Droit au déréférencement													
Droit à la suppression							CCPA						CERT
Interdiction (totale ou partielle) du profilage/des décisions automatisées	POT			CC			PART						
Interdiction (totale ou partielle) de la publicité ciblée			POT				POT		SENS				
Interdiction (totale ou partielle) d'utiliser les RP d'enfants à des fins nuisibles				CC		IND							
Interdiction (totale ou partielle) d'utiliser des interfaces truquées		POT			CC				CERT				
Interdiction (totale ou partielle) de communiquer les RP d'enfants					CC					IND			
Désignation explicite des RP d'enfants comme sensibles													
Réalisation d'une analyse d'impact si des RP d'enfants sont impliqués	LAPD			CC		IND							
Vérification d'âge par les fournisseurs de services	POT				CC								
Paramètres les plus protecteurs des RP par défaut													
Mise en place d'un code de pratiques			PART										
Mention de l'intérêt supérieur de l'enfant	IND				CC								

Légende

Prévu dans la loi	
Potentiellement/partiellement	
Prévu ailleurs	
CC	<i>Children's Code (Royaume-Uni)</i>
CCPA	<i>California Consumer Privacy Act</i>
LAPD	Listes nationales de cas visés par des analyses d'impact
POT	Potentiellement
CERT	Seulement dans certains cas
SENS	Seulement à partir de renseignements sensibles
RP	Renseignements personnels
IND	Indirectement
PART	Partiellement

Au-delà de ces mécanismes législatifs, certaines juridictions européennes se sont dotées de normes s'adressant aux entreprises et visant à mieux protéger les renseignements personnels des mineurs. Dans la section 4.3 du rapport, la Commission présente les initiatives de l'Irlande, des Pays-Bas et de la France, qui pour l'essentiel ressemblent au *Children's Code* élaboré par l'Information Commissioner's Office du Royaume-Uni¹², considéré comme le premier exemple d'une telle norme. Ces documents rassemblent des principes de collecte, d'utilisation et de communication de renseignements personnels et des principes de conception qui s'adressent aux entreprises concevant des produits et services auxquels les mineurs sont susceptibles d'avoir accès.

5. ANALYSE DE LA LOI 25

Dans cette section de son rapport, la Commission analyse des dispositions pertinentes de la Loi 25 à la lumière des éléments de contexte présentés préalablement et des législations, normes et documents internationaux consultés afin d'évaluer si les nouvelles obligations permettent d'atténuer certains des risques identifiés. Du point de vue de la Commission, le mécanisme du consentement parental, principal élément de protection particulière pour les mineurs, ne suffit pas.

Parmi les modifications substantielles que la Loi 25 apporte à la Loi sur le privé, plusieurs peuvent avoir un impact positif sur la protection des mineurs. La Commission salue les avancées en cette matière. Le tableau suivant, qui se base sur celui en page 13, présente certaines des mesures qui touchent les mineurs dans le cadre juridique québécois tel que modifié par la Loi 25.

Mesures	LP	Légende
Consentement parental jusqu'à un âge X	14	Prévu dans la loi
Exigence explicite d'adaptation des informations données à l'âge de l'enfant		Partiellement
Droit au déréférencement		CERT
Droit à la suppression	CERT	Seulement dans certains cas
Interdiction explicite (totale ou partielle) du profilage/des décisions automatisées	PART	Partiellement
Interdiction explicite (totale ou partielle) de la publicité ciblée		RP
Interdiction explicite (totale ou partielle) d'utiliser les RP d'enfants à des fins nuisibles		Renseignements personnels
Interdiction explicite (totale ou partielle) d'utiliser des interfaces truquées		

¹² INFORMATION COMMISSIONER'S OFFICE, *Age appropriate design: A code of practice for online services*, 2020, en ligne : <<https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf>>.

Mesures	LP
Interdiction explicite (totale ou partielle) de communiquer les RP d'enfants	
Désignation explicite des RP d'enfants comme sensibles	
Réalisation d'une analyse d'impact si des RP d'enfants sont impliqués	
Vérification d'âge par les fournisseurs de services	
Paramètres les plus protecteurs des RP par défaut	PART
Mise en place d'un code de pratiques	
Mention de l'intérêt supérieur de l'enfant	

Jusqu'à l'âge de 14 ans, c'est le titulaire de l'autorité parentale ou le tuteur du mineur qui pourra consentir à la collecte de renseignements personnels auprès de ce dernier ou à leur utilisation ou communication à d'autres fins que celles prévues lors de la collecte¹³. De 14 à 17 ans, tant le parent que le mineur pourront consentir. Le consentement ne sera pas requis dans les cas où la collecte ou l'utilisation sont manifestement au bénéfice du mineur. Cette mesure s'applique tant dans le monde physique que numérique.

La législation québécoise telle que modifiée prévoit aussi un droit au déréférencement tenant compte du fait que les renseignements personnels concernent un mineur, un droit à la suppression dans certains cas, la désactivation par défaut du profilage et l'obligation de régler les paramètres des produits et services technologiques au plus haut niveau de confidentialité par défaut. En outre, d'autres dispositions liées à la transparence, à la sensibilité des renseignements ou à l'évaluation des facteurs relatifs à la vie privée renforcent la responsabilité des entreprises et sont susceptibles d'avoir un effet protecteur pour les mineurs.

Bien que variées, ces mesures n'ont peut-être pas toute l'efficacité voulue pour prévenir les risques pour les droits des mineurs. Au premier chef, la disposition principale qui vise spécifiquement les mineurs – le mécanisme de consentement parental – souffre d'importantes limites. Entre autres :

- Le caractère libre et éclairé du consentement peut être remis en question en raison de certains paramètres de l'environnement numérique; par exemple :
 - Les interfaces ne sont pas toujours neutres et peuvent orienter les choix;
 - Refuser la collecte, l'utilisation ou la communication de renseignements personnels implique souvent de renoncer à un produit ou un service numérique, ce qui peut avoir d'importantes conséquences sur la socialisation des mineurs;
 - Les pratiques des entreprises sont opaques et complexes;

¹³ Loi sur le privé, art. 4.1 et 14.

- Les choix doivent être faits dans l'instantanéité;
- > Le consentement parental implique de fixer un âge seuil au-delà duquel il n'est plus requis et, potentiellement, de mener des vérifications de l'âge du mineur et de sa relation avec l'adulte qui consent en son nom, ces dernières présentant des difficultés techniques réelles;
- > Les intérêts du parent et du mineur ne sont pas toujours alignés et ce mécanisme peut nuire, dans certains cas, à l'autonomie du mineur;
- > Le consentement est un acte de contrôle individuel, alors que plusieurs des risques auxquels sont confrontés les mineurs dans le monde numérique sont de nature systémique et sont générés par les entreprises : confier le fardeau de la protection aux parents ou aux adolescents représente une forme de déséquilibre.

Ainsi, en cohérence avec les objectifs de la réforme que constitue la Loi 25 et en considérant les limites du consentement, d'ailleurs reconnues par les entreprises elles-mêmes, la Commission estime qu'il faut envisager des mesures supplémentaires visant à limiter certaines finalités et à responsabiliser davantage les entreprises afin de protéger les mineurs.

6. RECOMMANDATIONS ET PERSPECTIVES

Au terme de l'analyse présentée dans le rapport, la Commission conclut que **la Loi sur le privé devrait être bonifiée afin de protéger davantage les mineurs dans le contexte d'une collecte, d'une utilisation ou d'une communication de leurs renseignements personnels à des fins commerciales ou à des fins de profilage commercial**. Elle formule 12 recommandations quant aux mesures qui devraient être mises en place, revient sur les critères permettant d'en circonscrire l'application et offre quelques perspectives conclusives.

Recommendations

Recommandation 1 : La Commission recommande d'inclure dans la Loi sur le privé une interdiction explicite de recueillir, d'utiliser ou de communiquer les renseignements personnels d'un mineur (de moins de 18 ans) :

- a) dans le but de faire de la publicité commerciale ou de la prospection commerciale, qu'elles visent le mineur lui-même, une autre personne ou un groupe partageant certaines caractéristiques avec le mineur;
- b) dans le but d'influencer son comportement ou ses décisions, ou ceux d'une autre personne ou d'un groupe partageant certaines caractéristiques du mineur, dans un contexte commercial;
- c) à toute autre fin dont on sait ou dont il est raisonnable de penser qu'elle est susceptible de causer un préjudice important à ce mineur ou aux mineurs en général (par ex. discrimination, nuisance au bien-être physique ou mental, distorsion de l'image corporelle, etc.).

Recommandation 2 : La Commission recommande d'interdire explicitement, dans la Loi sur le privé, la vente de renseignements personnels concernant un mineur (de moins de 18 ans) en toutes circonstances, même avec l'obtention d'un consentement.

Recommandation 3 : La Commission recommande de modifier la Loi sur le privé afin qu'il soit explicite que les renseignements personnels inférés ou créés sont inclus dans sa portée et sont visés par les mêmes obligations, droits et recours que les autres renseignements personnels.

Recommandation 4 : La Commission recommande d'enchâsser, dans la Loi sur le privé :

- a) l'intérêt supérieur de l'enfant (en mentionnant que ce principe doit guider l'interprétation de la loi);
- b) son droit d'exprimer son opinion sur les questions l'intéressant;
- c) son droit d'être entendu dans toutes les procédures qui le concernent.

Recommandation 5 : La Commission recommande de modifier la Loi sur le privé afin que les entreprises aient un devoir particulier de protection envers tous les mineurs, avec égard pour leur catégorie d'âge; en particulier, en matière de transparence, la loi devrait obliger les entreprises à adapter les informations qu'elles fournissent à l'âge et aux capacités des mineurs visés et à les leur fournir au moment opportun, en ayant recours au besoin à des formats non textuels (ex. images, vidéos, etc.).

Recommandation 6 : La Commission recommande de modifier la Loi sur le privé afin d'accorder une préséance à l'opinion du mineur de 14 ans et plus, par rapport à celle du titulaire de l'autorité parentale ou du tuteur, pour le consentement, le refus de consentir ou le retrait de consentement.

Recommandation 7 : La Commission recommande de modifier la Loi sur le privé afin qu'il soit énoncé clairement que les fonctions permettant l'identification, la localisation ou le profilage doivent être désactivées par défaut.

Recommandation 8 : La Commission recommande que les paramètres de confidentialité des témoins de connexion tiers soient visés par le premier alinéa de l'article 9.1 de la Loi sur le privé, au moins dans les cas où ces témoins sont susceptibles de concerner un mineur.

Recommandation 9 : La Commission recommande d'exiger que l'évaluation de projets impliquant des renseignements personnels concernant des mineurs tienne également compte des impacts potentiels sur les autres droits fondamentaux des mineurs.

Recommandation 10 : La Commission recommande d'interdire explicitement, dans la Loi sur le privé, tout recours aux interfaces truquées ayant un effet sur la protection des renseignements personnels des mineurs.

Recommandation 11 : La Commission recommande d'encadrer la conception des produits et services numériques, par exemple en exigeant la mise en place de mécanismes simples pour que les mineurs ou leurs parents puissent exercer les droits d'accès, de rectification, de déréférencement et de portabilité ou en précisant que les fabricants d'objets connectés doivent fournir de l'information complète sur l'emballage.

Recommandation 12 : La Commission recommande d'accroître les ressources allouées à l'éducation et à la sensibilisation au fonctionnement, aux avantages et aux risques du numérique et aux droits liés à la protection des renseignements personnels, notamment :

- a) en intégrant ces notions à même les programmes d'enseignement général et en leur y accordant suffisamment de place;
- b) en augmentant le budget de la Commission de manière à lui permettre de remplir pleinement sa fonction de promotion et de sensibilisation auprès des jeunes.

Critères d'application

La Commission a évalué les critères qui pourraient être utilisés pour circonscrire l'application de certaines mesures de protection supplémentaires. Bien qu'elle juge que plusieurs de ses recommandations doivent s'appliquer de façon large, elle reconnaît qu'il ne serait pas proportionnel de demander à toutes les entreprises, quel que soit leur secteur d'activités, d'adapter les informations aux enfants ou de changer la conception de leurs services, par exemple.

Se fondant sur des modèles existants à l'international, la Commission estime que les entreprises offrant des produits et services « auxquels les mineurs sont susceptibles d'accéder » (« susceptibles » s'entendant d'une probabilité de plus de 50 %) devraient être soumises à des obligations supplémentaires.

Perspectives

La Commission conclut son rapport par les perspectives suivantes :

1. Si les recommandations de la Commission sont mises en place, il sera important d'organiser des discussions avec des groupes d'enfants et d'adolescents, dans le respect du droit des mineurs d'exprimer leur opinion sur les sujets qui les concernent.
2. La Commission des droits de la personne et des droits de la jeunesse, experte en droits fondamentaux, devrait être consultée au moment de considérer la façon d'appliquer les recommandations formulées dans le rapport. De même, l'apport d'autres organismes, comme l'Office de la protection du consommateur, pourrait être utile.
3. L'interaction entre l'exercice des droits liés aux renseignements personnels, comme le consentement, et le droit contractuel devrait être explorée plus avant.

4. Si le rapport se penche sur l'impact des activités du secteur privé sur les jeunes, il n'aborde pas les enjeux liés au secteur public. La collecte, l'utilisation et la communication de renseignements personnels par les organismes publics mériteraient un examen plus approfondi, notamment dans le contexte où l'intelligence artificielle est de plus en plus mise de l'avant dans le domaine de l'éducation et où les partenariats public-privé se font plus nombreux dans les écoles (ex. technologies éducatives, systèmes de surveillance, etc.).
5. Le rapport de la Commission ne traite pas en détail la question de la vérification de l'âge des mineurs en ligne et du consentement parental. Or, celle-ci retient énormément l'attention à l'international, en raison des défis techniques et juridiques qu'elle implique et des enjeux de minimisation des données et de préservation de l'anonymat auxquels elle est associée. De plus, l'ajout du consentement parental dans la Loi sur le privé soulève implicitement la possibilité que soient déployés des mécanismes de vérification. La Commission continuera par conséquent à suivre ce thème de près.



Commission
d'accès à l'information
du Québec

Québec

525, boul. René-Lévesque Est, bureau 2.36
Québec (Québec) G1R 5S9
Téléphone : 418 528-7741

Montréal

2045, rue Stanley, bureau 900
Montréal (Québec) H3A 2V4
Téléphone : 514 873-4196

www.cai.gouv.qc.ca