Commission
d'accès à l'information
du Québec

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

Rapport de la Commission d'accès à l'information présenté au ministre responsable de l'Accès à l'information et de la Protection des renseignements personnels

Août 2022

Pour préparer ce rapport, la Commission a consulté de la documentation publiée avant le 17 juin 2022, date de fin du travail de recherche.

Ce rapport est disponible sur le site Web de la Commission d'accès à l'information à l'adresse suivante : 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 : 978-2-550-92753-2 (version imprimée)
ISBN : 978-2-550-92752-5 (version PDF)

© Gouvernement du Québec 2022

MANDAT

Le présent rapport fait suite à une demande du ministre responsable de l'Accès à l'information et de la Protection des renseignements personnels, M. Éric Caire, transmise le 21 octobre 2021 en vertu de l'article 118 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[1] :

« Lors de l'étude détaillée du projet de loi nº 64[2], l'article 4.1 de la Loi sur la protection des renseignements personnels dans le secteur privé (RLRQ, chapitre P-39.1, ci-après "Loi sur le secteur privé"), tel que proposé par le projet de loi nº 64, a fait l'objet de discussions concernant la possibilité d'interdire la collecte de renseignements personnels concernant un mineur de moins de 14 ans lorsque celle-ci est faite à des fins commerciales ou à des fins de profilage commercial, et ce, malgré le consentement du titulaire de l'autorité parentale ou du tuteur. Il a notamment été question des jouets connectés qui collectent des renseignements personnels sur des mineurs de moins de 14 ans.

Au moment de l'étude détaillée, j'ai pris l'engagement de recourir à l'expertise de la Commission d'accès à l'information afin d'obtenir une analyse et des recommandations concernant la possibilité d'inclure une telle interdiction dans la Loi sur le secteur privé. Cependant, je souhaite que l'analyse de la Commission d'accès à l'information ait une portée plus large.

Ainsi, selon la Commission d'accès à l'information, en tenant compte des dispositions prévues à la Loi sur le secteur privé, telles que modifiées par le projet de loi nº 64, et du contexte dans lequel évoluent les entreprises, est-ce que des mesures supplémentaires devraient être envisagées dans la Loi sur le secteur 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? Si oui, quelles sont les mesures recommandées par la Commission d'accès à l'information (interdiction complète, interdiction partielle en fonction de certains critères, etc.)? »

[Caractères gras ajoutés]

---

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

2 Désormais adopté : *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, L.Q. 2021, c. 25.

SOMMAIRE

La récente réforme de la *Loi sur la protection des renseignements personnels dans le secteur privé* (Loi sur le privé) y ajoute une mesure de protection explicite des renseignements personnels des 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.

La Commission d'accès à l'information s'est penchée sur la suffisance de cette mesure pour protéger les mineurs dans le contexte d'une collecte, d'une utilisation, d'une communication ou d'une conservation de leurs renseignements à des fins commerciales, y compris de profilage, plus spécifiquement dans l'environnement numérique.

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*, qui interdit de faire de la publicité commerciale destinée aux enfants, la Commission recommande d'interdire la collecte, l'utilisation 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.

Contexte

Les entreprises du numérique agissent comme intermédiaires de bon nombre des activités et interactions des mineurs. Elles peuvent donc recueillir beaucoup d'informations sur eux. Les frontières de plus en plus poreuses entre vies physique et numérique favorisent d'ailleurs cette tendance. L'environnement numérique est aussi dominé par le secteur privé, qui cherche principalement à tirer profit des renseignements recueillis. Il faut enfin souligner qu'il évolue extrêmement rapidement.

Les renseignements personnels des mineurs sont précieux, car ils permettent de mieux les comprendre et les influencer. Les entreprises peuvent vendre ces renseignements, mais aussi les valoriser. Par exemple, dans le modèle d'affaires très répandu de la publicité ciblée (ou économie de l'attention), leurs vrais clients sont d'autres entreprises. Les services offerts aux mineurs sont donc gratuits, mais permettent de générer des données qui servent tant à améliorer le service (pour générer plus de données) qu'à permettre aux clients commerciaux de rejoindre les segments de population qui les intéressent. Suivant ce modèle, les entreprises sont en compétition constante pour obtenir l'attention des mineurs et orientent leurs choix de design et leurs algorithmes, par exemple, pour maximiser l'engagement. Même si de grandes multinationales dictent bon nombre de normes en cette matière, il ne faut pas négliger l'effet des activités des plus petites entreprises.

Très tôt, souvent avant l'entrée au primaire, les jeunes se servent des outils numériques pour apprendre, socialiser et se divertir. Avec la pandémie de COVID-19, leur utilisation de ces outils s'est accentuée. S'ils se soucient bel et bien de leur vie privée et de leur capacité à faire des erreurs sans qu'elles les suivent toute leur vie, les stratégies de protection qu'ils emploient relèvent cependant surtout de la dissimulation d'informations *à d'autres personnes*. Ils ont ainsi peu conscience de la dimension commerciale de la vie privée, et comprennent mal l'écosystème numérique (circulation des renseignements, quantité d'acteurs impliqués, etc.). L'opacité des pratiques des entreprises contribue à cette méconnaissance. Sensibles à la pression par les pairs et prompts à l'impulsivité, les jeunes adoptent rapidement les nouvelles technologies et perçoivent généralement peu les risques à long terme, se concentrant davantage sur ceux qui concernent leur sécurité immédiate (ex. inconnus malveillants).

Les parents ont le souci d'épauler leurs enfants pour la gestion de leur vie privée en ligne, mais bien qu'ils soient de grands utilisateurs du numérique eux aussi, leur littératie en cette matière ne leur permet pas toujours de les soutenir adéquatement. À plusieurs égards, leurs attitudes et connaissances sont semblables à celles des jeunes.

Dans l'environnement numérique, les mineurs sont exposés à de nombreux risques : ils peuvent par exemple faire l'objet de microciblage, être exposés à la désinformation, voir leur sommeil déréglé, se faire voler leur identité ou subir de la discrimination. Fréquemment interreliés, ces risques se manifestent souvent en partie en raison de l'exploitation des renseignements personnels. Puisque les entreprises du numérique sont des intermédiaires de la vie numérique des jeunes, les choix qu'elles opèrent sur la base de leurs intérêts commerciaux ne sont pas neutres**.** Ils peuvent influencer de manière importante la probabilité et la nature des risques auxquels sont exposés les mineurs.

De l'avis de la Commission, la vulnérabilité des mineurs et l'asymétrie de pouvoirs très importante entre les entreprises et eux militent pour une protection légale renforcée, qui doit toutefois respecter leur autonomie et leur droit de profiter des avantages offerts par le numérique. Elle observe que le Québec protège les mineurs de façon particulière dans d'autres domaines, comme la publicité commerciale. En effet, la *Loi sur la protection du consommateur* interdit à quiconque de faire de la publicité à but commercial destinée à des moins de 13 ans. L'objectif de cette mesure – un choix de société opéré dans les années 1970 – est d'éviter l'exploitation économique des mineurs. Cet objectif, toujours d'actualité, devrait amener le Québec à renforcer l'encadrement des pratiques commerciales impliquant les renseignements personnels des mineurs dans le contexte d'une économie numérique où les données servent notamment à profiler ou à cibler des messages publicitaires pour vendre davantage.

Recommandations

La Commission a analysé la nouvelle Loi sur le privé à la lumière de recommandations internationales en matière de protection des renseignements personnels des mineurs et de textes législatifs et normatifs proposés ou adoptés dans d'autres juridictions.

Elle conclut qu'en dépit d'ajouts intéressants par rapport à l'ancien régime, le mécanisme de protection principal spécifique aux mineurs – soit le consentement parental – n'est pas suffisant pour protéger adéquatement les jeunes de l'exploitation commerciale de leurs renseignements personnels. Le fardeau de cette

protection ne doit plus reposer essentiellement sur les épaules des mineurs et de leurs parents.

Par conséquent, la Commission formule les recommandations suivantes :

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 avec le 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.

TABLE DES MATIÈRES

Mandat ..... **i**

Sommaire ..... **ii**

Contexte ii

Recommandations iii

Liste des sigles et abréviations ..... **viii**

1. Introduction **1**

Structure et contenu du rapport 2

2. Principes et concepts **4**

2.1 Convention relative aux droits de l'enfant 4

2.1.1 Principes 5

2.1.2 Droits 6

2.2 Cycle de vie et typologie des renseignements personnels 7

2.3 Dimensions de la vie privée numérique 9

2.4 Portée de l'analyse de la Commission 11

3. Contexte **12**

3.1 Caractéristiques de l'environnement numérique 12

3.1.1 Mise en données 13

3.1.2 Hyperconnectivité 14

3.1.3 Commercialisation 15

3.1.4 Vitesse d'évolution 16

3.2 Caractéristiques des acteurs en place 16

3.2.1 Entreprises 16

3.2.2 Mineurs 23

3.2.3 Parents 31

3.3 Risques numériques pour les mineurs 35

3.3.1 Typologie 36

3.3.2 Place centrale des renseignements personnels et exemples 39

3.3.3 Probabilité et impact potentiel des préjudices 44

3.4 Raisons d'agir 45

3.4.1 Vulnérabilité des mineurs 46

3.4.2 Protections existantes dans d'autres domaines 47

4. Moyens pour protéger les mineurs **50**

4.1 Mesures proposées par diverses organisations 50

4.1.1 Miser sur les individus 52

4.1.2 Miser sur les entreprises 57

4.1.3 Réaffirmer la primauté des principes de la Convention 66

4.2 Mesures mises en œuvre ou envisagées dans la législation 67

4.2.1 Europe 72

4.2.2 Amérique du Nord 77
4.2.3 Autres pays 86
4.3 Mesures mises en œuvre ou proposées dans des normes 88
4.3.1 Irlande 88
4.3.2 Pays-Bas 90
4.3.3 France 90
5. Analyse de la Loi 25 93
5.1 Présentation du cadre juridique modernisé 93
5.2 Analyse de la protection accordée aux mineurs 96
5.2.1 Nécessité, intérêt légitime, licéité de la collecte et consentement 97
5.2.2 Caractère libre et éclairé du consentement 99
5.2.3 Choix du seuil d'âge et vérifications 101
5.2.4 Consentement parental et autonomie du mineur 102
5.2.5 Consentement, individualisation de la réflexion et effets de groupe 103
5.2.6 Autres dispositions de la Loi 25 105
6. Recommandations et perspectives 106
6.1 Recommandations 106
6.1.1 Interdire la collecte, l'utilisation et la communication de renseignements personnels de mineurs pour certaines finalités 107
6.1.2 Inclure explicitement les renseignements inférés dans la portée de la loi 109
6.1.3 Inscrire certains droits de l'enfant dans la loi 109
6.1.4 Garantir des protections pour tous les mineurs, adaptées à leur âge 110
6.1.5 Accorder une préséance à l'opinion de l'adolescent 111
6.1.6 Étendre la protection par défaut 112
6.1.7 Exiger des analyses d'impact sur les droits des mineurs au sens large 112
6.1.8 Encadrer la conception des produits et services numériques 113
6.1.9 Renforcer l'éducation et la sensibilisation des mineurs et de leurs parents 114
6.2 Critères 114
6.3 Limites et perspectives 116
Références 119
ANNEXE 1 – Exemples d'interfaces truquées 137
ANNEXE 2 – Principes et catégories d'âge du *Children's Code* 140

LISTE DES SIGLES ET ABRÉVIATIONS

Forme courte	Forme longue
AMVP	Assemblée mondiale pour la protection de la vie privée (*Global Privacy Assembly*)
C-27	Projet de loi C-27, *Loi de 2022 sur la mise en œuvre de la Charte du numérique* (Canada)
CAADCA	*California Age-Appropriate Design Code Act* (États-Unis)
CCPA	*California Consumer Privacy Act* (États-Unis)
C.c.Q.	*Code civil du Québec* (Québec)
CDPDJ	Commission des droits de la personne et des droits de la jeunesse (Québec)
CEPD	Comité européen de la protection des données (Union européenne)
CIPVP	Commissariat à l'information et à la protection de la vie privée (Ontario)
CNIL	Commission nationale de l'informatique et des libertés (France)
COPPA	*Children's Online Privacy Protection Act* (États-Unis)
CPA	*Colorado Privacy Act* (États-Unis)
CPVPC	Commissariat à la protection de la vie privée du Canada (Canada)
CVK	*Code Voor Kinderrechten* (Pays-Bas)
DPA18	*Data Protection Act 2018* (Royaume-Uni)
DPC	Data Protection Commission (Irlande)
GTCVP	Groupe de travail des commissaires à la vie privée et des défenseurs canadiens des enfants et des jeunes sur la protection des renseignements personnels des enfants en ligne (Canada)
ICO	Information Commissioner's Office (Royaume-Uni)
KOSA	*Kids' Online Safety Act* (États-Unis)
LBO	Livre blanc *Modernisation de la protection de la vie privée en Ontario - Autonomiser les Ontariens et favoriser l'économie numérique* (Ontario)
LGPD	*Lei Geral de Proteção de Dados Pessoais* (Brésil)
LIA	*Législation sur l'intelligence artificielle* (Union européenne)
Loi 25	*Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Québec)
Loi sur l'accès	*Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Québec)
Loi sur le privé	*Loi sur la protection des renseignements personnels dans le secteur privé* (Québec)
LPC	*Loi sur la protection du consommateur* (Québec)
LSN	*Législation sur les services numériques* (Union européenne)

ONU	Organisation des Nations unies
PDPB	*Personal Data Protection Bill 2019* (Inde)
RGPD	*Règlement général sur la protection des données* (Union européenne)
UNICEF	Fonds des Nations unies pour l'enfance
WPA	*Washington Privacy Act* (États-Unis)

1. INTRODUCTION

L'environnement numérique offre une myriade d'opportunités aux mineurs. Ils peuvent y apprendre une multitude de choses, y découvrir d'autres cultures, y nouer des relations sociales qui contribuent à leur épanouissement, y exprimer leur opinion et la confronter à d'autres, y libérer leur créativité grâce à des outils toujours plus puissants, s'y divertir de maintes façons, et bien d'autres choses encore.

Le lustre des possibles est néanmoins terni par une abondance tout aussi remarquable de risques.

La formidable vitesse de développement du numérique y a fait entrer les mineurs par la force des choses, mais cet environnement n'a pas été conçu pour eux à l'origine. Les intérêts commerciaux qui y règnent en maîtres, les flux de données qui le traversent, les choix de conception des produits et services qui le constituent et la collecte, l'utilisation, la communication et la conservation de toujours plus de renseignements personnels qui le sous-tendent sont autant d'éléments qui peuvent entraîner des risques pour les droits fondamentaux des mineurs, au-delà même de celui à la vie privée.

Avec à l'horizon des espaces de réalité virtuelle toujours plus accessibles, de nouvelles possibilités de connexion dès les premiers instants de vie et une relation de plus en plus forte entre les univers physique et numérique, les mineurs feront vraisemblablement l'objet d'une exploitation croissante de leurs renseignements personnels. Ceux-ci serviront certes à leur offrir des services, mais aussi à les profiler pour prédire ou influencer leur comportement ou leur présenter de la publicité, ou à prendre des décisions à leur sujet, entre autres.

À travers le monde, les initiatives visant à renforcer la protection accordée aux mineurs dans le monde numérique, notamment en matière de vie privée, se multiplient. De nombreuses juridictions étudient actuellement des textes législatifs comportant des dispositions spécifiques à la protection des renseignements personnels des mineurs. En parallèle, suivant l'exemple du Royaume-Uni, plusieurs gouvernements adoptent ou envisagent d'adopter des codes normatifs présentant des orientations concrètes en matière de protection de renseignements personnels et de design numérique aux organisations offrant des produits, services et fonctionnalités auxquels les mineurs sont susceptibles d'accéder.

Au Québec, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, devenue la Loi 25 de 2021, prévoit une protection explicite pour les renseignements personnels des mineurs. Elle confie aux parents la responsabilité de consentir à la collecte, à l'utilisation et à la communication de ces renseignements lorsque les mineurs sont âgés de moins de 14 ans. Ils conservent ensuite cette possibilité jusqu'à 18 ans, conjointement avec le mineur.

Compte tenu des enjeux, ce mécanisme de protection est-il suffisant? L'autorité parentale peut-elle légitimer toute pratique reposant sur les renseignements personnels des mineurs?

Selon la Commission, **il faut répondre par la négative à ces deux questions**. Vu le contexte de l'environnement numérique et les caractéristiques des acteurs en place, les risques pour les mineurs et leurs droits l'amènent ainsi à conclure, comme cela a été le cas dans d'autres juridictions, au besoin d'une plus grande protection pour les mineurs à ce chapitre. Bien que la Loi 25 améliore la protection accordée aux renseignements personnels de tous, certaines protections additionnelles sont requises pour protéger les jeunes notamment de l'exploitation commerciale, dans le même esprit que celui qui a guidé l'interdiction de faire de la publicité commerciale destinée à des personnes de moins de 13 ans dans la *Loi sur la protection du consommateur*[3] (ci-après la LPC).

Le présent rapport présente ces éléments de réflexion et recommande des mesures de protection concrètes.

Structure et contenu du rapport

Dans les premières sections de ce rapport, la Commission **contextualise le problème**. Dans la section 2, elle revient d'abord sur les droits des mineurs, qui doivent constituer le fondement de toute discussion sur la protection des mineurs – et permettre aussi de préserver leur autonomie. Elle se penche aussi sur plusieurs concepts qui reviennent à travers la suite du rapport, puis apporte des précisions à sa façon d'aborder le mandat du ministre.

Dans la section 3, la Commission caractérise l'environnement numérique en fonction des tendances qui le traversent. Elle s'intéresse aux pratiques des entreprises, puis présente un tour d'horizon des données disponibles sur les connaissances, les pratiques et les attitudes des mineurs et de leurs parents dans l'environnement numérique. Elle fait également le point sur les risques qui se posent dans cet environnement et sur leur typologie, puis tire des constats qui imposent selon elle de protéger de manière particulière les renseignements personnels des mineurs. À cette occasion, elle dresse des parallèles avec l'interdiction de la publicité commerciale visant les moins de 13 ans.

Puisque la thématique de ce rapport retient beaucoup l'attention à l'international, la Commission **examine ensuite les interventions proposées ou mises en œuvre dans d'autres juridictions**, que ce soit dans des analyses d'autres organisations ou dans des lois et des normes. Cet exercice d'étalonnage, réalisé dans la section 4, vise notamment l'Europe, l'Ontario et les États-Unis, mais aussi l'Inde et le Brésil. Parmi les faits intéressants repérés ailleurs, la Commission note que plusieurs juridictions se sont dotées ou envisagent de se doter de normes souples qui encadrent plus spécifiquement la conception des produits et services numériques ayant un impact sur les mineurs.

---

[3] *Loi sur la protection du consommateur*, RLRQ, c. P -40.1.

Dans la section 5, après avoir présenté les modifications pertinentes apportées par la Loi 25, la Commission **analyse l'adéquation de la *Loi sur la protection des renseignements personnels dans le secteur privé*[4] (ci-après la Loi sur le privé) telle que modifié** à la lumière des éléments de contexte et des expériences internationales. Elle s'attarde en particulier sur l'efficacité du consentement parental comme mécanisme de protection.

Cet exercice la mène ensuite à **formuler 12 recommandations** dans la section 6. En un mot, la Commission estime que le Québec doit aller au-delà du consentement parental pour bien protéger les mineurs. Selon elle, il est notamment nécessaire :

- d'interdire certaines finalités pour la collecte, l'utilisation et la communication de leurs renseignements personnels;
- de faire clairement référence à l'intérêt supérieur de l'enfant et à certains autres droits des mineurs au sein même de la Loi sur le privé;
- d'intervenir sur la conception des produits et services numériques.

Les choix des entreprises étant à l'origine de plusieurs des risques encourus par les mineurs en ligne, la Commission croit que la responsabilité leur revient de mieux les protéger. Ce thème est d'ailleurs déjà prédominant dans la Loi 25.

Beaucoup d'entreprises sont déjà au fait des problèmes rencontrés par les mineurs dans l'environnement numérique et tentent de s'organiser pour mieux protéger leurs renseignements personnels. À titre d'exemple, l'initiative TeenAge Privacy Program du Center for Industry Self-Regulation américain propose notamment une feuille de route à haut niveau pour aider les entreprises à adopter des mesures limitant les risques liés à la collecte, à l'utilisation et à la communication de renseignements personnels concernant des mineurs[5]. Le Forum économique mondial se penche aussi sur des normes semblables dans le domaine de l'intelligence artificielle[6]. Bien que la Commission maintienne, comme nombre de ses homologues à l'international, que l'autoréglementation a fait son temps en matière de protection des renseignements personnels, de telles initiatives témoignent selon elle du fait que le secteur privé convient qu'il est pertinent de rendre l'environnement numérique plus sûr pour les mineurs.

Dans ce rapport, la Commission se concentre sur les enjeux liés à la commercialisation des données des mineurs par les entreprises. Ce choix impose de laisser de côté certains aspects qui mériteraient eux aussi plus d'attention. La Commission conclut donc ce rapport par une mention de quelques limites et perspectives qui s'en dégagent.

---

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

5 THE CENTER FOR INDUSTRY SELF-REGULATION, *A Roadmap for Considering Teen Privacy & Safety*, 2022, en ligne : <https://bbbnp-bbbp-stf-use1-01.s3.amazonaws.com/docs/librariesprovider5/default-document-library/tapp_roadmap.pdf>.

6 FORUM ÉCONOMIQUE MONDIAL, *Artificial Intelligence for Children - Toolkit*, 2022, en ligne : <https://www3.weforum.org/docs/WEF_Artificial_Intelligence_for_Children_2022.pdf>.

2. PRINCIPES ET CONCEPTS

Ce rapport adopte un cadre conceptuel qu'il convient d'expliciter dès le départ. Au premier chef, tout comme beaucoup de documents internationaux et de recherches traitant de la protection des renseignements personnels des mineurs, il s'appuie sur la Convention relative aux droits de l'enfant de l'ONU[7], ci-après appelée la Convention.

À travers ce document, la Commission fait également souvent référence au cycle de vie des renseignements personnels (collecte, utilisation, communication, conservation et destruction), de même qu'à leur typologie. Elle en distingue en effet trois catégories : les renseignements fournis, observés et inférés. Elle présente ensuite des « dimensions de la vie privée numérique » (interpersonnelle, institutionnelle et commerciale) issues de recherches internationales sur la protection des mineurs dans l'environnement numérique. Celles-ci permettent d'éclairer différents enjeux vécus par les mineurs en matière de protection des renseignements personnels.

À partir des différents éléments présentés dans cette section, la Commission apporte enfin quelques précisions quant à la portée de l'analyse qu'elle a menée afin de produire ce rapport.

2.1 Convention relative aux droits de l'enfant

Ratifiée par le gouvernement du Québec en 1991[8], la Convention énonce des principes et des droits que les États s'engagent à faire respecter pour tous les enfants, soit les personnes de moins de 18 ans[9]. Elle constitue un socle important pour envisager à la fois la protection et l'autonomie des mineurs, qui doivent être conciliées dans toutes décisions qui les concernent[10].

Puisque la Convention a été adoptée en 1989, plusieurs années avant qu'Internet soit couramment utilisé et avant l'expansion des technologies de l'information, son application au monde numérique soulevait plusieurs questions. Le Comité des droits de l'enfant de l'ONU a donc élaboré et diffusé, en 2021, l'Observation générale nº 25 sur les droits de

7 ORGANISATION DES NATIONS UNIES, *Convention relative aux droits de l'enfant*, (1989), traité nº 27531, en ligne : <https://www.ohchr.org/FR/ProfessionalInterest/Pages/CRC.aspx>.

8 « Convention relative aux droits de l'enfant », *Commission des droits de la personne et des droits de la jeunesse*, en ligne : <https://www.cdpdj.qc.ca/fr/vos-droits/lois-qui-protegent-vos-droits/convention-relative-aux-droits-de-lenfant> (consulté le 4 mars 2022).

9 Convention, art. 1.

10 Valerie STEEVES, *It's Time for a Change: Rethinking Policies to Protect Children's Rights in a Datafied World*, coll. Kids & Technology Essay Series, 2021, p. 12, en ligne : <https://www.mediatechdemocracy.com/s/Steeves_Nov21.pdf>.

l'enfant en relation avec l'environnement numérique[11]. Cet addendum précise la portée à donner aux articles de la Convention en lien avec les pratiques numériques actuelles.

2.1.1 Principes

La Convention consacre quatre grands principes[12] : la non-discrimination, l'intérêt supérieur de l'enfant, le droit à la vie, à la survie et au développement et la participation. Ceux-ci constituent « le filtre à travers lequel il faudrait envisager la mise en œuvre de tous les autres droits consacrés par la Convention »[13]. De plus, l'application de la Convention doit tenir compte de l'évolution des capacités de l'enfant, qui accède graduellement à l'autonomie en acquérant plus de maturité.

Le tableau suivant résume chacun de ces principes. Il résume également les considérations relatives au numérique mentionnées dans l'Observation générale nº 25 et ayant un lien avec la protection des renseignements personnels[14].

Convention	Observation générale nº 25
Non-discrimination : Les droits de la Convention s'appliquent à tout enfant, sans distinction aucune[15].	La discrimination peut notamment être causée par un traitement injuste dans l'environnement numérique. Elle peut aussi survenir lorsque des informations partiales, partielles ou obtenues de manière inéquitable sont utilisées par des processus automatisés (filtrage de l'information, profilage, prise de décision) visant l'enfant[16].
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[17].	L'intérêt supérieur doit être une considération primordiale dans toutes les décisions concernant l'environnement numérique (réglementation, conception, utilisation, etc.)[18]. **Note** : L'observation générale nº 14 précise les paramètres à considérer lors de l'évaluation de l'intérêt supérieur de l'enfant : son opinion, son identité, la préservation de son milieu familial et le maintien de ses relations, sa prise en charge, sa protection et sa sécurité, sa situation particulière de

11 COMITÉ DES DROITS DE L'ENFANT DE L'ORGANISATION DES NATIONS UNIES, *Observation générale nº 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%2fPPRiCAqhKb7yhsqlkirKQZLK2M58RF%2f5F0vEG%2bcAAx34gC78FwvnmZXGFsdFXGQsWU46nx%2b5vAg3QbGXlnOwo3Oquj8nN7ltX6yUYoRpe7N%2b7Q6mEUIz2mfWi> (consulté le 16 décembre 2021).

12 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, précité, note 8.

13 Observation générale nº 25, précité, note 11, par. 8.

14 Ces liens sont clarifiés dans la section 3.3 de ce rapport.

15 Convention, art. 2.

16 Observation générale nº 25, précité, note 11, par. 10.

17 Convention, art. 3.

18 Observation générale nº 25, précité, note 11, par. 12.

Convention	Observation générale nº 25
	vulnérabilité, son droit à la santé et son droit à l'éducation[19].
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 social et culturel[20].	Les États doivent prendre les mesures nécessaires pour réduire les risques de contenus, de contacts, de comportements et de contrats[21] (voir section 3.3.1 de ce rapport). L'utilisation des appareils numériques ne devrait pas être nocive ou remplacer les interactions en personne, particulièrement dans les premières années de vie[22].
Participation : L'opinion de l'enfant doit être prise en compte lorsque des décisions sont prises à son sujet[23].	Les États devraient promouvoir les outils numériques permettant aux enfants de faire valoir leur opinion[24], associer les enfants à l'élaboration de politiques, de programmes ou de services qui les visent[25] et recourir au numérique pour les consulter au besoin. Dans ce cas, ils doivent s'assurer que cette consultation ne mène pas à une collecte exagérée de renseignements personnels[26].
Évolution des capacités : Le besoin de protection de l'enfant diminue 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[27].	Les risques et les possibilités associés au numérique varient avec le stade de développement de l'enfant[28]. Les États devraient s'assurer que les services numériques respectent son développement[29]. De plus, ils devraient agir en matière de sensibilisation et d'éducation au numérique auprès des personnes qui s'occupent des enfants afin de les aider à apporter un soutien adéquat, qui respecte le droit à la vie privée, l'autonomie et les capacités de l'enfant[30].

2.1.2 Droits

Outre les principes qu'elle établit, la Convention reconnaît aux enfants de nombreux droits. Parmi ceux-ci, plusieurs entrent en ligne de compte lorsque les entreprises

---

19 COMITÉ DES DROITS DE L'ENFANT DE L'ORGANISATION DES NATIONS UNIES, *Observation générale nº 14 (2013) sur le droit de l'enfant à ce que son intérêt supérieur soit une considération primordiale*, 2013, en ligne : <http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2f5F0vEAXPu5AtSWvliDPBvwUDNUcLY%2bjlY9LwV%2bqu%2f76ghnFz5ngXgCakqefOzjKZHk9XN8vDnGlPnxGqaEEn4Buo1n> (consulté le 16 décembre 2021).

20 Convention, art. 6.

21 Observation générale nº 25, précité, note 11, par. 14.

22 *Id.*, par. 15.

23 Convention, art. 12.

24 Observation générale nº 25, précité, note 11, par. 16.

25 *Id.*, par. 17.

26 *Id.*, par. 18.

27 Convention, art. 5.

28 Observation générale nº 25, Observation générale nº 25, précité, note 11, par. 19.

29 *Id.*, par. 20.

30 *Id.*, par. 21.

recueillent, utilisent, communiquent ou conservent des renseignements personnels à leur sujet :

- Droit de s'exprimer et de penser librement[31];
- Droit à la vie privée[32];
- Droit à l'information[33];
- Droit de jouer, de se relaxer et de participer pleinement à la vie culturelle et artistique[34];
- Droit de ne pas être exploités économiquement[35] ou de toute manière qui nuit à leur bien-être[36].

Plusieurs pratiques numériques actuelles constituent des risques pour ces droits, ce qui sera détaillé à travers ce rapport, notamment dans la section 3.3.

2.2 Cycle de vie et typologie des renseignements personnels

Un renseignement personnel est une information qui permet, directement ou indirectement (en combinaison avec d'autres), d'identifier un individu[37]. Il peut s'agir par exemple d'un nom, d'un âge, d'une position GPS précise, d'une adresse IP, d'un identifiant publicitaire ou d'une adresse courriel, mais aussi d'informations concernant les intérêts, les émotions, les attitudes, les habitudes, l'identité, les activités, les relations, etc.[38].

Lorsqu'il est détenu par une autre personne ou par une organisation, le renseignement personnel traverse cinq étapes qui constituent son cycle de vie. Chacune de ces étapes, représentées ci-après, est associée à des risques particuliers et est encadrée par des dispositions légales qui balisent les possibilités et les obligations des organisations :

31 Convention, art. 13 -14.
32 *Id.*, art. 16.
33 *Id.*, art. 17.
34 *Id.*, art. 31.
35 *Id.*, art. 32.
36 *Id.*, art. 36.
37 Loi sur le privé telle que modifiée par la Loi 25, article 2.
38 Observation générale nº 25, précité, note 11, par. 68.

Collecte	Utilisation	Communication	Conservation	Destruction
Moment où le renseignement personnel est recueilli, créé ou inféré	Moment(s) où le renseignement personnel est mis à profit pour atteindre une finalité	Moment(s) où le renseignement personnel est transmis à des tiers	Période où le renseignement personnel est détenu	Moment où le renseignement personnel est détruit, et n'est donc plus détenu

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. La juriste Simone van der Hof classe les renseignements personnels en trois catégories[39], que l'on peut représenter avantageusement à l'aide de la métaphore de l'iceberg :

39 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. Van der Hof utilise le terme *data* (données), potentiellement plus large que *renseignement personnel*. Voir aussi Mariya STOILOVA, 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>; COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, *Who knows what about me? A Children's Commissioner report into the collection and sharing of children's data*, 2018, en ligne : <https://dera.ioe.ac.uk//32673/1/who-knows-what-about-me.pdf>.

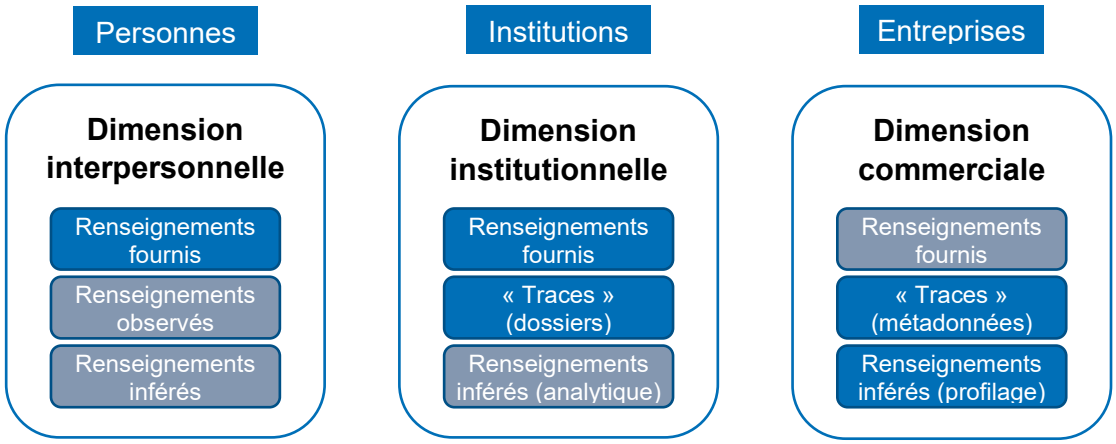
2.3 Dimensions de la vie privée numérique

Lorsqu'il s'agit des comportements par rapport à la protection des renseignements personnels, plusieurs parlent de *paradoxe de la vie privée* : alors que les individus se disent soucieux de leur vie privée, ils semblent adopter des pratiques de partage de leurs renseignements qui contredisent cette préoccupation.

Les mineurs n'échappent pas à cette tendance. De l'avis des chercheuses Mariya Stoilova, Sonia Livingstone et Rishita Nandagiri[40], ce paradoxe n'est pas réel[41] : il découle plutôt d'une vision de la vie privée qui ne tient pas suffisamment compte du *contexte* des échanges informationnels.

De leur point de vue, pour exercer leur droit à l'autodétermination informationnelle (qui est une dimension du droit à la vie privée), les individus exercent des choix par rapport aux renseignements personnels qu'ils souhaitent partager – ou non – avec les différents acteurs avec qui ils interagissent. Les stratégies déployées à cet effet varient donc en fonction du contexte. C'est ce que vise à refléter la typologie suivante, proposée par ces chercheuses[42] pour décrire les comportements informationnels des mineurs.

Cette typologie distingue trois dimensions de la vie privée numérique en fonction de l'acteur avec lequel l'individu est en relation. Chaque dimension est caractérisée par l'emploi prédominant de certains types de renseignements personnels (fournis, observés ou inférés).



40 M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39.

41 Voir aussi Samantha MCALEESE, Matthew JOHNSON et Marc LADOUCEUR, *Les jeunes Canadiens s'expriment : une recherche qualitative sur la protection de la vie privée et le consentement*, Ottawa, HabiloMédias, 2020, p. 6-7, en ligne : <https://habilomedias.ca/sites/default/files/publication-report/full/rapport_jeunes_canadiens_sexpriment.pdf>.

42 M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39, p. 7, notre traduction. Pour plus de details, voir 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, en ligne : <https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review.pdf>.

- **La dimension interpersonnelle** concerne la gestion des renseignements personnels dans les relations du mineur avec d'autres personnes (membres de sa famille, pairs, étrangers) dans l'objectif de créer et de maintenir une *identité informationnelle* à travers des liens sociaux.
    - Ce contexte est caractérisé par une prédominance 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.
    - Dans ce contexte, les renseignements personnels du mineur sont soit fournis par lui, soit observés – les dossiers (scolaire, médical, etc.) à son sujet en sont un exemple.
    - Il faut noter une interaction croissante entre les dimensions institutionnelle et commerciale (voir ci-bas). Par exemple, le mineur peut avoir l'obligation d'interagir avec un acteur commercial dans un contexte institutionnel, comme s'il utilise une technologie éducative à l'école[43].
- **La dimension commerciale** concerne la collecte, l'utilisation, la communication ou la conservation des renseignements personnels du mineur par des entreprises à des fins commerciales.
    - Dans ce contexte, les renseignements fournis ont peu de poids. L'essentiel des activités commerciales repose sur des renseignements observés (par exemple, grâce à des métadonnées ou à des témoins de connexion) ou inférés (par exemple, par profilage[44]).

Dans ce cadre conceptuel, le paradoxe de la vie privée évoqué précédemment s'explique par le fait que les mineurs ont une vision essentiellement *interpersonnelle* de la vie privée[45]. Cela affecte leurs relations avec les institutions et les entreprises et teinte leur compréhension des pratiques de ces acteurs par rapport aux renseignements personnels, notamment parce qu'elles reposent beaucoup sur des renseignements observés ou inférés, dont ils ont moins conscience. Cet aspect est présenté plus en détail dans la section 3.2.2.2.

---

43 Mark GOLLOM, « Educational tech, including CBC Kids, harvested personal data from children, new report claims », *CBC News* (25 mai 2022), en ligne : <https://www.cbc.ca/news/canada/cbc-kids-personal-data-educational-technology-1.6465739> (consulté le 2 juin 2022); voir aussi HUMAN RIGHTS WATCH, *« How Dare They Peep into My Private Life? » Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic*, 2022, en ligne : <https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments> (consulté le 8 juin 2022).

44 Tant le *Règlement général sur la protection des données* que la Loi 25 définissent le profilage de manière semblable : il s'agit d'une forme automatisée de collecte ou d'utilisation de renseignements personnels qui vise à évaluer les caractéristiques d'un individu, notamment à des fins d'analyse ou de prédiction en différentes matières, comme la santé, les préférences personnelles, les intérêts ou le comportement. *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) (Texte présentant de l'intérêt pour l'EEE)*, (2016), OOJ 2016 L 119/1, art. 4, en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679>.; Loi 25, articles 19 et 107.

45 S. LIVINGSTONE, M. STOILOVA et R. NANDAGIRI, précité, note 42, p. 23.

2.4 Portée de l'analyse de la Commission

À la lumière des éléments présentés dans cette section, la Commission a ajusté la portée de sa recherche et de son analyse en lien avec le mandat qui lui a été donné :

- Suivant l'article premier de la Convention, un enfant est une personne de moins de 18 ans. Puisque les enjeux de protection des renseignements personnels des adolescents sont nombreux, et en cohérence avec ses prises de position antérieures[46], **la Commission considère également les 14 à 17 ans dans son analyse**. **Sauf mention contraire, l'utilisation du terme « mineur » dans la suite de ce rapport renvoie donc aux moins de 18 ans.**
- Comme l'indique l'Observation générale nº 25, le numérique joue désormais un rôle prépondérant dans la vie des mineurs. Par conséquent, **l'analyse de la Commission se concentre sur la protection des renseignements personnels dans cet environnement**.
- Étant donné la question posée par le ministre, la dimension commerciale de la vie privée est au cœur de ce 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, bien que la question du ministre se concentre sur la collecte et l'utilisation, **la Commission a élargi son analyse pour considérer également la communication et la conservation des renseignements**.

[46] COMMISSION D'ACCÈS À L'INFORMATION, *Révision du programme d'études Éthique et culture religieuse – Mémoire de la Commission d'accès à l'information présenté au Secteur de l'éducation préscolaire et de l'enseignement primaire et secondaire du ministère de l'Éducation et de l'Enseignement supérieur*, 2020, p. 3, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_M_ECR_MEES_vf.pdf>, note 3.

3. CONTEXTE

Quelles sont les caractéristiques des mineurs? Leurs parents ont-ils tous les outils pour les épauler? Quelles sont les pratiques des entreprises qui impliquent des renseignements personnels? Quel est l'éventail des risques que peut présenter le numérique? Pour arriver à formuler des recommandations sur les mesures de protection des renseignements personnels des mineurs, ces questions méritent un examen attentif.

Dans cette section, la Commission caractérise d'abord l'environnement numérique, incontournable dans la vie des jeunes Québécoises et Québécois, afin de préciser les tendances qui le traversent et qui cadrent les interactions dont il est le théâtre. Elle constate qu'il génère des risques importants pour les mineurs.

La Commission s'attarde ensuite aux pratiques actuelles des entreprises qui fournissent des produits et des services numériques. Entre autres, les modèles reposant sur la publicité comportementale ou sur la vente de renseignements personnels sont source de préoccupations importantes. Les comportements et les attitudes des mineurs et de leurs parents, qui permettent de mieux comprendre de quelle façon les mineurs sont confrontés à ces risques et y réagissent, sont ensuite décrits. En particulier, les recherches tendent à démontrer que tous deux ont une littératie numérique limitée entre autres en raison de la grande complexité des pratiques de collecte, d'utilisation, de communication et de conservation de renseignements personnels, qui les défavorise face aux entreprises.

Une fois présenté un tour d'horizon des catégories de risques qui se posent pour les mineurs en ligne et de leur impact potentiel sur leurs droits, la Commission met en relation tous ces éléments pour souligner la vulnérabilité particulière des mineurs dans le monde numérique, et fait le parallèle avec les considérations qui ont animé le Québec à l'époque de l'interdiction de la publicité commerciale visant les moins de 13 ans.

3.1 Caractéristiques de l'environnement numérique

L'environnement numérique est une source intarissable d'opportunités pour les mineurs, qui peuvent par exemple y faire des apprentissages, y nouer des relations sociales ou y exprimer leur point de vue. Les outils qu'il comprend sont devenus incontournables dans la vie des jeunes Québécoises et Québécois. Néanmoins, nombre de ces produits et services devenus courants sont gourmands de renseignements personnels.

Selon la juriste Simone van der Hof, trois grandes tendances caractérisent l'environnement numérique[47] : la mise en données, l'hyperconnectivité et la commercialisation. L'évolution rapide de cet environnement en constitue également une

[47] S. VAN DER HOF, précité, note 39, p. 103 et suivantes.

propriété transversale. L'effet combiné de ces forces sur la vie privée des mineurs et la réalisation de leurs droits est particulièrement important.

3.1.1 Mise en données

L'environnement numérique est un espace de **mise en données** (*datafication* en anglais), que l'Office québécois de la langue française définit comme la « captation de données reliées à une activité en vue de leur exploitation »[48].

Grâce aux nouvelles technologies, cette mise en données se réalise désormais en continu. Elle concerne presque tous les aspects de la vie des individus, y compris des mineurs. Les comportements, les corps, les émotions, les relations sociales ou les préférences font tous l'objet d'une quantification intensive[49].

Des données sont ainsi recueillies par des organisations quand les mineurs :

- interagissent avec des vidéos;
- clavardent avec des amis;
- utilisent des applications;
- cherchent des informations dans un moteur de recherche;
- formulent une demande vocale à une enceinte connectée;
- font du sport en portant un bracelet intelligent;
- font l'objet d'un partage de renseignements par un proche (ex. publication d'une photo)[50];
- etc.

Ces données sont en fait des *mégadonnées* : elles sont générées en énorme quantité (volume)[51], sont d'une multitude de types (variété) et sont obtenues, analysées et échangées en temps réel (vitesse)[52]. Elles sont surtout observées et inférées plutôt que

---

48 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Grand dictionnaire terminologique - mise en données », *Grand dictionnaire terminologique* (2014), en ligne : <https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26523020> (consulté le 9 mars 2022).

49 Giovanna MASCHERONI, « Researching datafied children as data citizens », *Journal of Children and Media* 2018.1-7, DOI : 10.1080/17482798.2018.1521677.

50 COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, précité, note 39.

51 Selon une estimation de l'entreprise de publicité pour enfants SuperAwesome en 2017, les enfants sont en contact avec un à deux millions d'outils de traçage chaque année, chacun recueillant plusieurs données à leur sujet. **À l'âge de treize ans, pas moins de 72 millions de données à leur sujet auraient déjà été recueillies**. Richard HARRIS, « 72M data points collected on children in spite of COPPA », *App Developer Magazine* (27 décembre 2017), en ligne : <https://appdevelopermagazine.com/72m-data-points-collected-on-children-in-spite-of-coppa/> (consulté le 9 mars 2022).

52 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Grand dictionnaire terminologique - mégadonnées », *Grand dictionnaire terminologique* (2020), en ligne : <https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26507313> (consulté le 9 mars 2022).

fournies par les personnes concernées elles-mêmes, suivant la typologie présentée dans la section 2.2 de ce rapport.

Ce concept de mise en données comporte une dimension sociologique : en quantifiant l'individu, les organisations le positionnent comme un objet dont elles peuvent exploiter les caractéristiques[53]. Il devient ainsi en quelque sorte un « assemblage de données numériques » qui le représente (sommairement et imparfaitement) dans l'environnement numérique[54]. Dans le cas des mineurs en particulier, cette situation pose un risque pour la réalisation de leurs droits : par exemple, alors qu'ils sont en pleine construction identitaire, les données recueillies à leur sujet les cristallisent dans un état antérieur et peuvent poser d'importants problèmes d'exactitude[55]. Ce problème peut être amplifié par la conservation à long terme de renseignements à leur sujet, alors que l'évolution du mineur peut rapidement les rendre périmés. En parallèle, ces « assemblages de données numériques » et les décisions dont ils sont la base peuvent contribuer à définir la perception que les mineurs ont d'eux-mêmes ou leurs comportements en ligne[56].

3.1.2 Hyperconnectivité

Aujourd'hui, les montres, les haut-parleurs, les télévisions, les électroménagers, les caméras et même les jouets sont reliés à Internet[57]. C'est le résultat d'une deuxième tendance qui caractérise l'environnement numérique : l'**hyperconnectivité**. Celle-ci émerge des nouveaux moyens techniques qui permettent désormais aux objets et aux lieux de s'intégrer aux réseaux où interagissent déjà les personnes et les organisations.

L'hyperconnectivité accroît considérablement la mise en données, puisqu'elle permet d'interrelier les environnements physique et numérique. La chercheuse Giovanna Mascheroni l'explique ainsi[58] :

> Une fois que les objets sont connectés à l'Internet et équipés de capteurs et de composantes électroniques qui permettent la production et l'échange de données, ils deviennent des *médias* [ou *instruments*] qui « médiatisent[59] ce qui n'était pas

---

53 S. LIVINGSTONE, M. STOILOVA et R. NANDAGIRI, précité, note 42, p. 3, note 1; V. STEEVES, précité, note 10, p. 12; G. MASCHERONI, précité, note 49, p. 3.

54 Deborah LUPTON et Ben WILLIAMSON, « The datafied child: The dataveillance of children and implications for their rights », (2017) 19-5 *New Media & Society* 780-794, DOI : 10.1177/1461444816686328.

55 UNICEF et MINISTÈRE DES AFFAIRES ÉTRANGÈRES DE LA FINLANDE, *Policy guidance on AI for children*, UNICEF, 2020, p. 19, en ligne : <https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf>.

56 Valerie STEEVES et Jane BAILEY, « Our project », *eQuality Project*, en ligne : <https://www.equalityproject.ca/our-project/> (consulté le 17 mars 2022).

57 S. VAN DER HOF, précité, note 39; G. MASCHERONI, précité, note 49; Valérie MONTCALM, Alexandre PLOURDE et Elise THÉRIAULT, *Enfants sous écoute – La protection de la vie privée dans l'environnement des jouets intelligents*, Option consommateurs, 2018, en ligne : <https://option-consommateurs.org/wp-content/uploads/2018/11/oc-jouets-i-rapport-final.pdf>.

58 G. MASCHERONI, précité, note 49, p. 2, notre traduction.

59 Ce mot est utilisé aussi en son sens didactique : « Servir d'intermédiaire pour transmettre quelque chose ». Voir ÉDITIONS LAROUSSE, « Définitions : médiatiser - Dictionnaire de français Larousse », *Dictionnaire Larousse en ligne*, en ligne : <https://www.larousse.fr/dictionnaires/francais/m%C3%A9diatiser/50110> (consulté le 9 mars 2022).

> médiatisé auparavant ». Il en résulte une reconfiguration de l'expérience et du sens mêmes d'être « en ligne ». Alors que le fait d'être en ligne peut être qualifié de discontinu, « être connecté est une expérience continue ». Nous générons un flux constant de traces numériques en naviguant à travers les mondes en ligne et hors ligne, de telle sorte que la mise en données […] et la *dataveillance* (la surveillance continue des pratiques des citoyens et des consommateurs rendue possible par la mise en données) forment désormais, pour plusieurs, le cadre général de la vie quotidienne.
>
> [Références omises]

Par conséquent, la mise en données au sujet des mineurs survient de manière quasi permanente, peu importe l'activité à laquelle ils prennent part.

3.1.3 Commercialisation

La troisième tendance identifiée par Simone van der Hof est la **commercialisation** de l'environnement numérique, un « monde qui, de façon prédominante, est construit et programmé par des entreprises pour servir leurs intérêts économiques »[60]. La plupart des éléments familiers de l'écosystème numérique, comme les applications, la fourniture de services Internet, les sites Web ou les objets connectés sont ainsi conçus et contrôlés par le secteur privé, et ce, depuis l'avènement du Web. Ce sont donc les entreprises qui dictent pour l'essentiel le design du numérique et ses fonctionnalités, généralement en suivant des impératifs commerciaux[61].

La recherche du profit explique en grande partie les dynamiques de mise en données et d'hyperconnectivité, qui permettent de constamment raffiner la compréhension des consommateurs (y compris potentiels, comme les mineurs) par les entreprises. Celles-ci déploient tout un éventail de stratégies et d'outils pour obtenir plus de données, lesquelles sont à la base de plusieurs modèles d'affaires et constituent un moteur pour l'innovation. Leurs pratiques sont souvent volontairement opaques[62], ce qui crée selon van der Hof une « visibilité invisible » : **les individus, y compris les mineurs, sont de plus en plus transparents pour les organisations, mais d'une manière qui leur est inconnue**[63].

---

60 S. VAN DER HOF, précité, note 39, p. 107, notre traduction.

61 Voir REVEALING REALITY, *Pathways: How digital design puts children at risk*, 5Rights Foundation, 2021, en ligne : <https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf>; 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, citée dans; V. STEEVES, précité, note 10, p. 11.

62 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*, Québec, 2020, p. 17-18, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_M_projet_loi_64_modernisation_PRP.pdf>; COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, précité, note 39, p. 11.

63 S. VAN DER HOF, précité, note 39, p. 109-110; David LYON, *Au-delà de la surveillance des mégadonnées - Liberté et équité. Rapport pour tous les Canadiens et Canadiennes*, Surveillance Studies Centre/Queen's University, 2022, p. 8, en ligne : <https://www.sscqueens.org/sites/sscqueens.org/files/bds_rapport_fr_2022-05-17.pdf>; voir aussi Kara

Les autorités de contrôle et les experts eux-mêmes peinent à comprendre ce qu'il advient des données une fois qu'elles sont collectées[64].

3.1.4 Vitesse d'évolution

Comme le souligne le Forum économique mondial[65], la quatrième révolution industrielle, que l'on peut lier notamment aux caractéristiques de l'environnement numérique présentées précédemment, implique des changements à une vitesse jamais égalée. L'effet des technologies entraîne une progression exponentielle plutôt que linéaire. Cela implique notamment que :

- Les enjeux connus par rapport au monde numérique actuel ne sont qu'une partie de ceux qui sont appelés à émerger au cours des prochaines années[66];
- Les innovations dans les pratiques vont souvent à un rythme plus rapide que les mécanismes de protection mis en place pour en limiter les impacts négatifs[67];
- La réglementation et les lois élaborées aujourd'hui sont susceptibles de devoir être mises à jour fréquemment pour atteindre leurs objectifs[68].

3.2 Caractéristiques des acteurs en place

La collecte, l'utilisation et la communication à des fins commerciales des renseignements personnels des mineurs impliquent trois acteurs : les **entreprises**, les **mineurs** et leurs **parents** (qui jouent un rôle de médiateurs, et auxquels la Loi 25 confie explicitement la responsabilité de consentement jusqu'à ce que le mineur ait 14 ans). Cette section vise à brosser le portrait de chacun d'entre eux par rapport à l'environnement numérique.

3.2.1 Entreprises

Derrière les finalités commerciales se trouvent bien sûr des entreprises. Celles-ci occupent une place clé dans l'écosystème numérique, étant à l'origine de la plupart des produits et services courants utilisés par les mineurs.

BRISSON-BOIVIN et Samantha MCALEESE, *Averti aux algorithmes : Les jeunes Canadiens discutent l'intelligence artificielle et la confidentialité*, HabiloMédias, 2021, p. 16, en ligne : <https://habilomedias.ca/recherche-et-politique/averti-aux-algorithmes%C2%A0-les-jeunes-canadiens-discutent-l%E2%80%99intelligence-artificielle-et-la> – ceux-ci désignent ce phénomène sous le nom de « paradoxe de l'information ».

64 COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, précité, note 39, p. 11.

65 Klaus SCHWAB, « The Fourth Industrial Revolution: what it means and how to respond », *World Economic Forum* (14 janvier 2016), en ligne : <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> (consulté le 9 mars 2022).

66 COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, précité, note 39, p. 11, 13 -16.

67 D. LYON, précité, note 63, p. 10.

68 *Id.*

En effet, les mineurs sont une clientèle particulièrement intéressante[69] – et constituent même le tiers des utilisateurs d'Internet[70]. Ils forment un marché à trois couches[71] :

- **Marché primaire :** les mineurs ont des moyens (en temps ou en argent) qu'ils peuvent mobiliser directement en utilisant des services ou en procédant à des achats;
- **Marché d'influence :** ils ont un certain pouvoir sur les choix de consommation de leurs parents;
- **Marché futur :** ils seront un jour des consommateurs avec un plus grand pouvoir d'achat, et il est avantageux de les fidéliser.

Une poignée d'entreprises, souvent multinationales, mènent des activités dont l'ampleur est particulièrement vaste. Elles contrôlent une part substantielle du marché et détiennent un pouvoir certain quant à l'évolution des pratiques numériques. On ne saurait toutefois banaliser l'importance des activités commerciales des entreprises de moins grande envergure[72]. Comme le souligne l'organisme britannique 5Rights Foundation, « [les petits fournisseurs] ne devraient pas être assujettis à des standards moins élevés que ceux qui comptent plus d'utilisateurs ou d'employés. […] Les enfants ont le droit d'être protégés où qu'ils soient en ligne »[73]. Par ailleurs, tant les entreprises qui accumulent des données et les vendent que celles qui les obtiennent et les utilisent peuvent être à l'origine de risques pour les mineurs. Les éléments présentés ci-bas doivent donc être envisagés pour le secteur privé de manière générale.

La Commission 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 fondamentalement problématiques pour la protection des renseignements personnels, notamment celui de la publicité comportementale.

3.2.1.1 Contexte économique

Dans l'économie moderne, les entreprises ont un intérêt marqué pour les données. Celles-ci leur permettent d'innover, de comprendre les consommateurs et de proposer des

---

69 OFFICE DE LA PROTECTION DU CONSOMMATEUR, *Vos enfants et la pub*, 2008, p. 5, en ligne : <https://www.opc.gouv.qc.ca/fileadmin/media/documents/consommateur/sujet/publicite-pratique-illegale/EnfantsPub.pdf>.

70 Emma DAY, « Data governance for children: An emerging priority area for privacy professionals », *Unicef* (19 mai 2022), en ligne : <https://www.unicef.org/globalinsight/stories/data-governance-children-emerging-priority-area-privacy-professionals> (consulté le 25 mai 2022).

71 Milda MAČĖNAITĖ, « Protecting Children Online: Combining the Rationale and Rules of Personal Data Protection Law and Consumer Protection Law », dans Mor BAKHOUM, Beatriz CONDE GALLEGO, Mark-Oliver MACKENRODT et Gintarė SURBLYTĖ-NAMAVIČIENĖ (dir.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?*, coll. MPI Studies on Intellectual Property and Competition Law, Berlin, Heidelberg, Springer, 2018, p. 331-375, p. 332, en ligne : <https://doi.org/10.1007/978-3-662-57646-5_13> (consulté le 6 décembre 2021).

72 Dans les termes de la juriste Emma Day, « il y a peu d'entreprises qui traitent des données qui ne traitent pas aussi des données d'enfants ». E. DAY, précité, note 70, notre traduction.

73 REVEALING REALITY, précité, note 61, p. 11, notre traduction.

produits et services plus attrayants. De plus en plus, on constate que les entreprises modernes intègrent les données à tous les niveaux[74]. Il peut aussi en résulter un effet d'entraînement lié à la nature compétitive du marché.

Pour une partie des entreprises, ces données sont même une, sinon *la* source de valeur qui leur permet ultimement de générer du profit[75]. Par exemple, elles peuvent les accumuler et les vendre directement à des tiers qui souhaitent les mobiliser à leur tour. Elles peuvent aussi vendre des services d'analytique. Puisque les données sont intangibles, elles peuvent d'ailleurs être mobilisées à cette fin de façon complémentaire aux activités principales de l'entreprise.

Étant donné leur objectif ultime de générer du profit, les entreprises du numérique sont à l'origine de choix de conception et de modèles d'affaires qui ont un impact considérable sur les utilisateurs, y compris sur les mineurs. L'économie fondée sur les données mène à des activités qui analysent et influencent les comportements et qui les exploitent : les visées sous-jacentes sont celles de persuader, de créer des habitudes, de vendre, etc.[76].

L'un des modèles d'affaires numériques les plus connus est celui de la publicité comportementale, élément fondamental de l'économie dite « de l'attention ».

3.2.1.2 Publicité comportementale et économie de l'attention

Une bonne partie des services en ligne qui se sont graduellement imposés dans nos vies et dans celles des mineurs ces dernières années nous est proposée gratuitement. Nul besoin de débourser quoi que ce soit pour s'inscrire sur un réseau social ou pour regarder des vidéos sur des sites de partage, par exemple. Pour d'autres services, des frais sont exigés, mais ils sont minimes par rapport aux frais d'exploitation assumés par l'entreprise (ex. abonnement à 10 $ par mois pour un service d'écoute de musique en continu). En fait, les modèles par abonnement ou autres sont de plus en plus rares, puisqu'ils sont difficiles à rentabiliser[77].

---

74 « L'entreprise de 2025 pilotée par les données », *Ministère de l'Économie et de l'Innovation* (23 mars 2022), en ligne : <https://www.economie.gouv.qc.ca/objectifs/informer/vecteurs/entreprise-entrepreneuriat-et-croissance-des-pme-html/lentreprise-de-2025-pilotee-par-les-donnees/> (consulté le 25 mars 2022).

75 Maximilian BOCK et Martin WIENER, *Towards a Taxonomy of Digital Business Models – Conceptual Dimensions and Empirical Illustrations*, *ICIS 2017 Proceedings*, Séoul (Corée du Sud), International Conference on Information Systems, décembre 2017, en ligne : <https://www.researchgate.net/profile/Maximilian-Bock/publication/325627453_Towards_a_Taxonomy_of_Digital_Business_Models_-_Conceptual_Dimensions_and_Empirical_Illustrations/links/5b1950eea6fdcca67b635a99/Towards-a-Taxonomy-of-Digital-Business-Models-Conceptual-Dimensions-and-Empirical-Illustrations.pdf>; S. ZUBOFF, précité, note 61, p. 97.

76 Laurien DESIMPELAERE, Liselot HUDDERS et Dieneke Van de SOMPEL, « Children's and Parents' Perceptions of Online Commercial Data Practices: A Qualitative Study », (2020) 8-4 *Media and Communication* 163-174, p. 164, DOI : 10.17645/mac.v8i4.3232.

77 Anirudh EKAMBARANATHAN, Jun ZHAO et Max VAN KLEEK, *« Money makes the world go around »: Identifying Barriers to Better Privacy in Children's Apps From Developers' Perspectives*, *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, Yokohama Japan, ACM, CHI '21:

Cependant, comme le veut une populaire expression imagée, « si c'est gratuit, c'est vous le produit ». En réalité, l'utilisation de ces services n'est gratuite ou abordable que *financièrement*, mais implique d'accepter une collecte étendue de renseignements personnels[78]. M[e] Alexandre Plourde, juriste à l'organisme Option consommateurs, l'explique en ces termes[79] :

> Pourtant, cette apparente gratuité a un coût pour le consommateur.
>
> En échange d'un compte Facebook ou d'une requête sur Google, il doit accepter de divulguer un nombre considérable de renseignements personnels : historique Web, termes recherchés, achats en ligne, adresse IP, etc. Ces renseignements, une fois combinés, permettent de dresser le profil du consommateur, de deviner ses habitudes, ses champs d'intérêt… et d'afficher des publicités y correspondant sur les sites qu'il fréquente.

Autrement dit, les entreprises qui fournissent des services numériques gratuits (ou très abordables) les financent en s'adressant à une autre clientèle : celle des publicitaires[80]. Vues sous cet angle, leurs activités commerciales comportent deux volets[81] :

- D'un côté, elles proposent un service aux individus, généralement axé sur le contenu (vidéos, nouvelles, musique, jeux, etc.);
- De l'autre, elles proposent des outils publicitaires à des tiers.

Ces tiers paient en argent. Leur objectif est de maximiser le rayonnement de leurs publicités. Les fournisseurs de services numériques peuvent leur offrir deux éléments importants, souvent simultanément[82] :

- L'attention des individus, sous forme de temps;
- Le ciblage de cette attention, sous forme de profils publicitaires créés grâce aux renseignements personnels (par un processus de profilage).

Au fil de leur navigation sur le service, les individus sont donc exposés à des publicités. Celles-ci sont adaptées à eux : elles varient selon leurs intérêts exprimés ou inférés, leur

---

CHI Conference on Human Factors in Computing Systems, 6 mai 2021, p. 1-15, p. 8, DOI : 10.1145/3411764.3445599.

78 M. MAČĖNAITĖ, précité, note 71, p. 338.

79 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://option-consommateurs.org/wp-content/uploads/2017/06/option-consommateurs-2014-2015-gratuite-rapport.pdf>.

80 *Id.*, p. 7.

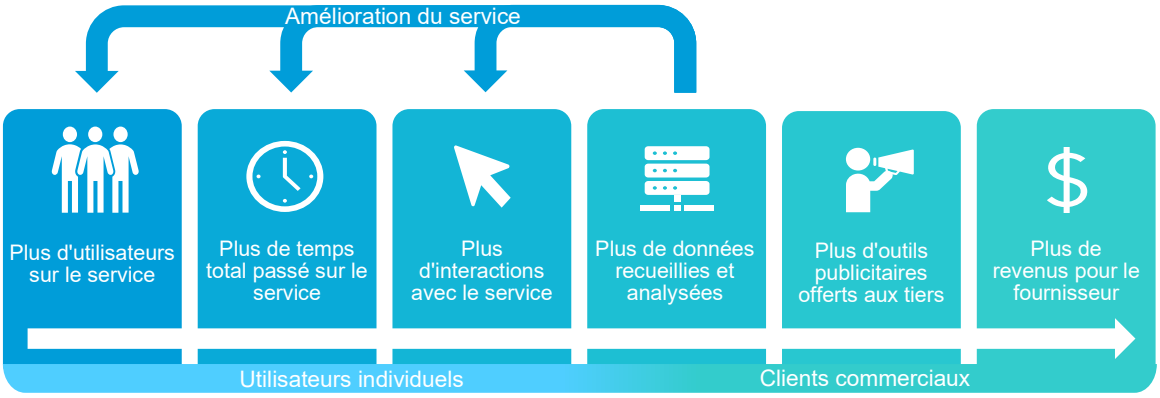
81 M. BOCK et M. WIENER, précité, note 75, p. 11.

82 Hervé LE CROSNIER, « Publicité ciblée : l'économie de l'attention », *L'observatoire mesdatasetmoi.fr* (27 mars 2017), en ligne : <https://www.mesdatasetmoi-observatoire.fr/article/l-economie-de-lattention> (consulté le 17 mars 2022).

géolocalisation, leur historique de navigation, leur profil sociodémographique, etc.[83]. C'est ce qu'on appelle la publicité ciblée ou comportementale[84].

Dans ce contexte, comme le souligne la chercheuse Giovanna Mascheroni[85], les individus sont vus comme une ressource. Ils sont d'une part des consommateurs qui demandent et obtiennent les services, et d'autre part des producteurs de données qui permettent le raffinement des publicités qui leur sont proposées.

Ces éléments contribuent à créer une économie dite « de l'attention »[86]. Il s'agit d'une chaîne de valeur qui sous-tend le modèle d'affaires des services numériques gratuits (ou très abordables). Essentiellement, ceux-ci doivent, pour obtenir du financement de la part des publicitaires, maximiser les ressources qu'ils peuvent leur offrir, soit l'attention des individus et le ciblage de cette attention, par l'entremise des données[87]. L'économie de l'attention peut être résumée par le schéma qui suit[88] :



Comme le souligne la 5Rights Foundation, « au cœur de cette chaîne de valeur se trouvent des stratégies de design persuasives qui attirent l'utilisateur sur le service et l'y gardent afin de créer davantage de données »[89]. Ces stratégies incluent par exemple[90] :

- les algorithmes de recommandation;
- la quantification de la popularité (par des boutons « J'aime » ou des mécanismes d'abonnement, par exemple);

---

83 A. PLOURDE, précité, note 79, p. 9.

84 A. PLOURDE, précité, note 79.

85 G. MASCHERONI, précité, note 49, p. 3.

86 H. LE CROSNIER, précité, note 82; Beeban KIDRON, Alexandra EVANS et Jenny AFIA, *Disrupted Childhood: The Cost of Persuasive Design*, 5Rights Foundation, 2018, p. 15-16, en ligne : <https://5rightsfoundation.com/static/5Rights-Disrupted-Childhood.pdf>.

87 REVEALING REALITY, précité, note 61, p. 24 et suivantes.

88 Voir aussi le parallèle avec le schéma du « surplus comportemental » proposé par S. ZUBOFF, précité, note 61, p. 97.

89 B. KIDRON, A. EVANS et J. AFIA, précité, note 86, p. 16, notre traduction.

90 REVEALING REALITY, précité, note 61, p. 25-30 et 35-47.

- les notifications poussées (*push notifications*)[91];
- les fonctions de réseautage avec d'autres utilisateurs;
- la réduction du nombre d'actions à poser (clics, moments de réflexion, etc.) pour accéder aux fonctionnalités qui impliquent la collecte de données[92].

L'économie de l'attention implique une forte compétition entre les différents fournisseurs : en effet, le temps d'attention des utilisateurs a une limite inhérente[93]. Les stratégies mentionnées ci-haut sont donc continuellement améliorées par les fournisseurs pour maintenir ou augmenter leurs revenus[94].

Les témoins utilisés par les tiers[95] pour recueillir des renseignements sont aussi inclus dans de plus en plus de librairies de développement (souvent proposées par de grands acteurs de l'économie numérique). Cela contribue à leur expansion, parfois contrairement aux intentions initiales des concepteurs[96]: une très forte pression s'installe en effet pour maintenir le système, comme le décrivent des concepteurs interrogés par des chercheurs britanniques[97]. Même s'ils souhaitent placer l'intérêt supérieur de l'enfant au premier plan et s'ils sont conscients de leur responsabilité sociale, ceux-ci sont souvent contraints de s'aligner aux pratiques du marché, sous peine que leurs produits et services ne soient pas rentables.

En outre, les données recueillies pour propulser la publicité peuvent ensuite resservir pour des fins qui ne sont pas encore connues. L'existence même du modèle favorise donc une certaine surveillance généralisée des mineurs et ouvre la voie à des utilisations insoupçonnées de leurs renseignements personnels, possiblement à leur détriment[98]. Déjà, des conséquences négatives émergent, comme le souligne Wojciech Wiewiórowski, contrôleur européen de la protection des données[99] :

> La publicité comportementale est un sujet de préoccupation pour les défenseurs de la protection des renseignements personnels depuis plusieurs années. C'est toutefois récemment seulement que je suis devenu douloureusement conscient de la façon dont ce modèle d'affaires mène à des préjudices sociétaux. Si Cambridge

---

91 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Grand dictionnaire terminologique - notification poussée », *Grand dictionnaire terminologique* (2014), en ligne : <https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26527127> (consulté le 17 mars 2022).

92 Voir REVEALING REALITY, précité, note 61, p. 27.

93 B. KIDRON, A. EVANS et J. AFIA, précité, note 86, p. 19.

94 REVEALING REALITY, précité, note 61, p. 24-32.

95 Ces témoins permettent à des tiers, qui ne fournissent pas de services directement au mineur, de recueillir des renseignements sur ses activités numériques au gré de sa navigation sur Internet. Voir « Cookie – Définition », *Commission nationale de l'informatique et des libertés*, en ligne : <https://www.cnil.fr/fr/definition/cookie> (consulté le 3 juin 2022).

96 A. EKAMBARANATHAN, J. ZHAO et M. VAN KLEEK, précité, note 77, p. 6 -9.

97 *Id.*, p. 6 -9.

98 COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, précité, note 39, p. 13-16; Observation générale nº 25, précité, note 11, par. 68.

99 Wojciech WIEWIÓROWSKI, « It is time to target online advertising », *European Data Protection Supervisor* (14 mars 2022), en ligne : <https://edps.europa.eu/press-publications/press-news/blog/it-time-target-online-advertising_en> (consulté le 16 mars 2022), notre traduction.

> Analytica était en train de devenir un souvenir lointain, le témoignage récent de Frances Haugen amène de nouveau à réfléchir. La polarisation politique et idéologique, la désinformation et la manipulation semblent être devenues des conséquences inhérentes de ce qu'on appelle aujourd'hui « l'économie de l'attention ».

En résumé, la collecte, l'utilisation et la communication de renseignements personnels sont au cœur des activités des services numériques dont le financement repose sur la publicité. Ce modèle est la cause ou le catalyseur de nombreux risques auxquels sont aujourd'hui exposés les mineurs dans le monde numérique. Ceux-ci sont abordés plus en détail à la section 3.3 de ce rapport.

3.2.1.3 Autres modèles d'affaires

Tous les produits et services numériques ne sont pas financés par le modèle présenté ci-haut. En fait, l'amélioration de la publicité n'est que l'une des façons d'exploiter commercialement les renseignements personnels, comme le soulignent la chercheuse Laurien Desimpelaere et ses collègues[100] :

> Les façons dont ces données peuvent être employées commercialement semblent infinies : on peut les utiliser pour raffiner des campagnes de publicité en créant des messages promotionnels qui sont plus susceptibles d'intéresser les utilisateurs ou pour améliorer l'expérience des clients de façon à ce que les produits et services satisfassent leurs attentes, ou encore les vendre en grandes quantités à d'autres entreprises pour en tirer du profit, entre autres.

Cette vision permet de comprendre les enjeux de protection des renseignements personnels qui se posent aussi avec des modèles d'affaires plus « classiques », tels que ceux qui reposent sur la vente directe de produits physiques ou virtuels, comme des objets connectés ou des logiciels.

Une analyse de l'organisme Option consommateurs montre par exemple que les jouets connectés proposés aux mineurs canadiens sont dotés de capteurs avancés qui leur permettent de recueillir une multitude de renseignements personnels[101]. Ceux-ci peuvent certes servir à fournir le service à l'utilisateur, mais grâce aux capacités de connectivité de ces objets, les données peuvent ensuite être transmises au fournisseur ou, éventuellement, à des partenaires[102]. Par ailleurs, les applications s'adressant aux enfants sont aussi parmi celles qui comptent le plus de témoins tiers[103].

---

[100] L. DESIMPELAERE, L. HUDDERS et D. V. de SOMPEL, précité, note 76, p. 164, notre traduction.

[101] V. MONTCALM, A. PLOURDE et E. THÉRIAULT, précité, note 57.

[102] *Id.*, p. 27 -28.

[103] Reuben BINNS, Ulrik LYNGS, Max VAN KLEEK, Jun ZHAO, Timothy LIBERT et Nigel SHADBOLT, *Third Party Tracking in the Mobile Ecosystem*, *Proceedings of the 10th ACM Conference on Web Science*, Amsterdam Netherlands, ACM, WebSci '18: 10th ACM Conference on Web Science, 15 mai 2018, p. 23-31, p. 6, DOI : 10.1145/3201064.3201089.

3.2.1.4 Pratiques problématiques

Au-delà des modèles d'affaires, en septembre 2015, la Commission a également pu constater d'elle-même un certain nombre de pratiques problématiques parmi les entreprises offrant des services numériques aux mineurs. Elle a ainsi participé à l'opération de ratissage du Global Privacy Enforcement Network au cours de laquelle 29 autorités de protection des renseignements personnels à travers 21 pays se sont intéressées aux sites Web et aux applications mobiles destinés aux mineurs ou populaires auprès d'eux[104].

La Commission s'est penchée de plus près sur 37 sites et applications mobiles principalement administrés au Québec. L'analyse a soulevé des inquiétudes quant au traitement des renseignements personnels des enfants, malgré certaines bonnes pratiques qui ont pu être observées. Cette opération de ratissage a entre autres permis de faire les constats suivants :

- 41 % des sites vérifiés recueillent des renseignements personnels auprès des mineurs;
- Seulement 35 % des sites ont mis en place des contrôles efficaces pour limiter la collecte de renseignements personnels auprès des mineurs;
- 38 % des sites offrent la possibilité aux mineurs d'être redirigés vers un autre site Web;
- Seulement 19 % des sites encouragent une implication des parents;
- 62 % des sites n'offrent pas de moyen simple pour supprimer les renseignements du compte.

3.2.2 Mineurs

Dans les relations commerciales impliquant des renseignements personnels de mineurs, les mineurs eux-mêmes sont les personnes concernées : leurs droits sont en cause. Bien que l'environnement numérique n'ait pas été conçu pour eux à l'origine[105], il occupe aujourd'hui une place prépondérante dans la vie des quelque 1 600 000[106] jeunes Québécoises et Québécois. Ils y font des découvertes, ils y jouent, ils y socialisent, ils y apprennent, et ils y développent une part fondamentale de leur identité. Les pages suivantes donnent un aperçu de leurs comportements et de leurs attitudes par rapport à cet espace.

---

[104] « Les renseignements personnels des enfants et Internet », *Commission d'accès à l'information* (17 septembre 2015), en ligne : <https://www.cai.gouv.qc.ca/les-renseignements-personnels-des-enfants-et-internet/> (consulté le 26 janvier 2022).

[105] Observation générale nº 25, précité, note 11, par. 12.

[106] Estimations de 2020 pour les moins de 18 ans. « Démographie : la population du Québec et les familles », *Ministère de la Famille du Québec* (12 février 2021), en ligne : <https://www.mfa.gouv.qc.ca/fr/Famille/chiffres-famille-quebec/chiffres-famille/Pages/demographie-population-familles.aspx> (consulté le 17 mars 2022).

3.2.2.1 Comportements et habitudes

Curieux et enthousiastes, les mineurs sont bien souvent les pionniers dans l'utilisation des nouvelles technologies, avant même que celles-ci aient fait l'objet d'un examen approfondi de la part des adultes[107]. Ils sont donc parmi les premiers à être exposés aux risques du numérique.

Selon les tout derniers chiffres de l'Académie de la transformation numérique[108], la quasi-totalité (98 %) des jeunes Québécoises et Québécois de 6 à 17 ans utilise des appareils électroniques. Même avant l'entrée au primaire, une bonne partie des enfants interagissent avec ceux-ci, selon des données américaines colligées par le Pew Research Center en 2020[109]. La plupart de ces appareils appartiennent aux enfants eux-mêmes : ordinateurs, tablettes, consoles de jeux et téléphones intelligents sont les plus fréquemment possédés[110].

Parmi les activités numériques populaires auxquelles s'adonnent les mineurs, on retrouve surtout[111] :

- le visionnement de vidéos (sur des sites de partage ou sur des plateformes de visionnement à la demande);
- le jeu vidéo;
- la socialisation (réseaux sociaux, applications de messagerie et de visioconférence, etc.);
- la réalisation d'activités scolaires;
- l'écoute de musique.

À titre d'exemple, 40 % des jeunes Québécoises et Québécois de 6 à 12 ans avaient un compte sur un réseau social en 2021, une proportion qui grimpait à 83 % chez les 13 à 17 ans[112] (un an plus tôt, ces chiffres étaient de 26 % et de 78 % respectivement[113]).

Collectivement, les activités mentionnées ci-haut font en sorte que 42 % des jeunes Québécoises et Québécois passaient plus de 10 heures par semaine sur Internet en

---

107 S. LIVINGSTONE, M. STOILOVA et R. NANDAGIRI, précité, note 42, p. 6, p. 6.

108 ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE, *La famille numérique (2021)*, 2022, en ligne : <https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/2022-03-la-famille-numerique>.

109 Brooke AUXIER, Monica ANDERSON, Andrew PERRIN et Erica TURNER, *Parenting Children in the Age of Screens*, Pew Research Center, 2020, p. 13, en ligne : <https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2020/07/PI_2020.07.28_kids-and-screens_FINAL.pdf>.

110 ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE, précité, note 108; Kara BRISSON-BOIVIN, *Le bien-être numérique des familles canadiennes*, Ottawa, HabiloMédias, 2018, p. 20, en ligne : <https://habilomedias.ca/sites/mediasmarts/files/publication-report/full/numerique-familles-canadiennes.pdf>.

111 ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE, précité, note 108, p. 10; K. BRISSON-BOIVIN, précité, note 110, p. 25 -33.

112 ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE, précité, note 108, p. 12, p. 12.

113 *Id.*, p. 14, p. 14.

2021[114]. En 2018, une étude d'HabiloMédias révélait que la plupart des soirs de la semaine, 47 % des jeunes de 15 ans et moins au Canada utilisaient la technologie numérique durant l'heure précédant le coucher et 30 % après s'être couchés pour la nuit[115]. Toutes ces estimations sont fournies par les parents, avec les limites que cela comporte[116]; une étude menée récemment auprès d'adolescents montréalais confirme toutefois que le temps d'écran de 70 % d'entre eux a beaucoup augmenté pendant les deux dernières années en raison de la pandémie de COVID-19[117].

3.2.2.2 Attitudes et connaissances

Les attitudes des mineurs envers le numérique et la vie privée et les connaissances qu'ils en ont font partie des éléments qui les rendent vulnérables. Ils sont de grands utilisateurs du numérique, mais n'en connaissent pas bien les rouages et n'en perçoivent pas tous les risques.

3.2.2.2.1 Valeurs et pratiques

Les études consultées montrent que les mineurs se soucient bel et bien de leur vie privée et agissent pour la protéger[118], contrairement à l'idée du *paradoxe de la vie privée* (voir section 2.3)[119]. Leur capacité à expérimenter et à faire des erreurs sans que celles-ci les suivent ou sans faire l'objet de jugements trop durs est notamment une préoccupation importante[121]. Afin de préserver cette capacité et leur vie privée, ils déploient

> ***« Évidemment, on peut changer comme personne, et tout le monde a déjà publié ou commenté quelque chose en ligne dont il n'est pas fier ou même envoyé un message privé à quelqu'un ou sauvegardé une publication. Je pense que c'est un peu une sorte de violation de la vie privée à ce moment-là. »***
>
> **(Andrew, 16 ans)[120]**

[114] *Id.*, p. 5, p. 14.

[115] K. BRISSON-BOIVIN, précité, note 110, p. 22-23, p. 22-23.

[116] Une enquête française menée en 2020 pour le compte de la CNIL a montré que les parents sous-estimaient la fréquence des comportements numériques de leurs enfants. INSTITUT FRANÇAIS D'OPINION PUBLIQUE, *Les comportements digitaux des enfants - Regards croisés parents et enfants*, Commission nationale de l'informatique et des libertés, 2020, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/sondage_ifop_-_comportements_digitaux_des_enfants_-_fevrier_2020.pdf>.

[117] Frédérik-Xavier DUHAMEL, « Plus de temps d'écran pour les adolescents, dont beaucoup sont tannés », *La Presse* (18 mai 2022), en ligne : <https://www.lapresse.ca/actualites/2022-05-18/plus-de-temps-d-ecran-pour-les-adolescents-dont-beaucoup-sont-tannes.php> (consulté le 25 mai 2022).

[118] M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39, p. 17-18; REVEALING REALITY, *Towards a better digital future – Informing the Age Appropriate Design Code*, Information Commissioner's Office, 2019, p. 9-12, en ligne : <https://ico.org.uk/media/about-the-ico/consultations/2614763/ico-rr-report-0703.pdf>.

[119] S. MCALEESE, M. JOHNSON et M. LADOUCEUR, précité, note 41, p. 6; K. BRISSON-BOIVIN et S. MCALEESE, précité, note 63, p. 16-17.

[120] S. MCALEESE, M. JOHNSON et M. LADOUCEUR, précité, note 41, p. 14; cette citation d'Andrew, qui s'exprime ainsi après avoir appris dans une vidéo informationnelle que des renseignements personnels pouvaient être partagés à de futurs employeurs et influencer les chances d'embauche, est reproduite intégralement avec la permission d'HabiloMédias.

[121] M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39, p. 18.

différentes stratégies qui impliquent un contrôle sur la circulation de leurs renseignements personnels[122], comme :

- fournir de fausses informations dans les formulaires (faux nom, fausse adresse, etc.);
- s'abstenir de communiquer des renseignements à certaines personnes ou dans certains contextes;
- altérer les images qu'ils partagent;
- choisir des canaux de communication différents en fonction de leurs paramètres de confidentialité.

> *« J'avais l'habitude de ne pas publier beaucoup parce que j'ai beaucoup d'abonnés sur mon compte Instagram. J'ai commencé à penser : ça c'est pas assez bon pour ce public; j'ai alors créé un deuxième compte, j'ai enlevé tous mes utilisateurs normaux d'Instagram et j'ai ensuite opté pour le mode privé. Les personnes sur ce compte étaient proches de moi; je me permettais donc de publier ce que je voulais; puis, sur mon compte principal, je publiais juste ce que je me sentais à l'aise de partager avec beaucoup de gens. »*
>
> **(Pavlina, 14 ans)** [123]

À propos du souci de la vie privée des mineurs et des stratégies mises en place pour la protéger, la chercheuse Valerie Steeves observe que les valeurs et les pratiques des mineurs ne s'alignent que rarement avec les pratiques commerciales des plateformes qu'ils utilisent[124] :

> […] Mais les jeunes n'assimilent pas la non-divulgation [à] la vie privée. [À la place], ils cherchent vie privée et [publicité] à la fois, en publiant de l'information, puis en cherchant à contrôler qui peut y accéder. Ils adoptent aussi un ensemble complexe de normes sociales qui établissent ce que certaines personnes devraient – et ne devraient pas – voir.
>
> De ce point de vue, afficher quelque chose en ligne n'est pas la même chose que consentir à sa collecte. Contrairement au modèle commercial à l'origine des sites Web que les élèves utilisent, 83 % des jeunes que nous avons interrogés nous ont

---

122 *Id.*, p. 18-19; L. DESIMPELAERE, L. HUDDERS et D. V. de SOMPEL, précité, note 76, p. 167; Matthew JOHNSON, Valerie STEEVES, Leslie Regan SHADE et Grace FORAN, *Partager ou ne pas partager : Comment les adolescents prennent des décisions en matière de vie privée à propos des photos sur les réseaux sociaux*, HabiloMédias, 2017, en ligne : <https://habilomedias.ca/sites/mediasmarts/files/publication-report/full/partager-ou-ne-pas-partager.pdf>.

123 M. JOHNSON, V. STEEVES, L. R. SHADE et G. FORAN, précité, note 122, p. 30; cette citation est reproduite intégralement avec la permission d'HabiloMédias.

124 Valerie STEEVES, *Jeunes Canadiens dans un monde branché, Phase III : Tendances et recommandations*, Ottawa, HabiloMédias, 2015, p. 14-15, en ligne : <https://habilomedias.ca/sites/mediasmarts/files/publication-report/full/jcmbiii_tendances_recommandations_rapport.pdf>.

dit que l'entreprise qui administre le site *ne devrait pas pouvoir* voir ce qu'ils y affichent et 95 % estimaient que les spécialistes du marketing ne devraient pas plus y avoir accès. Les chiffres sont encore plus bas en ce qui concerne la possibilité que les entreprises et les spécialistes du marketing puissent suivre leurs déplacements grâce aux GPS intégrés dans les appareils électroniques qu'ils ont sur eux.

Si certains comportements numériques des mineurs peuvent faire croire qu'ils ne se préoccupent pas de leur vie privée, certains rappellent que les enfants et les adolescents ont des besoins particuliers en matière de socialisation et de construction identitaire qui expliquent en partie leurs pratiques et leurs valeurs[125]. Il faut par exemple noter que les mineurs déclarent souvent que malgré leurs préoccupations liées à la protection des renseignements personnels, ils craignent d'être exclus socialement s'ils choisissent de ne pas utiliser les produits et services numériques populaires chez leurs pairs[126].

Enfin, les mineurs se disent pour plusieurs ouverts à fournir certains renseignements en retour de services qui leur bénéficient directement[127]. Cependant, comme le rappelle l'organisme britannique Revealing Reality, ils expriment ce point de vue sans être « nécessairement au courant de quelles données ils partagent et de la façon dont elles sont utilisées […], particulièrement quand il s'agit de partage moins direct, comme par l'utilisation de témoins de connexion ou de données de navigation. »[128] Cette attitude pourrait aussi refléter une certaine résignation face au principe « utilisateur-payeur » (en renseignements personnels) qui sous-tend une bonne partie de l'environnement numérique[129].

3.2.2.2.2 Compréhension des concepts

Entre autres en raison du manque de transparence des pratiques des entreprises, les mineurs ont une littératie numérique plutôt limitée : leur compréhension de l'écosystème numérique et de ses impacts sur leurs droits est partielle, quoiqu'ils soient de grands utilisateurs des nouvelles technologies. Les informations fournies dans les politiques de confidentialité ou les conditions d'utilisation ne leur servent d'ailleurs pas à y voir plus clair, puisqu'ils ne les lisent que rarement ou

> *« Je les ouvre, je les défile jusqu'en bas de la page et je clique sur "J'accepte". Il y a 13 pages! Personne ne veut lire 13 pages de jargon juridique. »*
>
> **(Natasha, 15 ans)** [130]

[125] M. Mačėnaitė, précité, note 71, p. 344-346 du chapitre.

[126] Revealing Reality, précité, note 118, p. 9; M. Johnson, V. Steeves, L. R. Shade et G. Foran, précité, note 122, p. 26.

[127] Revealing Reality, précité, note 118, p. 9-12, p. 9-12.

[128] *Id.*, p. 11, notre traduction.

[129] K. Brisson-Boivin et S. McAleese, précité, note 63, p. 17, p. 17.

[130] S. McAleese, M. Johnson et M. Ladouceur, précité, note 41, p. 12; cette citation de Natasha est reproduite intégralement avec la permission d'HabiloMédias.

ne sont pas confiants de leur capacité à les lire[131] – en effet, elles sont souvent peu adaptées à eux.

« Les enfants ne voient souvent pas que leurs activités en ligne génèrent des données et les font circuler au-delà du cercle social auquel elles sont destinées »[132] : s'ils sont au fait de certains processus de collecte de renseignements à leur sujet, ils ne prennent généralement pas conscience de l'ampleur de leur empreinte numérique.

De fait, l'une de leurs préoccupations prédominantes est la divulgation d'informations *à d'autres personnes*. Cela révèle une vision d'abord interpersonnelle de la vie privée, suivant la typologie présentée dans la section 2.3 de ce rapport. Ses dimensions institutionnelle et commerciale leur sont donc moins familières, et ils en ont une compréhension moins raffinée[133]. De la même façon, ils sont surtout conscients des renseignements qu'ils fournissent, et non de ceux qui sont observés ou inférés[134].

Dès lors, les mineurs sont tentés d'étendre leur compréhension interpersonnelle des concepts au contexte commercial, ce qui génère des incohérences. Par exemple, ils visualisent souvent les entreprises comme des individus ou les associent aux individus qui y travaillent (« le gars chez Facebook »), ne parvenant pas à déceler leurs intérêts à titre de personnes morales[135]. Cette confusion les conduit à anticiper certaines normes de traitement des renseignements personnels, qui s'alignent rarement avec la réalité[136], comme le fait pour une plateforme numérique de ne plus utiliser leurs informations s'ils rendent leur compte privé[137].

Par ailleurs, les mineurs éprouvent de la difficulté à comprendre certains concepts clés, comme la circulation accrue de leurs renseignements personnels, leur caractère permanent et la pluralité des acteurs y ayant accès[138]. Ils sont aussi peu familiers avec certaines technologies ou pratiques courantes, comme les témoins de connexion[139] ou le profilage[140]. Des problèmes terminologiques se posent parfois. Par exemple, les témoins étant appelés *cookies* (« biscuits ») en anglais, ils peuvent être perçus comme

---

131 REVEALING REALITY, précité, note 118, p. 55, p. 55; K. BRISSON-BOIVIN, précité, note 110, p. 38-42; S. LIVINGSTONE, M. STOILOVA et R. NANDAGIRI, précité, note 42, p. 29; S. MCALEESE, M. JOHNSON et M. LADOUCEUR, précité, note 41, p. 12-13.

132 M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39, p. 20, notre traduction.

133 *Id.*, p. 21-22; Jun ZHAO, Ge WANG, Carys DALLY, Petr SLOVAK, Julian EDBROOKE-CHILDS, Max VAN KLEEK et Nigel SHADBOLT, *« I make up a silly name »: Understanding Children's Perception of Privacy Risks Online*, *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, Glasgow Scotland Uk, ACM, CHI '19: CHI Conference on Human Factors in Computing Systems, 2 mai 2019, p. 1-13, DOI : 10.1145/3290605.3300336.

134 M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39, p. 21-22, p. 21-22.

135 L. DESIMPELAERE, L. HUDDERS et D. V. de SOMPEL, précité, note 76, p. 167, p. 167.

136 M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39, p. 21 -22.

137 S. MCALEESE, M. JOHNSON et M. LADOUCEUR, précité, note 41, p. 2.

138 M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39, p. 26-28; S. LIVINGSTONE, M. STOILOVA et R. NANDAGIRI, précité, note 42, p. 20.

139 L. DESIMPELAERE, L. HUDDERS et D. V. de SOMPEL, précité, note 76, p. 168.

140 REVEALING REALITY, précité, note 118, p. 22.

« mignons »[141]. En raison des disparités entre leurs attentes de nature interpersonnelle et la réalité d'une relation commerciale, les mineurs peuvent aussi ressentir de la confusion face à des termes comme « consentement » (obligatoire), « suppression » (de données) ou « privé »[143].

> *« Je cherche quelque chose et c'est presque comme si [les algorithmes] me traquent. Ou, on parle de quelque chose au téléphone, et ensuite une publicité apparaît et c'est à se demander… [les algorithmes] écoutent-ils nos conversations? C'est assez troublant. »*
>
> **(Nicole, 14 ans)** [142]

Bien qu'ils aient conscience de certaines pratiques commerciales, comme la publicité, les mineurs peinent parfois à envisager la valeur associée à leurs renseignements personnels. Plusieurs soulignent par exemple qu'ils ne sont après tout qu'un utilisateur parmi des millions, et qu'ils ne voient pas pourquoi une entreprise s'intéresserait à eux en particulier, ou que leurs activités sont tout à fait banales et qu'ils n'ont rien à cacher[144]. Ils ne décèlent pas toujours la nature d'un renseignement personnel lorsque celui-ci n'est pas clairement identificatoire (par ex. un jouet préféré, par rapport à une adresse physique)[145]. Leur compréhension des modèles d'affaires qui sous-tendent les services qu'ils utilisent est limitée[146]. Enfin, les mineurs ont généralement un fort sens moral, ce qui les amène à catégoriser les pratiques ou les acteurs comme « bons » ou « mauvais ». Ils ont tendance à présumer de la bonne foi des entreprises[147].

Tout cela ne les empêche pas de ressentir un inconfort avec certains scénarios de partage et d'utilisation de renseignements personnels lorsqu'on les leur présente en détail. Pendant des discussions sur les algorithmes, le profilage, la vente de renseignements personnels, la géolocalisation ou la publicité ciblée, par exemple, les mineurs qualifient souvent ces pratiques de « troublantes » (*creepy* en anglais) ou de « bizarres », ou les jugent dérangeantes[149]. Certains

> *On finit par en avoir assez de voir le même contenu; c'est comme si l'algorithme était en mode : « Oh, tu aimes ça? Tiens, voilà toutes les informations sur le sujet! »*
>
> **(Conor, 15 ans)** [148]

---

[141] 5RIGHTS FOUNDATION, *Tick to Agree - Age appropriate presentation of published terms*, 2021, p. 10, en ligne : <https://5rightsfoundation.com/TicktoAgree-Age_appropriate_presentation_of_published_terms.pdf>.

[142] K. BRISSON-BOIVIN et S. MCALEESE, précité, note 63, p. 18; cette citation de Nicole est reproduite intégralement avec la permission d'HabiloMédias.

[143] M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39, p. 23, p. 23.

[144] *Id.*, p. 22-25; REVEALING REALITY, précité, note 118, p. 25, p. 25.

[145] REVEALING REALITY, précité, note 118, p. 25.

[146] M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39, p. 23, p. 23.

[147] *Id.*, p. 24.

[148] K. BRISSON-BOIVIN et S. MCALEESE, précité, note 63, p. 34; cette citation de Conor est reproduite intégralement avec la permission d'HabiloMédias.

[149] *Id.*, p. 18; M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39, p. 41; L. DESIMPELAERE, L. HUDDERS et D. V. de SOMPEL, précité, note 76, p. 168; DATA PROTECTION COMMISSION, *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing*, 2021, p. 56, en ligne :

reconnaissent toutefois qu'elles comportent parfois des avantages, comme le fait de voir des publicités plus pertinentes ou de découvrir de nouvelles choses.

> *« [La précision algorithmique] a ce caractère flippant où il [l'algorithme] sait tout de nous, mais de l'autre côté, ils [les algorithmes] nous aident d'une certaine manière… en nous recommandant des choses. »*
>
> **(Erin, 17 ans)** [150]

Enfin, même si la compréhension de l'écosystème numérique progresse avec l'âge, les adolescents n'en ont pas non plus une vision parfaitement éclairée. Comme le résument les chercheuses Mariya Stoilova, Sonia Livingstone et Rishita Nandagiri : « nous avons rencontré des enfants de 11 ans bien informés et des adolescents de 16 ans confus – la compréhension dépend de plusieurs facteurs au-delà de l'âge »[151].

3.2.2.2.3 Perception du risque

De façon cohérente avec leur vision surtout interpersonnelle de la vie privée, la plupart des mineurs perçoivent essentiellement les risques du numérique dans la seule sphère de la sécurité en ligne (*e-safety* en anglais). Cette vision pourrait découler notamment d'un discours public et d'un cursus scolaire plutôt axés sur protection contre les individus malveillants[152]. Les mineurs redoutent ainsi la cyberintimidation, la prédation sexuelle, le cyberharcèlement ou le piratage[153], qui peuvent avoir des conséquences sur leur sécurité, leur réputation ou leur dignité. Ils se soucient aussi de ne pas être toujours suivis par leurs parents[154].

Les mineurs se concentrent davantage sur les *bénéfices* associés au partage de renseignements personnels dans l'environnement numérique (comme la socialisation ou le divertissement) que sur les *risques* que celui-ci comporte[155]. Lorsqu'ils réfléchissent à ces risques, ils envisagent surtout ceux qui sont interpersonnels et qui sont immédiats[156]. Les problèmes qui peuvent se poser à (très) long terme, comme d'éventuelles difficultés d'accéder à un emploi, des impacts sur les primes d'assurance ou le vol d'identité, les préoccupent généralement peu[157]. Les mineurs arrivent notamment difficilement à

<https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf>.

150 K. Brisson-Boivin et S. McAleese, précité, note 63, p. 45; cette citation d'Erin est reproduite intégralement avec la permission d'HabiloMédias.

151 M. Stoilova, S. Livingstone et R. Nandagiri, précité, note 39, p. 28-29, notre traduction.

152 V. Steeves, précité, note 10; M. Stoilova, S. Livingstone et R. Nandagiri, précité, note 39, p. 19-20; Revealing Reality, précité, note 118, p. 12.

153 M. Stoilova, S. Livingstone et R. Nandagiri, précité, note 39, p. 19-20; L. Desimpelaere, L. Hudders et D. V. de Sompel, précité, note 76, p. 168.

154 S. Livingstone, M. Stoilova et R. Nandagiri, précité, note 42, p. 15.

155 M. Stoilova, S. Livingstone et R. Nandagiri, précité, note 39, p. 19 -20.

156 Commissaire à l'enfance du Royaume-Uni, précité, note 39, p. 3, 9-16, p. 3, 9-16.

157 M. Stoilova, S. Livingstone et R. Nandagiri, précité, note 39, p. 21; M. Mačėnaitė, précité, note 71, p. 347.

imaginer les conséquences négatives des décisions automatisées, puisqu'elles n'impliquent pas d'individus[158].

3.2.3 Parents

Les adultes sont responsables des mineurs et sont appelés à jouer un rôle important dans la protection de leurs renseignements personnels. Pour des fins de simplicité, à travers ce rapport, la Commission les désigne par le terme « parents », qu'ils soient titulaires de l'autorité parentale ou tuteurs par rapport aux mineurs.

À bien des égards, il ressort de la documentation consultée que les parents font eux aussi face à d'importants défis en matière de protection des renseignements personnels en ligne. La Commission remarque qu'ils ne sont peut-être pas toujours bien outillés pour aider leurs enfants à protéger les renseignements personnels.

3.2.3.1 Comportements et habitudes

Tout comme les mineurs, les parents sont désormais de grands utilisateurs du numérique. Le dernier *Portrait numérique des foyers québécois* de l'Académie de la transformation numérique[159] révèle notamment les tendances suivantes chez les 18 à 54 ans, les plus susceptibles d'être parents de mineurs :

- Environ 95 % de ces adultes utilisent Internet au quotidien;
- Une très forte majorité d'entre eux possèdent un téléphone intelligent (dans une proportion qui atteint même 100 % chez les 18-34 ans) *et* un ordinateur;
- Plus de la moitié possèdent également une télévision intelligente et une console de jeu vidéo, dans une proportion qui décroît toutefois avec l'âge;
- Environ 70 % passent plus de temps devant les écrans qu'en 2020 (une proportion qui chute à 53 % chez les 45-54 ans);
- Les activités en ligne les plus communes sont celles liées à l'information et à la communication, au divertissement/loisirs et au magasinage.

Certaines habitudes numériques des parents peuvent se révéler problématiques pour les mineurs. Par exemple, on voit depuis plusieurs années se dessiner une tendance au surpartage parental (*sharenting* en anglais) sur les réseaux sociaux, qui conduit les parents à diffuser une grande quantité de renseignements personnels au sujet de leurs enfants : photos, récits de mésaventures, commentaires, vidéos de performances sportives, etc.[160]. Un peu plus de la moitié des parents interrogés dans une enquête

---

158 REVEALING REALITY, précité, note 118, p. 22 -23.

159 ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE, *Portrait numérique des foyers québécois (2021)*, 2022, en ligne : <https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/2022-01-portrait-numerique-des-foyers-quebecois>.

160 Josiane FRÉCHETTE, *Être parent à l'ère du numérique – Le partage de renseignements personnels sur les réseaux sociaux et ses conséquences sur le droit à la vie privée et à l'image des enfants*, Option consommateurs, 2019, en ligne : <https://option-consommateurs.org/wp-content/uploads/2019/09/parentalite-numerique-oc.pdf>.

qualitative d'Option consommateurs menée en 2019 indiquaient publier des renseignements personnels au sujet de leur enfant sur les réseaux sociaux[161].

Ce partage, qui n'est généralement pas fait avec de mauvaises intentions, mais plutôt aux fins de maintenir des liens sociaux significatifs ou d'exprimer de la fierté[162], débute souvent avant même la naissance des enfants[163]. En 2018, une étude qualitative menée dans 21 pays européens a établi que la majorité des enfants acquéraient ainsi une empreinte numérique avant l'âge de 2 ans en raison des activités numériques de leurs parents[164].

Même hors des réseaux sociaux, certains travaux soulignent aussi la possibilité que l'utilisation de toutes sortes d'applications pour téléphones intelligents par les parents (ex. suivi du développement de l'enfant, suivi de grossesse, embauche de gardiens d'enfants) mène, plus ou moins à leur insu, à la collecte et à la circulation accrue des renseignements personnels de leurs enfants[165].

L'une et l'autre de ces tendances pourraient avoir des conséquences à long terme sur les mineurs, sans même que ceux-ci n'en soient nécessairement informés[166]. Par exemple, les entreprises se réservent généralement le droit d'utiliser les renseignements personnels publiés sur leurs plateformes à des fins très larges[167].

3.2.3.2 Attitudes et connaissances

En plus d'être des utilisateurs du numérique eux-mêmes, les parents ont un rôle d'accompagnateurs à jouer auprès de leurs enfants par rapport aux technologies. Leurs valeurs et leurs pratiques, leur littératie numérique et leur vision du risque ont donc un impact important sur leur façon d'assumer cette responsabilité.

3.2.3.2.1 Valeurs et pratiques

Les parents peuvent avoir une attitude favorable à la technologie, ou se montrer plus sceptiques. Ils conviennent toutefois en général « qu'il est impossible (et non souhaitable) d'éviter l'utilisation de la technologie dans la vie de leurs enfants, tant à l'école qu'à la

---

161 *Id.*, p. 17.

162 *Id.*

163 Sheila DONOVAN, « 'Sharenting': The Forgotten Children of the GDPR », (2020) 4-03/2020 *Peace Human Rights Governance* 35-59, DOI : 10.14658/pupj-phrg-2020-1-2; voir aussi J. FRÉCHETTE, précité, note 160, p. 17 -18.

164 Stephane CHAUDRON, Rosanna DI GIOIA et Monica GEMO, *Young children (0-8) and digital technology: a qualitative study across Europe.*, European Commission – Joint Research Centre, Luxembourg, Publications Office, 2018, en ligne : <https://data.europa.eu/doi/10.2760/294383> (consulté le 25 mars 2022).

165 Suzanne PRIOR et Natalie COULL, *Parents Unwittingly Leak Their Children's Data: A GDPR Time Bomb?*, Abbas MOALLEM (dir.), *HCI for Cybersecurity, Privacy and Trust*, coll. Lecture Notes in Computer Science, Cham, Springer International Publishing, 2020, p. 471-486, DOI : 10.1007/978-3-030-50309-3_31.

166 COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, précité, note 39.

167 J. FRÉCHETTE, précité, note 160, p. 12-13.

maison »[168]. Malgré cela, plusieurs études constatent une tendance des parents à limiter l'accès à la technologie, et donc à être plus restrictifs que permissifs[169], bien que les stratégies varient d'un parent à l'autre – notamment en fonction de leur degré de littératie numérique[170]. L'encadrement offert varie avec l'âge, prenant graduellement moins de place au fur et à mesure que les enfants grandissent[171].

Même si les parents affichent un désir clair d'épauler leurs enfants pour la gestion de leur vie privée en ligne, ils sont souvent pris au dépourvu : ils jugent qu'ils ont peu de contrôle en matière de protection des renseignements personnels[172], se sentent mal préparés pour aider leurs enfants[173] et doutent d'avoir le temps de faire les vérifications qui s'imposent[174]. Lorsqu'ils mettent en place des stratégies, elles visent surtout les pratiques explicites de collecte de renseignements (c'est-à-dire les renseignements *fournis*)[175].

Les parents ont souvent relativement confiance dans les pratiques de protection des renseignements personnels des écoles ou des organisations gouvernementales, mais sont généralement plus méfiants envers les entreprises[176]. Ils se montrent notamment critiques des modèles d'affaires qui peuvent nuire aux droits des enfants[177].

Par exemple, leur attitude envers l'utilisation de données comportementales est surtout négative[178]. Ils s'opposent aussi à la collecte de renseignements personnels qui ne paraissent pas nécessaires à la fourniture directe du service demandé[179] et ont en majorité tendance à être mal à l'aise avec la publicité ciblée[180]. De même, insatisfaits des informations fournies aux enfants sur les services en ligne, les parents « ne [mâchent] pas leurs mots quant à la nécessité de créer des modalités et conditions d'utilisation claires, concises et *compréhensibles* pour les appareils numériques, les applications, les plateformes de réseaux sociaux et les services en ligne »[181]. Ils voient ainsi d'un bon œil des stratégies visant à présenter l'information de façon claire et au moment où elle est

---

168 S. CHAUDRON, R. DI GIOIA et M. GEMO, précité, note 164, p. 44-45, notre traduction; à ce sujet, voir aussi K. BRISSON-BOIVIN, précité, note 110, p. 65.

169 S. CHAUDRON, R. DI GIOIA et M. GEMO, précité, note 164, p. 45-46; L. DESIMPELAERE, L. HUDDERS et D. V. de SOMPEL, précité, note 76 p. 170-171; K. BRISSON-BOIVIN, précité, note 110, p. 65.

170 M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39, p. 33 -34.

171 *Id.*

172 L. DESIMPELAERE, L. HUDDERS et D. V. de SOMPEL, précité, note 76, p. 169-170.

173 M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39, p. 33 -34.

174 S. LIVINGSTONE, M. STOILOVA et R. NANDAGIRI, précité, note 42, p. 33.

175 L. DESIMPELAERE, L. HUDDERS et D. V. de SOMPEL, précité, note 76, p. 168; S. LIVINGSTONE, M. STOILOVA et R. NANDAGIRI, précité, note 42, p. 33.

176 M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39, p. 33-34; V. MONTCALM, A. PLOURDE et E. THÉRIAULT, précité, note 57, p. 34.

177 M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39, p. 33-34.

178 L. DESIMPELAERE, L. HUDDERS et D. V. de SOMPEL, précité, note 76, p. 169.

179 REVEALING REALITY, précité, note 118, p. 51.

180 *Id.*, p. 43.

181 K. BRISSON-BOIVIN, précité, note 110, p. 60.

opportune, par exemple par des alertes spécifiques apparaissant lors de la modification d'un paramètre de confidentialité[182].

3.2.3.2.2 Compréhension des concepts

Comme leurs enfants, les parents ne sont pas des lecteurs assidus des politiques de confidentialité des services numériques que leurs enfants ou eux-mêmes utilisent[183]. Ils sont d'ailleurs très peu confiants lorsque vient le temps de les consulter et de les comprendre[184]. Cela peut expliquer en partie leur sentiment d'être submergés d'informations[185] ou leur manque de connaissances quant au fonctionnement et aux implications des témoins de connexion[186], du ciblage publicitaire[187] ou des jouets connectés[188].

Ces faits témoignent d'une littératie numérique somme toute limitée sur certains aspects, surtout en ce qui concerne les pratiques commerciales des entreprises et les risques qu'elles posent[189]. Même s'ils comprennent les bases, en l'occurrence le compromis souvent demandé entre divulgation de renseignements personnels et fourniture d'un service numérique[190], 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[191]. De même, ils ont peu conscience des renseignements observés et inférés[192].

3.2.3.2.3 Perception du risque

En cohérence avec cette vision interpersonnelle et cet accent sur les renseignements fournis, les parents sont eux aussi essentiellement préoccupés par les risques immédiats et concrets du numérique pour leurs enfants[193]. Ils se concentrent beaucoup sur :

---

182 REVEALING REALITY, précité, note 118, p. 35.

183 V. MONTCALM, A. PLOURDE et E. THÉRIAULT, précité, note 57, p. 35; Karen MCCULLAGH, « The General Data Protection Regulation: A Partial Success for Children on Social Network Sites? », dans Tobias BRÄUTIGAM et Samuli MIETTINEN (dir.), *Data Protection, Privacy and European Regulation in the Digital Age*, Helsinki, Unigrafia, 2016, p. 110-139, p. 127, en ligne : <https://papers.ssrn.com/abstract=2985724>.

184 K. BRISSON-BOIVIN, précité, note 110, p. 35.

185 REVEALING REALITY, précité, note 118, p. 11-12.

186 L. DESIMPELAERE, L. HUDDERS et D. V. de SOMPEL, précité, note 76, p. 169.

187 *Id.*, p. 169.

188 V. MONTCALM, A. PLOURDE et E. THÉRIAULT, précité, note 57, p. 34 -36.

189 L. DESIMPELAERE, L. HUDDERS et D. V. de SOMPEL, précité, note 76, p. 169; S. LIVINGSTONE, M. STOILOVA et R. NANDAGIRI, précité, note 42, p. 33.

190 REVEALING REALITY, précité, note 118, p. 9; L. DESIMPELAERE, L. HUDDERS et D. V. de SOMPEL, précité, note 76, p. 169.

191 J. FRÉCHETTE, précité, note 160, p. 17.

192 L. DESIMPELAERE, L. HUDDERS et D. V. de SOMPEL, précité, note 76, p. 169.

193 REVEALING REALITY, précité, note 118, p. 60.

- les risques posés par des individus malveillants (ex. piratage, cyberharcèlement, prédation sexuelle, etc.)[194];
- les conséquences sociales du partage de renseignements personnels[195];
- les risques associés à l'exposition à du contenu inapproprié[196].

En d'autres termes, les risques à long terme et les risques commerciaux leur sont moins connus[197]. Ils manifestent néanmoins des inquiétudes par rapport au bien-être de leur enfant en lien avec l'utilisation (accrue) du numérique, que ce soit physique (vision, maux de tête, sommeil, etc.) ou psychologique (dépendance, dynamique de comparaison avec les pairs, etc.)[198].

Enfin, comme le souligne une enquête d'HabiloMédias[199], ces préoccupations sont communes, mais cohabitent avec la vision somme toute positive de la technologie mentionnée précédemment :

> **Plus de la moitié** des parents interrogés ont l'impression que moins leur enfant passe de temps avec la technologie numérique, mieux il se porte, tandis que les deux tiers des parents s'entendent pour dire que leur enfant ***bénéficie*** de la technologie numérique qu'il utilise. Ces deux points montrent l'ambivalence des parents entre les préoccupations concernant l'utilisation d'un écran (plus particulièrement le *temps* passé devant un écran) et le désir de s'assurer que leur enfant ait accès aux avantages que procure la technologie numérique.

3.3 Risques numériques pour les mineurs

L'écosystème numérique, la façon dont il est exploité par les entreprises et son utilisation par les individus exposent les mineurs à une grande variété de risques de préjudices. Cette section en présente d'abord une typologie. Elle précise ensuite le rôle de catalyseur que joue l'exploitation des renseignements personnels (collecte, utilisation, communication, conservation) dans la génération de ces risques et donne des exemples de situations problématiques pour les mineurs.

---

194 J. Fréchette, précité, note 160, p. 18-19; L. Desimpelaere, L. Hudders et D. V. de Sompel, précité, note 76, p. 169; V. Montcalm, A. Plourde et E. Thériault, précité, note 57, p. 36.

195 Revealing Reality, précité, note 118, p. 11-12.

196 S. Chaudron, R. Di Gioia et M. Gemo, précité, note 164, p. 45.

197 *Id.*, p. 46; L. Desimpelaere, L. Hudders et D. V. de Sompel, précité, note 76, p. 169; S. Livingstone, M. Stoilova et R. Nandagiri, précité, note 42, p. 33; J. Fréchette, précité, note 160, p. 20.

198 S. Chaudron, R. Di Gioia et M. Gemo, précité, note 164, p. 44-46; J. Fréchette, précité, note 160, p. 21; Revealing Reality, précité, note 118, p. 48.

199 K. Brisson-Boivin, précité, note 110, p. 6.

3.3.1 Typologie

S'il existe différentes façons de catégoriser les risques numériques, la typologie CO:RE[200] dite des « 4 C » est sans doute la plus répandue[201]. Élaborée en 2009[202] avec « 3 C » au départ, celle-ci vise à homogénéiser la présentation des risques pour guider l'élaboration de politiques. Elle permet de considérer d'autres risques que « la pornographie, le leurre et la cyberintimidation »[203], qui ont traditionnellement été au cœur des préoccupations quand il s'agit des mineurs.

3.3.1.1 Les « 4 C »

Les « C » décrivent le positionnement de l'enfant par rapport à l'environnement numérique[204] (dans tous les cas, l'enfant peut être l'initiateur ou la victime du risque[205]) :

- **Contenu :** Les risques de contenu surviennent lorsque l'enfant cherche à consulter du contenu potentiellement nuisible, ou lorsqu'il y est exposé, que le contenu provienne d'une organisation ou soit produit par un utilisateur;
- **Contact :** Les risques de contact émergent de l'interaction potentiellement préjudiciable entre l'enfant et un adulte malveillant, connu ou inconnu;
- **Conduite (ou comportement) :** Les risques de conduite ou de comportement sont le fruit des interactions potentiellement préjudiciables entre l'enfant et ses pairs, dans lesquelles l'enfant peut être l'initiateur ou la victime.

En 2021, la typologie originale en « 3 C » a été mise à jour[206]. L'inclusion du « quatrième C », soit « contrat », est le principal changement. Elle vise à rendre plus visibles les risques posés par les phénomènes de commercialisation et de mise en données qui traversent le numérique[207]. Pour bien comprendre ce qu'implique ce « C », il est utile de

---

200 « Children Online: Research and Evidence - A knowledge base on children and youth in the digital world », *CORDIS (Commission européenne)* (2020), en ligne : <https://cordis.europa.eu/project/id/871018/fr> (consulté le 29 mars 2022).

201 Elle a notamment été utilisée dans les documents suivants : OCDE, *Children in the digital environment - Revised typology of risks*, OCDE Digital Economy Papers, 302, 2021, en ligne : <https://www.oecd-ilibrary.org/science-and-technology/children-in-the-digital-environment_9b8f222e-en;jsessionid=-6yCMDDpCH2dHXQIOUo_-TiV.ip-10-240-5-51>; S. CHAUDRON, R. DI GIOIA et M. GEMO, précité, note 164; 5RIGHTS FOUNDATION, « Risky by design - Introduction », *Risky-By-Design* (2022), en ligne : <https://www.riskyby.design/introduction> (consulté le 28 février 2022); K. BRISSON-BOIVIN, précité, note 110; DIANA PAOLA ALVAREZ BAUTISTA, *Vie privée des mineurs en ligne: protection des données personnelles. Étude comparée entre le droit canadien, américain et celui de l'Union européenne*, [mémoire de maîtrise], Montréal, Université de Montréal, 2021, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/25850/Alvarez_Bautista_Diana_Paola_2021_memoire.pdf>.

202 Elisabeth STAKSRUD et Sonia LIVINGSTONE, « Children and online risk: Powerless victims or resourceful participants? », (2009) 12-3 *Information, Communication & Society* 364-387.

203 Sonia LIVINGSTONE et Mariya STOILOVA, « The 4Cs: Classifying Online Risk to Children », *CO:RE Short Report Series on Key Topics* 2021, p. 4, DOI : 10.21241/SSOAR.71817.

204 *Id.*, p. 11.

205 *Id.*, p. 4.

206 S. LIVINGSTONE et M. STOILOVA, précité, note 203.

207 *Id.*, p. 6. Voir aussi la section 3.1 de ce rapport.

reproduire au long la réflexion des chercheuses Sonia Livingstone et Mariya Stoilova au sujet de son nom (« contrat » plutôt que « commerce » ou « consommation »)[208] :

> En bref, les risques de contrat surviennent lorsque les enfants utilisent des services numériques de même que lorsqu'ils sont affectés par des transactions numériques menées par des tiers d'autres façons (par ex. par l'utilisation institutionnelle de bases de données numérisées qui incluent le profil de l'enfant, ou par le traitement algorithmique de renseignements personnels de l'enfant ou d'autres personnes liées à lui).
>
> En choisissant le nom « risques de contrat » pour cette catégorie de risques, nous notons les difficultés légales liées aux contrats impliquant des enfants, de même que le fait que les utilisateurs (de tous âges) peuvent ne pas réaliser la nature contractuelle de leur relation avec des fournisseurs de services numériques. Nous notons aussi que le contrat qui occasionne un risque peut ne pas impliquer l'enfant, mais plutôt son parent ou son école, ou même, être conclu entre un fournisseur de services et un tiers, entre autres possibilités dans l'écosystème numérique complexe. Néanmoins, dans l'ensemble, nous suggérons que l'étiquette « contrat » permet de mettre en évidence un mélange de risques contractuels, liés au marketing et au traitement de données qui méritent une attention particulière, dont la plupart, mais pas tous, sont commerciaux, et qui sont encore émergents pour plusieurs.
>
> [Références omises]

Plus brièvement, on peut résumer ce « quatrième C » ainsi :

- **Contrat :** Les risques de contrat surviennent lorsque l'enfant est partie à un contrat potentiellement nuisible ou lorsqu'il subit les effets d'un tel contrat conclu entre d'autres parties; ils peuvent aussi émerger des intérêts commerciaux des entreprises.

3.3.1.2 Tableau et cartographie des risques

Dans la typologie des « 4 C », les risques de contenu, de contact, de conduite et de contrat 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 Sonia Livingstone et Mariya Stoilova[209], qui recense également des exemples de risques pouvant être classés dans chaque cellule :

---

[208] *Id.*, p. 7-8, notre traduction.

[209] *Id.*, p. 12. 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 » (*gore*), explicite, raciste, haineuse ou extrémiste	Harcèlement, persécution, comportements haineux, surveillance excessive ou non désirée	Intimidation, communication ou activité de pairs haineuse ou hostile (ex. *trolling*, 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 néfaste)	Jeux d'argent, bulles de filtres, microciblage, interfaces truquées influant sur les croyances ou les achats
Risques transversaux	• **Violations de la vie privée** (interpersonnelle, institutionnelle, commerciale; normalisation de la surveillance[210]) • **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)			

Les exemples donnés n'offrent qu'un aperçu partiel de l'étendue des risques possibles. D'ailleurs, comme le souligne le Commissaire à l'enfance du Royaume-Uni, bon nombre de risques futurs nous sont aujourd'hui inconnus, puisqu'il est difficile de prévoir l'ampleur des nouvelles possibilités à venir et reposant sur l'exploitation des renseignements personnels[211].

Il est également important de noter que les risques peuvent être catégorisés dans plus d'une cellule à la fois[212]. En fait, ils sont de plus en plus liés.

Les fournisseurs de services numériques occupent en effet une place toute particulière dans la cartographie de ces risques. En plus d'être directement à l'origine de risques de

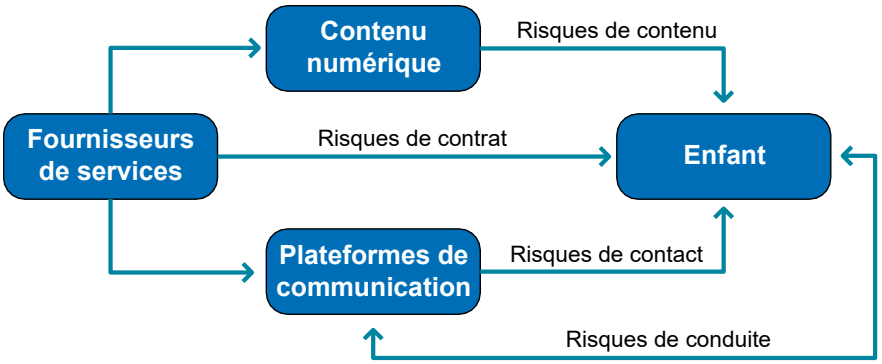
---

[210] À ce sujet, voir entre autres COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, précité, note 39, p. 12-13; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Les technologies de surveillance appliquées aux enfants », *Commissariat à la protection de la vie privée du Canada* (14 mars 2013), 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/2012/opc_201210/> (consulté le 31 janvier 2022); D. LUPTON et B. WILLIAMSON, précité, note 54.

[211] COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, précité, note 39, p. 11.

[212] DIANA PAOLA ALVAREZ BAUTISTA, précité, note 201, p. 45; S. LIVINGSTONE et M. STOILOVA, précité, note 203, p. 7, note de bas de page 9.

contrat, ils sont également des intermédiaires dans la manifestation des trois autres catégories de risques en raison de leur position dominante dans tous les aspects de la vie numérique, comme l'illustre le schéma suivant[213] :



Comme le résument Sonia Livingstone et Mariya Stoilova[214] :

> L'écosystème de données en pleine expansion fournit désormais une infrastructure non seulement pour les transactions commerciales qui affectent les enfants, mais aussi pour les produits et services numériques qui comportent des risques de contenu, de contact et de [conduite]. Le résultat est que ces types de risques sont de plus en plus interreliés, tout comme le sont les solutions – par exemple, la législation sur la protection des renseignements personnels peut prévenir certaines formes interpersonnelles ou sociales de risques numériques.
>
> [Référence omise]

Autrement dit, les entreprises gèrent les plateformes de communication utilisées par les individus. Les risques de contact et de conduite peuvent donc se matérialiser par leur entremise. De même, le contenu numérique est médiatisé par les fournisseurs, qui jouent alors un rôle dans l'émergence des risques de contenu pour les enfants.

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 numérique[215].

3.3.2 Place centrale des renseignements personnels et exemples

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

---

[213] Adapté et traduit, selon les termes de la licence CC BY 4.0 FR, de S. LIVINGSTONE et M. STOILOVA, précité, note 203, p. 7.

[214] *Id.*, p. 7, note de bas de page 9, notre traduction.

[215] 5RIGHTS FOUNDATION, précité, note 201.

universelles, leur collecte, leur utilisation, leur communication et leur conservation peuvent néanmoins ouvrir la porte aux risques figurant dans le tableau présenté à la page 38[216].

Les scénarios suivants illustrent cette situation[217]. Ils impliquent des outils techniques (de profilage, d'intelligence artificielle, etc.) et des éléments de design mis en place par les entreprises, qui peuvent mener à des violations des droits prévus à la Convention (voir section 2.1.2), indiqués en caractères soulignés. Ces scénarios sont présentés à titre informatif; leur mention n'implique pas que la Commission se prononce quant à leur conformité ou non-conformité à l'égard de la législation québécoise actuelle sur la protection des renseignements personnels, ou d'autres lois québécoises.

Scénario A

Pour renforcer l'attractivité de sa plateforme de visionnement de vidéos courtes, l'entreprise eView mise sur un algorithme de recommandation alimenté par les renseignements observés au sujet des habitudes de consommation de contenu des utilisateurs. Celui-ci infère leurs intérêts du moment et leur propose du contenu en conséquence, en tenant aussi compte des préférences des autres utilisateurs de leur pays et de leur âge. Cette situation peut présenter plusieurs risques, comme :

- **Désinformation** : Lucas, 11 ans, consulte eView tous les jours. Une publication mensongère, vue par beaucoup d'utilisateurs de profil semblable au sien, lui est proposée tout en haut de sa liste, l'incitant à la visionner. (Atteinte au droit à l'information)
- **Radicalisation** : Béatrice, 15 ans, tombe sur une vidéo qui encourage la violence. Le visionnement de ce contenu de nature radicale mène l'algorithme à inférer chez elle un intérêt pour la question et à lui proposer par la suite de plus en plus de contenus de ce type. (Atteinte au droit à la vie, à la survie et au développement)
- **Bulle de filtres** : Logan, 13 ans, regarde des vidéos de mathématiques, d'humour et de sciences, mais raffole particulièrement des vidéos de hockey. L'algorithme continue de lui proposer de plus en plus de contenus sportifs, risquant de réduire ses perspectives informationnelles et culturelles[218]. Progressivement, Logan finit par voir plus de 90 % de vidéos de hockey dans son fil. Le même phénomène pourrait être à l'œuvre sur un réseau social, par exemple[219]. (Atteinte au droit à l'information, au droit de penser librement et au droit de participer pleinement à la vie culturelle)

---

[216] À ce sujet, voir Anna JOHNSTON, « Big Tech, Individuation, and why Privacy must become the Law of Everything », *Salinger Privacy - Big Tech blog* (22 mars 2022), en ligne : <https://www.salingerprivacy.com.au/2022/03/22/big-tech-blog/?utm_source=pocket_mylist> (consulté le 31 mars 2022).

[217] Ces exemples sont pour la plupart inspirés ou adaptés des travaux de la 5Rights Foundation. Voir REVEALING REALITY, précité, note 61; 5RIGHTS FOUNDATION, précité, note 201.

[218] UNICEF et MINISTÈRE DES AFFAIRES ÉTRANGÈRES DE LA FINLANDE, précité, note 55, p. 19 -20.

[219] « Recommendation Systems », *Risky-By-Design* (février 2022), en ligne : <https://www.riskyby.design/recommendation-systems> (consulté le 31 mars 2022).

Scénario B

Le réseau social MaGang cherche à étendre son public. Il met en place un algorithme qui suggère de nouveaux amis à ses utilisateurs, en se fondant entre autres sur des renseignements personnels comme la distance entre les villes, les connaissances en commun et le profil d'intérêts. Les utilisateurs avec plus d'amis obtiennent plus de visibilité de leurs publications[220]. Cette situation peut présenter plusieurs risques, comme :

- **Leurre sexuel** : Un adulte malintentionné se bâtit un profil reflétant des intérêts populaires auprès des mineurs, puis MaGang le recommande comme ami à Emma, 14 ans, par le réseau social. Après quelques conversations, l'adulte encourage Emma à lui envoyer des photos intimes. (Atteinte au droit à la vie, à la survie et au développement)
- **Intimidation/violation de la vie privée interpersonnelle** : Une vague connaissance de Nathan, 13 ans, lui est proposée comme ami en raison de leur réseau commun. Une fois ajoutée, cette personne manifeste des comportements intimidants renforcés par les nouveaux renseignements sur Nathan auxquels elle a accès. (Atteinte au droit à la vie, à la survie et au développement et au droit à la vie privée)
- **Intégration à une communauté nuisible** : Curieuse à propos d'un mouvement prônant la minceur, Jade, 16 ans, s'abonne à quelques pages qui s'y consacrent. Elle est rapidement mise en relation avec des pairs qui ont les mêmes intérêts, puis est intégrée à des communautés valorisant la minceur extrême[221]. (Atteinte au droit à la vie, à la survie et au développement)

Scénario C

L'application de jeu Fishly, qui comporte un volet social important, souhaite susciter davantage d'engagement de la part de ses jeunes utilisateurs. Pour ce faire, ses concepteurs mettent en place un système de points virtuels qui permettent une progression plus rapide dans le jeu. Ceux-ci peuvent être achetés à un prix déterminé en fonction du profil de l'utilisateur, mais aussi obtenus d'autres manières. Par exemple, des notifications poussées incitent l'utilisateur à se connecter pour obtenir des points. De façon à être les plus efficaces possibles, ces notifications sont envoyées à des moments déterminés en fonction de ses habitudes de connexion (ex. heures, jours de la semaine, durée) et de ses partenaires de jeu. Cette situation peut présenter plusieurs risques, comme :

---

[220] « Friends Suggestions », *Risky-By-Design* (2022), en ligne : <https://www.riskyby.design/friend-suggestions> (consulté le 31 mars 2022).

[221] REVEALING REALITY, précité, note 61, p. 62.

- **Problèmes de sommeil** : Des notifications envoyées tard le soir, juste avant le coucher, incitent Mehdi, 9 ans, à prolonger indûment sa période de jeu, ce qui nuit à son sommeil. (Atteinte au droit à la vie, à la survie et au développement)
- **Anxiété** : Clara, 10 ans, accorde beaucoup d'importance à sa performance dans Fishly. Elle ressent beaucoup d'anxiété à l'idée de rater une notification, et donc l'occasion d'obtenir des points virtuels. (Atteinte au droit à la vie, à la survie et au développement)
- **Exploitation des vulnérabilités** : Le jeu utilise des données comportementales accumulées sur Mathis, 14 ans, pour modifier le prix des points virtuels qu'il lui propose d'acheter[222]. Lui qui est particulièrement actif sur Fishly se voit donc offrir un prix beaucoup moins avantageux en raison de sa susceptibilité à l'achat. (Atteinte au principe de non-discrimination et au droit de ne pas être exploité économiquement)

Scénario D

Konstella, une plateforme d'achats en ligne, transmet des renseignements personnels à plusieurs tiers dans le cadre de ses activités : gestionnaire de paiements (ex. informations de paiement), publicitaires (ex. profils d'utilisateurs, informations de contact), fournisseur de services d'analytique (ex. trafic Web, interactions avec les contenus), etc. Cette situation peut présenter plusieurs risques, comme :

- **Incident de confidentialité** : L'accroissement du nombre d'acteurs ayant accès aux renseignements personnels et l'augmentation de la circulation de ceux-ci sur des réseaux pourraient mener à un incident de confidentialité. Par exemple, un fournisseur de services de paiement néglige d'installer les correctifs de sécurité de son logiciel de gestion; des cybermalfaiteurs obtiennent l'accès à sa base de données et dérobent des renseignements concernant 250 000 mineurs. Cela les expose à d'éventuelles conséquences à long terme, comme des vols d'identité. (Atteinte au droit à la vie privée)
- **Influence du comportement/microciblage** : Les renseignements personnels fournis aux tiers leur permettent de cibler Sofia, 15 ans, avec des publicités. Ces tiers peuvent aussi chercher à influencer son comportement grâce à leurs connaissances préalables à son sujet. Cela pourrait affecter son développement. De même, ils pourraient cibler les parents de Sofia grâce aux renseignements

[222] Daniel L. KING, Paul H. DELFABBRO, Sally M. GAINSBURY, Michael DREIER, Nancy GREER et Joël BILLIEUX, « Unfair play? Video games as exploitative monetized services: An examination of game patents from a consumer protection perspective », (2019) 101 *Computers in Human Behavior* 131-143, p. 134, DOI : 10.1016/j.chb.2019.07.017.

concernant leur fille[223]. (Atteinte au droit de ne pas être exploité économiquement et atteinte au droit à la vie, à la survie et au développement[224])

- **Discrimination** : Dans quelques années, les renseignements obtenus sur Sofia par des tiers au cours de sa jeunesse pourraient nuire à ses occasions d'obtenir un emploi ou d'accéder à du crédit ou encore affecter ses primes d'assurance, par exemple, puisque le profilage est de plus en plus utilisé dans ces domaines[225]. Il existe un risque non négligeable, par ailleurs, que les renseignements concernant Sofia soient périmés ou inexacts au moment de les utiliser, étant donné que les mineurs évoluent et changent tout au long de leur enfance et de leur adolescence. (Atteinte possible au principe de non-discrimination)

Scénario E

L'application Geo-ZZ permet aux adolescents de se faire de nouveaux amis dans leur ville. Pour faciliter les rencontres, ses concepteurs créent une nouvelle fonctionnalité basée sur la proximité (telle que détectée par signal Bluetooth) : lorsqu'un jeune utilisateur se trouve à moins de 10 mètres d'un autre, tous deux reçoivent automatiquement une notification les invitant à socialiser ensemble[226]. S'ils décident de s'ajouter comme amis dans Geo-ZZ (ce qu'ils doivent valider sur le coup, lors de la première rencontre), ils peuvent ensuite avoir accès en temps réel à leur position géographique (par le GPS) de façon à pouvoir se voir plus facilement. S'ils font des activités ensemble dans les locaux de l'un des partenaires commerciaux de Geo-ZZ, qui fait affaire entre autres avec des restaurants, des cinémas et des salles de jeux, les utilisateurs peuvent recevoir des rabais instantanés sur leur téléphone. Cette situation peut présenter plusieurs risques, comme :

- **Normalisation de la surveillance** : Les utilisateurs de Geo-ZZ doivent activer la géolocalisation GPS et le Bluetooth en permanence pour que l'application fonctionne. Ce faisant, plusieurs personnes peuvent savoir en temps réel où ils se trouvent à tout moment. Ce phénomène contribue à habituer les jeunes à une surveillance permanente, effectuée par l'entreprise ou par d'autres individus. (Atteinte au droit à la vie privée et potentiellement au droit à la liberté d'association)

---

223 OPTION CONSOMMATEURS, *Projet de loi n° 64 – Loi modernisant des dispositions législatives en matière de protection des renseignements personnels - Commentaires d'Option consommateurs présentés à la Commission des institutions*, 2020, p. 11, en ligne : <https://option-consommateurs.org/wp-content/uploads/2020/09/option-consommateurs-pl64-memoire.pdf>.

224 V. STEEVES et J. BAILEY, précité, note 56.

225 COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, précité, note 39, p. 14 -16.

226 Un mécanisme semblable était exploité par de nombreuses applications de notification d'exposition développées dans le contexte de la pandémie de COVID-19. Voir AGENCE DE LA SANTÉ PUBLIQUE DU CANADA, « Alerte COVID : L'appli canadienne d'avis d'exposition à la COVID-19 » (31 juillet 2020), en ligne : <https://www.canada.ca/fr/sante-publique/services/publications/maladies-et-affections/appli-alerte-covid.html> (consulté le 10 août 2020).

- **Harcèlement sexuel/violation de la vie privée interpersonnelle** : Mya et Isaiah, 16 ans tous les deux, se rencontrent dans un café et s'ajoutent comme amis dans Geo-ZZ. Tout se passe bien au début, mais au bout de quelques semaines, Isaiah fait des avances à Mya et se fait insistant. Elle lui bloque l'accès à son compte; cependant, il a compris où et quand elle travaillait grâce à ses données de géolocalisation, et se présente plusieurs fois à la porte après la fin de ses quarts de travail pour demander à la voir. (Atteinte au droit à la vie, à la survie et au développement et au droit à la vie privée)
- **Violation de la vie privée commerciale** : Une chaîne de restauration rapide reçoit de la part de Geo-ZZ, avec qui elle est affiliée, la position des utilisateurs chaque fois que ceux-ci entrent dans un de ses établissements ou chez l'un de ses principaux concurrents[227]. Nolan, 14 ans, vient de terminer un repas chez un compétiteur; la chaîne lui envoie peu après une notification personnalisée sur son téléphone : « Il y a longtemps qu'on ne t'a pas vu! D'ici 5 jours, profite de 2 $ de rabais sur ton prochain repas chez nous! ». (Atteinte au droit de ne pas être exploité économiquement et au droit à la vie privée)

3.3.3 Probabilité et impact potentiel des préjudices

Les risques présentés ci-dessus ne sont pas purement théoriques. Certains événements des dernières années illustrent leur plausibilité :

- En 2021, la lanceuse d'alerte Frances Haugen a attiré l'attention du public et des gouvernements sur certaines pratiques de l'entreprise Meta (alors nommée Facebook)[228], qui serait au courant, grâce à des études internes, des effets néfastes de ses services sur la santé mentale des adolescents, surtout les filles : problèmes d'image, troubles du sommeil, troubles de l'alimentation, renforcement des stéréotypes de genre, etc.
- En 2021, le média d'enquête *The Markup* a diffusé une enquête sur l'application familiale Life360[229]. Celle-ci, utilisée par des millions de familles pour du partage

---

227 Voir, par exemple, COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, COMMISSION D'ACCÈS À L'INFORMATION, BUREAU DU COMMISSAIRE À L'INFORMATION ET À LA VIE PRIVÉE DE L'ABERTA, et BUREAU DU COMMISSAIRE À L'INFORMATION ET À LA VIE PRIVÉE DE LA COLOMBIE-BRITANNIQUE, *Rapport de conclusions - Enquête conjointe sur le Groupe TDL Corporation (exploitant franchiseur de Tim Hortons au Canada)*, 2022, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_TDL_RF_FR.pdf> (consulté le 31 mars 2022).

228 LE MONDE et AGENCE FRANCE-PRESSE, « Une lanceuse d'alerte accuse Facebook de "choisir le profit plutôt que la sécurité" de ses utilisateurs », *Le Monde.fr* (3 octobre 2021), en ligne : <https://www.lemonde.fr/pixels/article/2021/10/03/facebook-se-defend-d-avoir-contribue-a-l-assaut-du-capitole-le-6-janvier_6096981_4408996.html> (consulté le 31 mars 2022); Damien LELOUP, « Santé mentale des adolescents : Instagram mis en difficulté par les sénateurs américains », *Le Monde.fr* (30 septembre 2021), en ligne : <https://www.lemonde.fr/pixels/article/2021/09/30/sante-mentale-des-adolescents-audition-a-haut-risque-pour-instagram-au-senat-americain_6096605_4408996.html> (consulté le 31 mars 2022).

229 Jon KEEGAN et Alfred NG, « The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users – The Markup », *The Markup* (6 décembre 2021), en ligne : <https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user> (consulté le 8 décembre 2021).

de géolocalisation, entre autres, vendrait les renseignements personnels ainsi obtenus (y compris ceux d'enfants) à de nombreux courtiers de données.

- En 2020, le *New York Times* a révélé[230] les pratiques de l'entreprise Clearview AI, qui a constitué une énorme banque de photos à partir du Web pour créer un outil de reconnaissance faciale. La Commission et certains de ses homologues canadiens ont ensuite mené une enquête à ce sujet et ont conclu que des renseignements personnels au sujet d'enfants avaient été recueillis et utilisés à des fins de biométrie en contravention avec les lois sur la protection des renseignements personnels[231].

Envisagés un à un, les préjudices potentiels peuvent sembler avoir un impact faible ou modéré sur les droits des mineurs. Mais lorsqu'ils sont favorisés de façon systémique par des choix commerciaux, leur récurrence amplifie leurs conséquences possibles. Le fait que la majorité des aspects de la vie des mineurs soient médiatisés par des tiers qui peuvent en tirer des renseignements personnels augmente de beaucoup la probabilité que se matérialise une succession de préjudices dont la gravité collective devient substantielle. Comme le soulignent les professeurs Danielle Citron et Daniel Solove, 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[232]. Ceux-ci peuvent ainsi concerner *un mineur* en particulier, mais aussi *les mineurs* comme groupe[233].

3.4 Raisons d'agir

Les éléments dans les sections précédentes permettent de répondre partiellement à la question à l'origine de ce rapport[234] : oui, les lois doivent prévoir des mesures de protection des renseignements personnels particulières pour les mineurs. Ces mesures

---

230 Kashmir HILL, « The Secretive Company That Might End Privacy as We Know It », *The New York Times* (18 janvier 2020), en ligne : <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> (consulté le 31 mars 2022).

231 *Enquête à l'égard de Clearview AI Inc.*, dossier 1023158-S, 14 décembre 2021, en ligne : <https://decisions.cai.gouv.qc.ca/cai/ss/fr/item/518218/index.do> (consulté le 31 mars 2022), paragraphe 73. Cette décision a été portée en appel par l'entreprise (Cour du Québec, nº 500-80-042393-224).

232 Danielle Keats CITRON et Daniel J. SOLOVE, « Privacy Harms », *SSRN Journal* 2021, p. 19-22, DOI : 10.2139/ssrn.3782222; Ignacio COFONE, « Privacy Standing », *University of Illinois Law Review* (à paraître), p. 12-17, en ligne : <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782887>.

233 Voir Andrew YOUNG, *Responsible group data for children*, UNICEF, 2020, en ligne : <https://www.unicef.org/globalinsight/media/1251/file/UNICEF-Global-Insight-DataGov-group-data-issue-brief-2020.pdf>; Jasmina BYRNE, Emma DAY et Linda RAFTREE, *UNICEF Global Insight Data Governance Manifesto*, 2021, p. 31, en ligne : <https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf>; Daniel J. SOLOVE, « The Limitations of Privacy Rights », (à paraître) 98 *Notre Dame Law Review*, p. 12-17, DOI : 10.2139/ssrn.4024790; D. K. CITRON et D. J. SOLOVE, précité, note 232, p. 21-22.

234 Voir la page i de ce rapport.

doivent permettre de maximiser les opportunités qui s'offrent à eux dans l'environnement numérique tout en minimisant les risques auxquels ils sont exposés[235].

S'il reste à déterminer *quelles mesures sont requises* et à analyser la suffisance des nouvelles exigences de la Loi 25*,* ce à quoi est consacrée la suite de ce rapport, la Commission peut déjà expliquer pourquoi de telles mesures s'imposent : les mineurs sont dans une situation de vulnérabilité particulière, compte tenu des paramètres actuels du monde numérique commercial. Dans d'autres domaines déjà, comme en matière de protection du consommateur, cette vulnérabilité a poussé l'État à légiférer pour protéger les mineurs de façon particulière.

3.4.1 Vulnérabilité des mineurs

Comme l'a montré cette section, les mineurs adoptent les technologies rapidement, mais ne comprennent que partiellement leurs implications, notamment en matière de vie privée et dans une perspective à long terme. Naviguant dans un environnement numérique conçu avant tout pour des adultes, ils se concentrent sur la gestion interpersonnelle de la circulation de leurs renseignements personnels. Face à la complexité et à l'opacité des pratiques commerciales impliquant la collecte, l'utilisation, la communication et la conservation de leurs renseignements personnels (voir la section 3.2.1), ils demeurent peu informés et ne peuvent exercer toute la vigilance souhaitée.

Faisant le parallèle avec des considérations souvent examinées en matière de protection du consommateur, la chercheuse Milda Mačėnaitė énonce d'autres facteurs de vulnérabilité[236] :

- **Développement :** les mineurs n'ont pas les mêmes capacités de raisonnement que les adultes. Ils les exercent de façon moins constante, et sont affectés par une certaine volatilité émotionnelle ou impulsivité;
- **Sensibilité aux pairs :** les mineurs sont particulièrement sensibles à l'influence et à la pression exercée par leurs pairs. En ce sens, les choix qu'ils opèrent sont parfois faits par souci de conformité au groupe;
- **Difficulté à interpréter les intentions :** les mineurs ont une capacité plus limitée que celle des adultes à repérer, à évaluer et à comprendre les intentions commerciales (vendre, persuader, etc.).

---

[235] « **Affirmant que** dans la mise en œuvre des politiques relatives à leurs droits dans l'environnement numérique, la prise en compte de l'évolution des capacités des enfants et de leur intérêt supérieur doit être une considération primordiale. La détermination d'un équilibre approprié entre la protection des enfants et la prise en compte de leur autonomie émergente est plus que jamais nécessaire pour leur permettre de tirer pleinement profit de l'environnement numérique tout en minimisant les risques auxquels ils peuvent être exposés ». ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, *Résolution sur les droits numériques des enfants*, Mexico, 2021, p. 3, en ligne : <https://globalprivacyassembly.org/wp-content/uploads/2021/12/Resolution-sur-les-droits-numeriques-des-enfants-GPA-finale-le-21.10.2021.FR_.pdf>.

[236] M. MAČĖNAITĖ, précité, note 71, p. 343-352.

Cette vulnérabilité particulière des mineurs peut être résumée en deux aspects : d'une part, ils sont exposés à plus de situations potentiellement préjudiciables et peuvent en subir de graves conséquences – comme en témoignent la multiplicité et la variété de risques présentés dans la section 3.3.1.2. De l'autre, ils se trouvent en situation d'impuissance, « c'est-à-dire le manque de structure ou de ressources pour faire face avec succès à la situation de risque »[237]. Les cours et les lois canadiennes et québécoises ont reconnu cette situation à plusieurs reprises, entre autres en accordant la préséance à l'intérêt supérieur de l'enfant en différentes matières[238].

Dans la mesure où plusieurs pratiques commerciales exploitent ces facteurs de vulnérabilité, il existe en outre une forte asymétrie de pouvoirs entre les entreprises et les mineurs. Les premières[239] :

- ont accès à des données non seulement sur le mineur, mais sur de larges pans de la population et sur des membres de son réseau social;
- dictent bon nombre des règles en vigueur dans l'espace numérique par leurs choix de conception;
- ont souvent accès à des moyens techniques sophistiqués qui permettent d'inférer de nouvelles informations sur le mineur (ex. profilage);
- peuvent mobiliser des méthodes novatrices pour exercer une influence sur les comportements ou les intentions du mineur (ex. analyse émotionnelle).

Comme le souligne la 5Rights Foundation, « cette asymétrie de pouvoir entre le mineur qui se développe et les plus puissantes compagnies du monde n'est pas dans "l'intérêt supérieur" de l'enfant »[240].

3.4.2 Protections existantes dans d'autres domaines

La société québécoise, comme beaucoup d'autres[241], a mis en place des protections particulières pour les mineurs en d'autres matières pour protéger leur intérêt supérieur. Il est par exemple interdit de leur vendre de l'alcool[242] ou des produits du tabac[243] avant l'âge de 18 ans, en raison des impacts importants de ces produits sur le bien-être

---

237 DIANA PAOLA ALVAREZ BAUTISTA, précité, note 201, p. 28.

238 *Id.*, p. 27-31; en matière d'information vaccinale, voir par exemple *M.C. c. R.S.*, 2022 QCCS 1260, en ligne : <https://www.canlii.org/fr/qc/qccs/doc/2022/2022qccs1260/2022qccs1260.html> (consulté le 10 mai 2022).

239 D. LYON, précité, note 63, p. 8; voir aussi, dans le domaine du jeu en ligne, les explications dans D. L. KING et al., précité, note 222, p. 139-140.

240 B. KIDRON, A. EVANS et J. AFIA, précité, note 86, p. 38, notre traduction.

241 Dans l'introduction du code de pratiques pour les enfants de l'autorité irlandaise de protection des données, la commissaire Helen Dixon rappelle que « dans toutes les autres sphères de la société, que ce soit dans les sports, en éducation, en matière d'accès à l'alcool ou de droit de vote, la position spéciale et les capacités évolutives des enfants sont des faits universellement reconnus » (notre traduction). Voir *Fundamentals*, précité, note 149, p. 4; 5RIGHTS FOUNDATION, *But how do they know it's a child?*, 2021, p. 16-17, en ligne : <https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf>.

242 *Loi sur les infractions en matière de boissons alcooliques*, RLRQ, c. I-8.1, art. 103.1.

243 *Loi concernant la lutte contre le tabagisme*, RLRQ, c. L-6.2, art. 13.

physique des enfants. Également, le contenu des films est classé en fonction de différents âges minimaux (public général, 13+, 16+, 18+)[244], le tout à des fins de « protection de la jeunesse »[245] face aux risques de contenu. Les gestionnaires de salles et les locateurs de films doivent d'ailleurs respecter ce classement dans leur gestion des accès[246].

Dans un ordre d'idées plus proche du thème du présent rapport, le Québec a également fait le choix d'interdire la publicité commerciale adressée aux enfants de moins de 13 ans dans la LPC, à l'article 248. Quasiment unique au monde[247], cette interdiction témoigne d'un véritable choix de société plaçant l'intérêt supérieur de l'enfant au-dessus des intérêts commerciaux. C'est d'ailleurs la façon dont beaucoup d'intervenants qualifiaient cette mesure dans les années 1970, au cours des différents cycles d'élaboration de la LPC[248].

Il y a beaucoup de parallèles à dresser entre l'interdiction consacrée à l'article 248 de la LPC et la question examinée dans ce rapport, comme l'ont souligné les parlementaires lors de l'étude détaillée du projet de loi nº 64[249]. Elle met en jeu les intérêts des enfants et

---

244 *Loi sur le cinéma*, RLRQ, c. C-18.1, chapitre III, section I, plus particulièrement l'article 81.

245 *Id.*, art. 81.

246 *Id.*, art. 86 à 86.2.

247 À ce jour, une interdiction similaire n'existe qu'en Suède, bien que d'autres pays aient adopté des cadres réglementaires qui limitent la publicité adressée aux enfants. Voir Jacinthe LAUZON, Micheal Jared SIMKIN et Marie-Hélène BEAULIEU, *La publicité destinée aux enfants : Identifier la meilleure protection possible*, Option consommateurs, 2008, en ligne : <https://www.option-consommateurs.org/documents/principal/fr/File/rapports/pratiques_commerciales/oc_ic_publicite_enfant_200804.pdf>, chapitre V; voir aussi OFFICE DE LA PROTECTION DU CONSOMMATEUR, précité, note 69, p. 13.

248 Voir les débats tenus à l'Assemblée nationale au cours du processus législatif entourant les projets de loi nº 45 (29e lég., 1re sess.), nº 7 (30e lég., 4e sess.) et nº 72 (31e lég., 3e sess.). :

- « Index du Journal des débats - 29e législature, 1re session (9 juin 1970 - 19 décembre 1970) – 45 - Loi de la protection du consommateur (le ministre de la Justice) », *Assemblée nationale du Québec*, en ligne : <http://www.assnat.qc.ca/fr/travaux-parlementaires/journaux-debats/index-jd/recherche.html?cat=sv&Session=jd29l1se&Section=projlois&Requete=45+-+Loi+de+la+protection+du+consommateur+ (le+ministre+de+la+Justice)> (consulté le 27 janvier 2022).
- « Index du Journal des débats - 30e législature, 4e session (16 mars 1976 - 18 octobre 1976) – 7 - Loi sur la protection du consommateur (le ministre des Consommateurs, des Coopératives et des Institutions financières) », *Assemblée nationale du Québec*, en ligne : <http://www.assnat.qc.ca/fr/travaux-parlementaires/journaux-debats/index-jd/recherche.html?cat=sv&Session=jd30l4se&Section=projlois&Requete=7+-+Loi+sur+la+protection+du+consommateur+ (le+ministre+des+Consommateurs%2c+des+Coop%c3%a9ratives+et+des+Institutions+financi%c3%a8res)> (consulté le 27 janvier 2022).
- « Index du Journal des débats - 31e législature, 3e session (21 février 1978 - 20 février 1979) – 72 - Loi sur la protection du consommateur (le ministre des Consommateurs, des Coopératives et des Institutions financières) », *Assemblée nationale du Québec*, en ligne : <http://www.assnat.qc.ca/fr/travaux-parlementaires/journaux-debats/index-jd/recherche.html?cat=sv&Session=jd31l3se&Section=projlois&Requete=72+-+Loi+sur+la+protection+du+consommateur+ (le+ministre+des+Consommateurs%2c+des+Coop%c3%a9ratives+et+des+Institutions+financi%c3%a8res)> (consulté le 27 janvier 2022).

249 « Étude détaillée du projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels », *Journal des débats de la Commission des institutions de l'Assemblée nationale du Québec* (12 mai 2021), en ligne : <http://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/ci-42-1/journal-debats/CI-210512.html#16h30> (consulté le 4 avril 2022), voir à partir de 16 h 40 environ.

ceux des entreprises. Elle concerne aussi le financement d'un service (ex. émissions de télévision, magazines, etc.) par la publicité, comme en l'occurrence (voir section 3.2.1.2). Par ailleurs, c'est notamment en raison de la vulnérabilité intrinsèque des enfants, peu habiles à déceler les intentions commerciales[250], qu'elle a été mise en place, avec l'objectif de les prémunir de l'exploitation commerciale.

S'il est clair pour l'Office de la protection du consommateur que l'interdiction de l'article 248 de la LPC vise également les publicités diffusées sur Internet[251], il subsiste néanmoins un flou par rapport à son applicabilité à la publicité ciblée[252]. Par ailleurs, elle n'offre aucune protection pour les adolescents et elle n'empêche pas l'exploitation des renseignements personnels à des fins d'influence du comportement par d'autres moyens que la publicité, ou à des fins d'analyse prédictive, par exemple.

L'objectif principal de l'article 248 de la LPC était de protéger les mineurs contre l'exploitation économique. Dans le contexte d'une économie numérique où les données servent notamment à profiler ou à cibler des messages publicitaires pour vendre davantage, il est plus que jamais important de veiller à ce que cet objectif se traduise dans la loi afin que soit respecté l'esprit de cette interdiction.

---

250 Cet aspect a d'ailleurs été validé par la Cour suprême du Canada dans l'affaire *Irwin Toy Ltd. c. Québec (Procureur général)*, [1989] 1 RCS 927, en ligne : <https://scc-csc.lexum.com/scc-csc/scc-csc/fr/item/443/index.do>: « L'objectif de réglementer la publicité commerciale destinée à des enfants est conforme au but général d'une loi sur la protection du consommateur, c. à d. de protéger un groupe qui est très vulnérable à la manipulation commerciale. Les enfants n'ont pas les capacités des adultes pour évaluer la force persuasive de la publicité. Le législateur a raisonnablement conclu qu'il fallait empêcher les annonceurs d'exploiter la crédulité des enfants. ».

251 OFFICE DE LA PROTECTION DU CONSOMMATEUR, *Publicité destinée aux enfants de moins de 13 ans – Guide d'application des articles 248 et 249, Loi sur la protection du consommateur*, 2012, p. 3, en ligne : <https://cdn.opc.gouv.qc.ca/media/documents/consommateur/bien-service/index-sujet/guide-application.pdf?1379440600>.

252 Voir OPTION CONSOMMATEURS, précité, note 223, p. 11; DIANA PAOLA ALVAREZ BAUTISTA, précité, note 201, p. 86-88; Vincent GAUTRAIS et Adriane PORCIN, « Les 7 péchés de la L.p.c. : actions et omissions applicables au commerce électronique », (2009) 43-3 *Revue juridique Thémis* 45, p. 587-590.

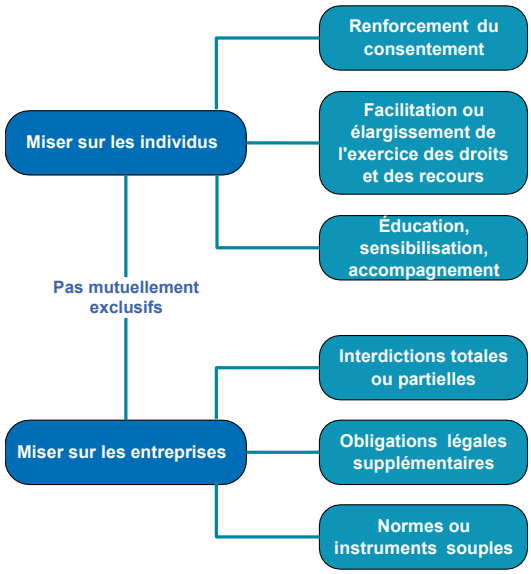
4. MOYENS POUR PROTÉGER LES MINEURS

Étant établi qu'il est nécessaire d'accorder une protection particulière aux mineurs par rapport à leurs renseignements personnels, la Commission analyse ci-après les moyens d'y parvenir.

Elle 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);
- En misant sur les **entreprises** pour renforcer leurs obligations de protection (prévention).

La figure suivante résume les grandes catégories de mesures présentées dans cette section, 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.



4.1 Mesures proposées par diverses organisations

Depuis un peu plus d'une dizaine d'années, la protection des renseignements personnels des mineurs fait l'objet de plus en plus de travaux supra-gouvernementaux, gouvernementaux et non gouvernementaux dans différentes juridictions. Ceux-ci incluent souvent une analyse des problèmes auxquels font face les mineurs dans le monde numérique, mais présentent également des pistes d'action pour les décideurs.

Pour préparer ce rapport, la Commission a réévalué ses recommandations passées. De plus, elle a consulté la documentation préparée par les organisations suivantes :

- Organisation des Nations unies;
  - Fonds des Nations unies pour l'enfance (ci-après UNICEF);
- Organisation de coopération et de développement économiques (OCDE);
- Assemblée mondiale pour la vie privée (ci-après AMVP);
  - Groupe de travail international sur la protection des données dans les télécommunications;
- International Consumer Protection and Enforcement Network;
- Conseil de l'Europe;
- Comité européen de la protection des données (ci-après CEPD) et sa forme antérieure, le Groupe de travail « Article 29 » sur la protection des données;
- Autorités de protection des renseignements personnels;
  - Ontario : Commissaire à l'information et à protection de la vie privée (ci-après CIPVP)
  - Canada : Commissariat à la protection de la vie privée (ci-après CPVPC)
  - Et celles d'Irlande, de France et du Royaume-Uni, dont les travaux sont présentés plus bas (sections 4.2.1.2 et 4.3);
- Instances nationales chargées de la protection des droits ou de l'enfance :
  - Royaume-Uni : Children's Commissioner;
  - Québec : Commission des droits de la personne et des droits de la jeunesse (ci-après CDPDJ);
  - Canada : Groupe de travail des commissaires à la vie privée et des défenseurs canadiens des enfants et des jeunes sur la protection des renseignements personnels des enfants en ligne (2009) (ci-après GTCVP);
- Organisations non gouvernementales;
  - Royaume-Uni : 5Rights Foundation;
  - Québec : Option consommateurs;
  - Canada : HabiloMédias.

Beaucoup de points de convergence se dégagent des différents documents consultés. Dans l'ensemble, les recommandations qui y sont formulées s'appuient sur des considérations similaires à celles présentées dans la section 3 de ce rapport : pour cette raison, les cadres théoriques et les arguments en faveur d'une protection particulière pour les mineurs ne sont pas répétés.

Les pages suivantes détaillent les mesures et orientations proposées pour renforcer ou mettre en œuvre cette protection des renseignements personnels des mineurs. Il faut noter qu'elles doivent être envisagées si possible autant pour les *services* que pour les

produits numériques (ex. objets connectés), considérant que ceux-ci sont de plus en plus nombreux et intégrés à la vie des mineurs[253].

4.1.1 Miser sur les individus

Une première catégorie de mesures vise les individus. Elles ont pour objectif d'améliorer leur capacité d'agir et leurs connaissances pour les aider à faire de meilleurs choix concernant la protection de leurs renseignements personnels, ou encore pour qu'ils puissent réagir en cas de préjudice, par l'entremise de droits et de recours. 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.

On peut distinguer trois grands types de mesures misant sur les individus, qu'il s'agisse des mineurs ou de leurs parents :

- le renforcement du consentement;
- la facilitation ou l'élargissement de l'exercice des droits et des recours;
- l'éducation, la sensibilisation et l'accompagnement.

4.1.1.1 Renforcement du consentement

Les mesures détaillées ci-après visent à renforcer la capacité des individus à exercer leur consentement de manière significative. Par exemple, on peut augmenter le nombre de situations où le consentement est demandé, exiger qu'il soit donné de manière expresse, instaurer des seuils d'âge pour un consentement valide ou améliorer la qualité de l'information fournie à l'individu.

4.1.1.1.1 Exiger l'obtention d'un consentement parental avant un certain âge

Les différents documents consultés incluent pour plusieurs des recommandations concernant le consentement parental, avec plus ou moins de portée. Cette mesure est ainsi vue comme l'une des façons de renforcer la protection des renseignements personnels des mineurs, sans être la seule : doué de plus de discernement que le mineur en deçà d'un certain âge, l'adulte se voit confier la responsabilité d'accepter ou de refuser certaines collectes, utilisations ou communications de données.

Plusieurs reconnaissent l'utilité de ce mécanisme[254]. Diverses nuances s'imposent toutefois : par exemple, on souligne souvent qu'en vertu du principe de l'intérêt supérieur

[253] CONSEIL DE L'EUROPE, *Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique*, Recommandation CM/Rec (2018) 7 du Comité des Ministres, 2018, par. 36, en ligne : <https://rm.coe.int/lignes-directrices-relatives-au-respect-a-la-protection-et-a-la-realis/16808d881b>; Observation générale nº 25, précité, note 11, par. 74.

[254] INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, *Protecting the Privacy of Children in Online Services - Working paper*, 2019, par. 17 et 20, en ligne : <https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2019/2019-IWGDPT-Working_Paper_Online_Services_for_Children.pdf>; GROUPE DE TRAVAIL DES COMMISSAIRES À LA VIE PRIVÉE ET DES DÉFENSEURS CANADIENS DES ENFANTS ET DES JEUNES SUR LA PROTECTION DES RENSEIGNEMENTS

de l'enfant, certaines situations (ex. demander de l'aide en raison d'une situation violente) ne doivent pas être visées par l'obligation d'obtenir un consentement parental[255]. Certains insistent aussi sur l'importance d'associer l'enfant à l'expression du consentement parental, même s'il n'a pas atteint l'âge du « consentement numérique »[256].

Pour sa part, dans un document d'orientations sur l'intelligence artificielle visant les enfants, l'UNICEF reconnaît que les parents doivent avoir un rôle à jouer dans le consentement pour les enfants plus jeunes; cela dit, à mesure qu'ils grandissent et acquièrent de l'autonomie, il faut revoir le partage des rôles afin de promouvoir l'agentivité des mineurs[257]. Cette idée est présente dans les travaux du CIPVP et du GTCVP, qui proposent des mécanismes par paliers d'âge[258]. Dans le cas du GTCVP, la particularité de la suggestion est que toute collecte, utilisation ou communication de renseignements personnels concernant un enfant de moins de 13 ans est *interdite*; le parent est ensuite impliqué pour le consentement pendant un certain nombre d'années au cours de l'adolescence.

Plusieurs organisations proposent de valider le consentement donné par un parent auprès du mineur lui-même une fois que celui-ci atteint l'âge nécessaire pour consentir de façon autonome à la collecte, à l'utilisation ou à la communication de ses renseignements personnels, ou à tout le moins d'informer le mineur de la possibilité de retirer son consentement[259].

PERSONNELS DES ENFANTS EN LIGNE, *Il devrait y avoir une loi : Les sauts périlleux de la vie privée des enfants au 21e siècle*, 2009, p. 17-19, en ligne : <https://www.bibliotheque.assnat.qc.ca/DepotNumerique_v2/AffichageFichier.aspx?idf=32966>; « Vous recueillez des renseignements auprès des enfants? Voici dix conseils sur les services destinés aux enfants et aux jeunes », *Commissariat à la protection de la vie privée du Canada* (14 décembre 2015), en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/bus_kids/02_05_d_62_tips/> (consulté le 17 janvier 2022); CONSEIL DE L'EUROPE, précité, note 253, par. 30.

255 INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, précité, note 254, par. 17; Observation générale nº 25, *Observation générale nº 25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique*, 2021, par. 78, en ligne : <https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2f5F0vEG%2bcAAx34gC78FwvnmZXGFsdFXGQsWU46nx%2b5vAg3QbGXlnOwo3Oquj8nN7ltX6yUYoRpe7N%2b7Q6mEUIz2mfWi> (consulté le 16 décembre 2021).

256 ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 6.

257 UNICEF et MINISTÈRE DES AFFAIRES ÉTRANGÈRES DE LA FINLANDE, précité, note 55, p. 31.

258 COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, *Commentaires du CIPVP sur le livre blanc du gouvernement de l'Ontario intitulé Modernisation de la protection de la vie privée en Ontario*, 2021, p. 27-28, en ligne : <http://www.ipc.on.ca/wp-content/uploads/2021/09/2021-09-03-commentaires-du-cipvp-le-livre-blanc-du-gouv-on-modernisation-protection-vie-privee-en-on.pdf>; GROUPE DE TRAVAIL DES COMMISSAIRES À LA VIE PRIVÉE ET DES DÉFENSEURS CANADIENS DES ENFANTS ET DES JEUNES SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DES ENFANTS EN LIGNE, précité, note 254, p. 18.

259 COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679*, 2020, par. 147-149, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf>; INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, précité, note 254, par. 23; GROUPE DE TRAVAIL DES COMMISSAIRES À LA VIE PRIVÉE ET DES DÉFENSEURS CANADIENS DES ENFANTS ET DES JEUNES SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DES ENFANTS EN LIGNE, précité, note 254, p. 18.

Puisque beaucoup de juridictions choisissent un seuil d'âge de 13 ou 14 ans pour le consentement autonome du mineur, l'UNICEF souligne toutefois que le mécanisme du consentement parental est souvent une protection insuffisante pour les adolescents dans le monde numérique[260].

4.1.1.1.2 Obliger à adapter les informations à l'âge des enfants visés et renforcer la transparence

Comme la Commission en a fait état dans la section 3.2, la compréhension par les mineurs des pratiques des entreprises et des finalités envisagées pour leurs renseignements personnels est imparfaite, en partie parce que les informations qui leur sont fournies sont souvent partielles ou nébuleuses. Comme piste de solution, dans son rapport quinquennal de 2011, la Commission proposait de simplifier l'information transmise grâce à des pictogrammes standardisés[261].

La quasi-totalité des organisations dont la documentation a été consultée reconnaît aussi ce problème et recommande d'obliger les entreprises à adapter les informations données à l'âge des enfants visés[262]. Cette orientation consensuelle se décline en différents volets :

- Prévoir des informations adaptées aux adultes et d'autres, parallèles, adaptées aux enfants, en tenant compte des stades de développement de la littératie;
- Donner les informations de différentes façons (textes, images, vidéos, etc.);
- Donner l'information en amont (par exemple, avant l'obtention du consentement à la création d'un compte d'utilisateur), puis « juste à temps », au moment où elle est requise (par exemple, au moment de changer un paramètre de confidentialité).

Pour renforcer la transparence, tant envers les mineurs que les parents, il est également proposé d'obliger les fournisseurs de produits et de services numériques à publier des politiques de confidentialité différenciées, c'est-à-dire qui visent chacun de leurs produits

---

260 J. BYRNE, E. DAY et L. RAFTREE, précité, note 233, p. 60 -62.

261 COMMISSION D'ACCÈS À L'INFORMATION, *Technologies et vie privée à l'heure des choix de société*, 2011, p. 35-36, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_RQ_2011.pdf>.

262 UNICEF et MINISTÈRE DES AFFAIRES ÉTRANGÈRES DE LA FINLANDE, précité, note 55, p. 33-35; Observation générale nº 25, précité, note 11, par. 39; ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *Recommandation du Conseil sur les enfants dans l'environnement numérique*, OCDE/LEGAL/0389, Organisation de coopération et de développement économiques, 2021, p. 14, en ligne : <https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0389%20> (consulté le 16 décembre 2021); INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, précité, note 254, par. 25-28; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 5; INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS, *Resolution on Children's Online Privacy*, Strasbourg, 2008, en ligne : <http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Childrens-Online-Privacy-.pdf>; COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, précité, note 259, par. 70 et 126; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, précité, note 254; CONSEIL DE L'EUROPE, précité, note 253, par. 14; COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, précité, note 39, p. 21-22; 5RIGHTS FOUNDATION, précité, note 141; 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 no 64, Loi modernisant les dispositions législatives en matière de protection des renseignements personnels*, Cat. 2.412.42.8, 2020, p. 85, en ligne : <https://www.cdpdj.qc.ca/storage/app/media/publications/memoire_PL64_renseignements-personnels.pdf>.

ou services spécifiques[263]. Si un fournisseur propose à la fois un site Web et trois jouets connectés, il devrait alors prévoir une politique particulière pour chacun de ces quatre éléments plutôt que de n'en rédiger qu'une concernant le seul site Web.

Enfin, certaines organisations recommandent que les entreprises soient tenues de mettre en place des mécanismes pour aviser les enfants lorsqu'une fonctionnalité de contrôle parental ou de surveillance parentale est activée[264]. Par exemple, elles pourraient avoir recours à une icône clignotante sur l'appareil visé (téléphone intelligent, bracelet connecté, etc.). Cette mesure vise davantage à mitiger les risques en matière de vie privée interpersonnelle que ceux liés à sa dimension commerciale.

4.1.1.2 Facilitation ou élargissement de l'exercice des droits et des recours

Certaines mesures proposées visent à élargir les droits et les recours des individus ou à en faciliter l'exercice.

Ainsi, comme solution notamment aux problèmes émergeant de la dimension interpersonnelle de la vie privée, certains travaux internationaux mettent de l'avant un droit au déréférencement (c'est-à-dire de demander qu'un renseignement personnel ne soit plus diffusé par un tiers) pour les mineurs[265]. D'autres suggèrent l'ajout d'un droit plus large de demander la *suppression* de leurs renseignements personnels[266]. Entre autres, ces droits visent à préserver la capacité des mineurs à « expérimenter et [à] se découvrir sans s'inquiéter de la permanence des renseignements qu'ils affichent sur eux-mêmes en ligne »[267].

Par ailleurs, plusieurs organisations soulignent l'importance de travailler à faciliter l'exercice des droits par les mineurs, notamment en s'assurant que ceux-ci puissent les faire valoir seuls à partir d'un certain âge, qui n'a pas forcément à être le même que celui lié au consentement autonome, et en implantant des mécanismes simplifiés de demande d'exercice des droits (d'accès, de rectification, de déréférencement, de portabilité, etc.)[268].

---

263 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, précité, note 254; COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, précité, note 39, p. 21-22; V. MONTCALM, A. PLOURDE et E. THÉRIAULT, précité, note 57, p. 24 et 62.

264 Observation générale nº 25, précité, note 11, par. 76; CONSEIL DE L'EUROPE, précité, note 253, par. 54; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 8.

265 COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, précité, note 258, p. 13; J. FRÉCHETTE, précité, note 160, p. 48.

266 V. MONTCALM, A. PLOURDE et E. THÉRIAULT, précité, note 57, p. 63; INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, précité, note 254, par. 18-19; J. BYRNE, E. DAY et L. RAFTREE, précité, note 233, p. 61.

267 Ces propos du Commissaire à l'information et à la protection de la vie privée de l'Ontario sont rapportés dans le document suivant : GOUVERNEMENT DE L'ONTARIO, *Modernisation de la protection de la vie privée en Ontario - Autonomiser les Ontariens et favoriser l'économie numérique*, 2020, p. 9, en ligne : <https://www.ontariocanada.com/registry/showAttachment.do?postingId=37468&attachmentId=49464>.

268 INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, précité, note 254, par. 38-39; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 5; CONSEIL DE L'EUROPE, précité, note 253, par. 28 et 34; COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, précité, note 258, p. 27; ARTICLE 29 DATA PROTECTION WORKING PARTY, *Avis 2/2009 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier*

Des propositions semblables sont faites en ce qui concerne les interfaces de consentement, notamment[269].

Les droits et les recours sont essentiels, mais ils sont généralement exercés *après* la survenance d'un préjudice. Ils ne constituent par ailleurs qu'une solution partielle pour des individus précis qui choisissent de les exercer[270]; autrement dit, ce ne sont pas des interventions systémiques permettant de protéger l'aspect *collectif* du droit à la vie privée.

4.1.1.3 Éducation, sensibilisation, accompagnement

L'éducation, la sensibilisation ou l'accompagnement des individus sont d'excellents moyens de renforcer leur littératie en matière de numérique et de protection des renseignements personnels, ce qui peut les aider à faire de meilleurs choix. L'importance de ces éléments fait d'ailleurs consensus à travers les documents consultés. Le souci de renforcer la littératie numérique et la connaissance de leurs droits des mineurs, des parents et des éducateurs est exprimé par plusieurs organisations[271], dont la Commission[272]; il traverse aussi les travaux du groupe canadien HabiloMédias[273]. Voici par exemple comment l'Observation générale nº 25 présente sa recommandation :

> 21. Conformément au devoir qu'ont les États de fournir une assistance appropriée aux parents et aux personnes qui s'occupent des enfants dans l'exercice de leurs responsabilités éducatives, les États parties devraient sensibiliser les parents et les personnes qui s'occupent des enfants à la nécessité de respecter le développement de l'autonomie, des capacités et de la vie privée des enfants. Ils devraient aider les parents et les personnes qui s'occupent des enfants à acquérir une culture numérique et à prendre conscience des risques que courent les enfants, afin de les aider à apporter un appui aux enfants aux fins de la réalisation de leurs droits, y compris le droit à une protection, en relation avec l'environnement numérique.

La Commission a elle aussi recommandé à plusieurs reprises d'agir davantage sur les fronts de l'éducation et de la sensibilisation, en plus d'entreprendre des initiatives en ce sens. À titre d'exemple, elle proposait en 2020[274] d'intégrer des notions de citoyenneté numérique (liées notamment au droit à l'information et au droit au respect de la vie privée)

---

des écoles), 398/09/EN WP 160, 2009, p. 6, en ligne : <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_fr.pdf>.

269 S. McALEESE, M. JOHNSON et M. LADOUCEUR, précité, note 41, p. 19-31.

270 D. J. SOLOVE, précité, note 233.

271 Observation générale nº 25, précité, note 11, par. 21; ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, précité, note 262, principe 2; INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, précité, note 254, par. 40; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 5 et 8-9; Résolution de Strasbourg, précité, note 262; CONSEIL DE L'EUROPE, précité, note 253, par. 41; COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, précité, note 39, p. 22; V. MONTCALM, A. PLOURDE et E. THÉRIAULT, précité, note 57, p. 63; J. FRÉCHETTE, précité, note 160, p. 48; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, précité, note 262, p. 85-86.

272 COMMISSION D'ACCÈS À L'INFORMATION, précité, note 261, p. 32.

273 HABILOMÉDIAS, « HabiloMédias.ca », en ligne : <https://habilomedias.ca/> (consulté le 16 mai 2022).

274 COMMISSION D'ACCÈS À L'INFORMATION, précité, note 46.

au nouveau cours issu de la révision du programme d'études *Éthique et culture religieuse*. Depuis de nombreuses années, en cohérence avec la communauté internationale[275] et pancanadienne[276] des autorités de protection des renseignements personnels, la Commission souligne l'importance de renforcer l'éducation des mineurs et de leurs parents au numérique et à la vie privée et pose des gestes en ce sens. Par exemple, elle a conçu et recensé du matériel adressé aux mineurs et aux enseignants au fil des années[277] et a effectué une tournée des écoles de 2016 à 2020 pour parler de protection des renseignements personnels et de cyberrisques[278].

L'une des limites de ces mesures est qu'elles doivent être appliquées dans la durée, et n'ont généralement pas d'effet immédiat sur la population.

4.1.2 Miser sur les entreprises

La deuxième catégorie rassemble des mesures qui visent les entreprises : elles ont pour objectif de renforcer la responsabilité de celles-ci afin de prévenir les préjudices pouvant affecter les mineurs. La Commission en distingue trois grands types :

- les interdictions, qu'elles soient totales ou partielles;
- les obligations légales supplémentaires;
- l'élaboration de normes ou d'instruments souples.

4.1.2.1 Interdictions totales ou partielles

Les lois sur la protection des renseignements personnels peuvent contenir des interdictions totales ou partielles afin de limiter les pratiques préjudiciables aux mineurs, un peu à l'image de l'interdiction de diffuser des publicités s'adressant aux enfants consacrée dans la LPC[279].

En ce sens, beaucoup des travaux consultés suggèrent que certaines des pratiques des entreprises présentées dans la section 3 devraient être interdites ou limitées, compte tenu de leur impact marqué sur les droits des mineurs. C'est le cas du profilage, de la publicité comportementale, de l'utilisation des renseignements personnels des mineurs à des fins qui leur sont autrement nuisibles et des décisions automatisées. On retrouve aussi des recommandations visant la communication de renseignements personnels de mineurs à

---

275 Résolution de Strasbourg, précité, note 262; plus récemment, voir ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235.

276 COMMISSAIRES À LA PROTECTION DE LA VIE PRIVÉE ET RESPONSABLES DE LA SURVEILLANCE DE LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *La vie privée des enfants en ligne – Résolution des commissaires à la protection de la vie privée et responsables de la surveillance de la protection de la vie privée du Canada*, Regina, Saskatchewan, 2008, en ligne : <https://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_080604/?wbdisable=true>.

277 « Espace jeunesse », *Commission d'accès à l'information*, en ligne : <https://www.cai.gouv.qc.ca/jeunes/> (consulté le 6 avril 2022).

278 *Id.*

279 LPC, art. 248.

des tiers, la collecte de renseignements personnels de mineurs et le recours à des interfaces truquées.

4.1.2.1.1 Profilage, publicité comportementale, décisions automatisées et utilisation à des fins nuisibles

Très répandus dans le monde numérique, le profilage et la publicité comportementale – qui en constitue un cas d'application précis – reposent un peu sur les renseignements fournis, mais surtout sur les renseignements observés et inférés. Ils sont généralement jugés néfastes pour les mineurs, entre autres en raison de leur potentiel d'influence du comportement et de discrimination. Plusieurs soulignent qu'ils constituent une forme d'exploitation économique des mineurs[280]. Les recommandations visant à les interdire ou à les limiter sont nombreuses.

Dans son rapport quinquennal de 2011, la Commission demandait déjà au législateur d'envisager l'interdiction du profilage des mineurs[281]. Quelques autres organisations vont aussi loin[282], avec parfois des nuances sur des situations exceptionnelles où le profilage peut se justifier dans l'intérêt supérieur de l'enfant. Très précisément, on fait référence aux cas où celui-ci permet de vérifier leur âge (en vue de limiter leur exposition à certains risques) ou de leur fournir un service qui les protège.

D'autres organisations recommandent de restreindre le profilage pour éviter entre autres les cas où il désavantage les enfants, influence négativement leur comportement ou leurs décisions ou sert à des fins de marketing[283]. De son côté, l'UNICEF rappelle qu'encadrer le profilage est nécessaire pour protéger non seulement le droit individuel des mineurs à la vie privée, mais aussi pour préserver des droits collectifs, puisque le profilage met souvent en relation de grandes quantités d'individus entre eux[284].

Unanimement, les organisations qui abordent le problème de la publicité comportementale ou ciblée recommandent qu'elle soit interdite lorsqu'elle vise les enfants

---

280 UNICEF et MINISTÈRE DES AFFAIRES ÉTRANGÈRES DE LA FINLANDE, précité, note 55, p. 31; J. BYRNE, E. DAY et L. RAFTREE, précité, note 233, p. 21; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 7.

281 COMMISSION D'ACCÈS À L'INFORMATION, précité, note 261, p. 35 -36.

282 Observation générale nº 25, précité, note 11, par. 42; ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, précité, note 262, p. 14; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 6-7; CONSEIL DE L'EUROPE, précité, note 253, par. 37.

283 J. BYRNE, E. DAY et L. RAFTREE, précité, note 233, p. 59; UNICEF et MINISTÈRE DES AFFAIRES ÉTRANGÈRES DE LA FINLANDE, précité, note 55, p. 31; COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, précité, note 258, p. 10; COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, précité, note 39, p. 22; COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679*, WP251rev.01, 2018, p. 31-33, en ligne : <https://ec.europa.eu/newsroom/article29/items/612053>.

284 UNICEF et MINISTÈRE DES AFFAIRES ÉTRANGÈRES DE LA FINLANDE, précité, note 55, p. 31.

ou jugent que les entreprises ne devraient pas y avoir recours[285]. Cela implique également que soit proscrit le profilage utilisé aux fins de cibler cette publicité.

Par ailleurs, profilage et décisions automatisées sont fortement associés[286]; dans l'environnement numérique, tous deux résultent généralement de l'action d'un algorithme nourri par des renseignements personnels fournis, observés ou inférés (l'inférence elle-même peut constituer la décision automatisée). Il n'est donc pas étonnant que certaines voix estiment que les entreprises ne devraient pas prendre de décisions entièrement automatisées concernant les mineurs lorsqu'elles peuvent avoir un impact significatif (ex. juridique ou autre) sur eux[287].

De manière plus générale, plusieurs recommandations visent l'interdiction de l'utilisation des renseignements personnels de mineurs à des fins qui nuisent à leur bien-être (de façon démontrée)[288], comme :

- Le neuromarketing[289];
- L'analytique ou l'influence émotionnelle[290];
- La publicité immersive et en réalité augmentée ou virtuelle[291];

---

285 J. BYRNE, E. DAY et L. RAFTREE, précité, note 233, p. 59; Observation générale nº 25, précité, note 11, par. 40-42; GROUPE DE TRAVAIL DES COMMISSAIRES À LA VIE PRIVÉE ET DES DÉFENSEURS CANADIENS DES ENFANTS ET DES JEUNES SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DES ENFANTS EN LIGNE, précité, note 254, p. 16; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 7; Résolution de Strasbourg, précité, note 262, p. 2; COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, précité, note 283, p. 32; REVEALING REALITY, précité, note 61, p. 10; OPTION CONSOMMATEURS, précité, note 223, p. 12; INTERNATIONAL CONSUMER PROTECTION AND ENFORCEMENT NETWORK, *Best Practice Principles for Marketing Practices Directed Towards Children Online*, 2020, par. 40-41, en ligne : <https://icpen.org/sites/default/files/2020-06/ICPEN%20-%20Best%20Practice%20Principles%20for%20Marketing%20Practices%20Directed%20Towards%20Children%20Online%202020.pdf>; « Position de principe sur la publicité comportementale en ligne », *Commissariat à la protection de la vie privée du Canada* (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 31 janvier 2022).

286 Par exemple, le RGPD les évoque parfois conjointement : RGPD, notamment considérant 71 et article 13 (2) (f).

287 UNICEF et MINISTÈRE DES AFFAIRES ÉTRANGÈRES DE LA FINLANDE, précité, note 55, p. 34; ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, précité, note 262, p. 14; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 6; COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, précité, note 283, p. 31 -33.

288 Observation générale nº 25, précité, note 11, par. 42, 53 et 61; J. BYRNE, E. DAY et L. RAFTREE, précité, note 233, p. 59; ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, précité, note 262, p. 14; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 6; COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, précité, note 258, p. 10; CONSEIL DE L'EUROPE, *Recommandation CM/Rec (2021) 8 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre du profilage*, Strasbourg, Editions du Conseil de l'Europe, 2021, par. 2.2, en ligne : <https://search.coe.int/cm/pages/result_details.aspx?ObjectId=0900001680a46148>.

289 Observation générale nº 25, précité, note 11, par. 42.

290 *Id.*; J. BYRNE, E. DAY et L. RAFTREE, précité, note 233, p. 60.

291 Observation générale nº 25, précité, note 11, par. 42.

- Les systèmes de recommandation priorisant le contenu payant ayant une motivation commerciale ou politique[292];
- Le design persuasif visant à prolonger le temps d'utilisation[293];
- Les pratiques manipulatrices ou qui influencent abusivement le comportement ou les émotions[294];

Dans son mémoire sur le projet de loi nº 64, la Commission recommandait elle-même que la loi interdise certaines utilisations de renseignements personnels préjudiciables aux individus ou portant atteinte à leurs droits fondamentaux[295]. Dans ces cas, elle estimait qu'un consentement ne pouvait pas légitimer ces pratiques.

4.1.2.1.2 Communication de renseignements personnels de mineurs à des tiers

La circulation accrue des renseignements personnels des mineurs entre les différents acteurs de l'écosystème numérique accentue les risques qui se posent pour leurs droits. Entre autres, elle peut mener à leur utilisation à de nouvelles fins, sans nécessairement que les mineurs ou leurs parents en soient informés.

Pour cette raison, il est parfois proposé d'interdire aux entreprises de communiquer les renseignements personnels concernant des mineurs à des tiers à des fins commerciales ou de limiter cette communication pour les seules fins liées à la fourniture du service demandé[296].

4.1.2.1.3 Collecte de renseignements personnels de mineurs

L'étape de la collecte[297], la première du cycle de vie du renseignement personnel, est cruciale pour la gestion des risques subséquents pour les mineurs. Un certain nombre d'organisations recommandent aux États ou aux entreprises elles-mêmes de limiter cette collecte au strict minimum lorsqu'elle est réalisée à des fins commerciales[298].

---

292 *Id.*, par. 53 et 61.

293 J. BYRNE, E. DAY et L. RAFTREE, précité, note 233, p. 59.

294 ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 6.

295 COMMISSION D'ACCÈS À L'INFORMATION, précité, note 62, p. 37-38.

296 Observation générale nº 25, précité, note 11, par. 73; ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, précité, note 262, p. 14; Résolution de Strasbourg, précité, note 262; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 7; GROUPE DE TRAVAIL DES COMMISSAIRES À LA VIE PRIVÉE ET DES DÉFENSEURS CANADIENS DES ENFANTS ET DES JEUNES SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DES ENFANTS EN LIGNE, précité, note 254, p. 18 (pour les moins de 15 ans); J. FRÉCHETTE, précité, note 160, p. 48.

297 C'est-à-dire sa fourniture par la personne concernée, ou son observation ou inférence par l'entreprise.

298 ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, précité, note 262, p. 14; Résolution de Strasbourg, précité, note 262; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, précité, note 254; J. FRÉCHETTE, précité, note 160, p. 48.

De son côté, en 2009, le GTCVP allait jusqu'à proposer l'interdiction pure et simple de recueillir des renseignements personnels concernant des enfants de moins de 13 ans, et des limites importantes concernant la collecte pendant l'adolescence[299].

4.1.2.1.4 Recours à des interfaces truquées

Les interfaces truquées sont définies par l'Office québécois de la langue française comme des « interface[s] d'un site Internet comportant des astuces ergonomiques destinées à duper les utilisateurs »[300]. De façon plus large, ce terme désigne les éléments de design déployés tant dans les produits que dans les services numériques qui, selon les termes du CEPD, « conduisent les utilisateurs à prendre des décisions non intentionnelles, non volontaires et potentiellement préjudiciables concernant le traitement de leurs données personnelles » et « peuvent entraver leur capacité à protéger efficacement leurs données personnelles et à faire des choix consciencieux »[301].

Les interfaces truquées sont courantes. Par exemple, dans une récente étude des 45 sites Web et 30 applications mobiles les plus populaires en Europe réalisée pour la Commission européenne, un panel de « consommateurs mystères » supervisés par des chercheurs a noté que 97 % des services présentaient au moins une interface truquée[302]. Dans ce cas, étaient considérées comme telles les interfaces pouvant nuire aux droits des consommateurs en général, y compris à leur droit à la vie privée.

L'Annexe 1 de ce rapport présente certains exemples d'interfaces truquées; citons notamment les choix visuels mettant en valeur un accord à la communication de renseignements personnels ou le fait « d'enfouir » les paramètres de confidentialité dans un menu difficile d'accès, nécessitant plusieurs opérations pour être consulté.

Les interfaces truquées sont contraires aux droits fondamentaux des enfants, selon l'UNICEF et la 5Rights Foundation[303] : elles peuvent indûment influencer leurs choix[304] et les mener à partager plus de renseignements personnels qu'ils ne le souhaiteraient, par exemple. Certaines organisations soulignent donc que les entreprises ne devraient pas

---

299 GROUPE DE TRAVAIL DES COMMISSAIRES À LA VIE PRIVÉE ET DES DÉFENSEURS CANADIENS DES ENFANTS ET DES JEUNES SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DES ENFANTS EN LIGNE, précité, note 254, p. 15 et 17 -19.

300 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « interface truquée », *Grand dictionnaire terminologique* (2018), en ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26544648> (consulté le 20 septembre 2020).

301 COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognise and avoid them*, 2022, p. 2, en ligne : <https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf>, notre traduction.

302 Francisco LUPIÁÑEZ-VILLANUEVA, Alba BOLUDA, Francesco BOGLIACINO, Giovanni LIVA, Lucie LECHARDOY 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. 41-60, en ligne : <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418>.

303 J. BYRNE, E. DAY et L. RAFTREE, précité, note 233, p. 20; 5RIGHTS FOUNDATION, précité, note 141, p. 24.

304 Dans l'étude de la Commission européenne (note 302), des expériences comportementales menées auprès de sujets tests indiquent un impact réel de plusieurs types d'interfaces truquées sur les décisions des adultes. Voir F. LUPIÁÑEZ-VILLANUEVA et al., précité, note 302, p. 101-108.

(pouvoir) y avoir recours dans les produits et services susceptibles d'atteindre les moins de 18 ans[305].

4.1.2.2 Obligations légales supplémentaires

D'autres mesures visent à renforcer la responsabilité des entreprises[306] en leur imposant des obligations légales supplémentaires lorsqu'il s'agit de la protection des renseignements personnels des mineurs. Entre autres, elles peuvent être tenues de traiter leurs renseignements comme sensibles, de réaliser des analyses d'impact lorsqu'elles envisagent des projets impliquant des renseignements personnels concernant des mineurs, de vérifier l'âge des utilisateurs qui donnent leur consentement ou la validité du consentement parental ou d'établir par défaut des paramètres élevés de protection des renseignements personnels.

Les obligations peuvent constituer un fardeau pour les entreprises, aussi peut-il être souhaitable de prévoir des critères pour préciser celles qu'elles visent.

4.1.2.2.1 Considérer les renseignements d'enfants comme sensibles

Dans nombre de juridictions, les renseignements sensibles jouissent de protections particulières. On les définit tantôt de manière large, tantôt en faisant une énumération des types de renseignements qui sont inclus dans cette catégorie. Désigner explicitement les renseignements personnels des mineurs comme sensibles peut être une façon de mieux les protéger.

La Commission soulignait dans son rapport quinquennal de 2016 que les renseignements personnels des mineurs pouvaient revêtir un caractère sensible[307]. À la suite d'une enquête sur un incident de sécurité survenu chez le fabricant de jouets connectés VTech, le CPVPC indiquait la même chose[308]. Sur cette base entre autres, Option consommateurs recommande que la Loi sur le privé fasse une mention explicite du caractère sensible des renseignements personnels des mineurs[309].

---

305 COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, précité, note 301; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 5-7; INTERNATIONAL CONSUMER PROTECTION AND ENFORCEMENT NETWORK, précité, note 285, par. 36-43.

306 REVEALING REALITY, précité, note 61, p. 10.

307 COMMISSION D'ACCÈS À L'INFORMATION, *Rétablir l'équilibre*, Québec, 2016, p. 88-89, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf>.

308 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Rapport de conclusions d'enquête en vertu de la LPRPDE nº 2018-001 : Un manufacturier de jouets connectés améliore les mesures de sécurité pour protéger adéquatement les renseignements d'enfants », *Commissariat à la protection de la vie privée du Canada* (8 janvier 2018), en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2018/lprpde-2018-001/> (consulté le 9 décembre 2021).

309 V. MONTCALM, A. PLOURDE et E. THÉRIAULT, précité, note 57, p. 52 et 63.

4.1.2.2.2 Obliger à réaliser une analyse d'impact lorsque des renseignements de mineurs sont impliqués

Dans l'esprit de la protection de la vie privée dès la conception (*privacy by design*), de nombreuses organisations recommandent que les entreprises mènent des analyses d'impact lorsqu'elles planifient des projets impliquant des renseignements personnels de mineurs[310]. Si l'évaluation des facteurs relatifs à la vie privée est un type d'analyse d'impact, la pratique mise de l'avant est généralement la réalisation d'une analyse plus large. Celle-ci permet de prendre en compte non seulement les enjeux de vie privée, mais aussi ceux liés à d'autres droits fondamentaux de l'enfant consacrés dans la Convention – un élargissement de portée utile dans le contexte de l'interrelation entre les risques numériques, comme expliqué dans la section 3.3.

La Commission recommandait un mécanisme semblable dans son mémoire sur le projet de loi nº 64 pour la conception des systèmes d'intelligence artificielle[311]. De son côté, la CDPDJ suggérait que les évaluations des facteurs relatifs à la vie privée soient remplacées par des « évaluations des facteurs relatifs aux droits et libertés de la personne garantis par la Charte »[312].

4.1.2.2.3 Inciter ou obliger à vérifier l'âge et/ou la validité du consentement parental

Plusieurs organisations proposent ou conçoivent que les États incitent ou obligent les entreprises à évaluer la pertinence de vérifier l'âge des utilisateurs lorsque leur produit ou service ne s'adresse vraisemblablement pas qu'à un public adulte[313]. Elles estiment qu'en sachant à qui elles ont affaire, les entreprises pourraient mieux adapter le contenu et les paramètres et solliciter un consentement parental lorsque le mineur n'a pas atteint l'âge du consentement autonome.

Étant donné les enjeux de minimisation de la collecte soulevés par cette mesure, les travaux internationaux recommandent généralement d'user de circonspection dans le choix d'une modalité de vérification d'âge, notamment en adoptant une approche fondée sur le risque[314]. Ainsi, on pourra mieux évaluer la collecte de renseignements personnels supplémentaires en sachant quels sont le degré de probabilité et la gravité potentielle des préjudices auxquels seraient exposés des mineurs n'ayant pas atteint un certain âge en

---

310 Observation générale nº 25, précité, note 11, par. 38; J. BYRNE, E. DAY et L. RAFTREE, précité, note 233, p. 59; UNICEF et MINISTÈRE DES AFFAIRES ÉTRANGÈRES DE LA FINLANDE, précité, note 55, p. 32; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 7; INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, précité, note 254, par. 29 et 33; CONSEIL DE L'EUROPE, précité, note 253, par. 31; REVEALING REALITY, précité, note 61, p. 10.

311 COMMISSION D'ACCÈS À L'INFORMATION, précité, note 62, p. 22.

312 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, précité, note 262, p. 89.

313 Observation générale nº 25, précité, note 11, par. 55 et 114; INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, précité, note 254, par. 21-22; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 6; COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, précité, note 259, par. 132-135; 5RIGHTS FOUNDATION, précité, note 241; REVEALING REALITY, précité, note 61, p. 12-13; INFORMATION COMMISSIONER'S OFFICE, *Information Commissioner's opinion: Age Assurance for the Children's Code*, 2021, p. 16-21, en ligne : <https://ico.org.uk/media/about-the-ico/documents/4018659/age-assurance-opinion-202110.pdf>.

314 Voir par exemple 5RIGHTS FOUNDATION, précité, note 241, p. 19.

utilisant le produit ou le service – cela permettant d'établir le niveau d'exactitude requis pour le système. Le CEPD, par exemple, exprime cette idée en ces termes[315] :

> La vérification de l'âge de la personne concernée ne doit pas entraîner un traitement de données supplémentaire excessif. Le mécanisme choisi pour vérifier l'âge d'une personne concernée devrait comprendre une évaluation des risques liés au traitement envisagé. Dans certaines situations à faible risque, il pourrait être approprié de demander à un nouvel abonné à un service de révéler son année de naissance ou de remplir un formulaire stipulant qu'il est ou n'est pas mineur. En cas de doute, le responsable du traitement devrait réviser ses mécanismes de vérification de l'âge dans un cas donné et évaluer si des méthodes de vérification alternatives sont nécessaires.
>
> [Références omises]

Les mêmes enjeux se posent dans le cas de la vérification de la validité du consentement parental, un deuxième de type de vérification recommandé par certaines organisations à l'international[316]. Dans ce cas, il s'agit pour l'entreprise de s'assurer que le parent qui donne le consentement au nom de l'enfant n'ayant pas atteint l'âge du consentement autonome est bel et bien lié à cet enfant, c'est-à-dire titulaire de l'autorité parentale ou du statut de tuteur par rapport à lui.

Dans tous les cas, l'analyse de l'entreprise doit pouvoir la conduire à évaluer que compte tenu des préjudices potentiels, la vérification d'âge ou la vérification de la validité du consentement parental ne sont pas requises. En effet, d'importants enjeux sont associés à la systématisation de ces pratiques[317], aussi la prudence est-elle de mise. Pour cette raison, certaines organisations ont réalisé des analyses approfondies des tenants et aboutissants de la vérification d'âge et du consentement parental afin de suggérer des approches nuancées[318].

---

315 COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, précité, note 259, par. 135.

316 Observation générale nº 25, précité, note 11, par. 71; CONSEIL DE L'EUROPE, précité, note 253, par. 30; COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, précité, note 259, par. 136-146; INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, précité, note 254, par. 21-22; V. MONTCALM, A. PLOURDE et E. THÉRIAULT, précité, note 57, p. 63.

317 Par exemple, elles peuvent soumettre tant les adultes que les mineurs à des collectes plus étendues de renseignements personnels. La vérification systématique de *l'identité* plutôt que de l'âge ou de la nature de la relation avec le mineur peut aussi mettre en péril la notion d'anonymat en ligne. Le Groupe de travail sur la protection des données dans les télécommunications de l'AMVP recommande d'ailleurs de cheminer vers des systèmes reposant sur des preuves à divulgation nulle de connaissances (*zero-knowledge proof*) afin de n'obtenir que l'information essentielle (par ex. : l'enfant a plus ou moins de 13 ans) : INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, précité, note 254, par. 22.

318 5RIGHTS FOUNDATION, précité, note 241; FUTURE OF PRIVACY FORUM, *The State of Play: Verifiable Parental Consent and COPPA (Discussion draft)*, 2021, en ligne : <https://fpf.org/wp-content/uploads/2021/11/FPF-The-State-of-Play-Verifiable-Parental-Consent-and-COPPA.pdf> (consulté le 6 décembre 2021); INFORMATION COMMISSIONER'S OFFICE, *Age Assurance for the Children's Code*, 2021, en ligne : <https://ico.org.uk/media/about-the-ico/documents/4018659/age-assurance-opinion-202110.pdf>.

4.1.2.2.4 Obliger à établir par défaut des paramètres robustes de protection des renseignements personnels

Afin de maximiser la protection offerte aux mineurs dans l'espace numérique, plusieurs organisations[319] recommandent d'obliger les fournisseurs de produits et de services numériques à :

- Offrir, par défaut, des paramètres offrant le plus haut niveau de protection, par exemple :
  - En désactivant des fonctionnalités à haut risque, comme la géolocalisation ou le profilage[320];
  - En cachant les renseignements du mineur aux autres utilisateurs d'un service numérique[321];
- Prévoir des paramètres précis et granulaires, qui permettent d'ajuster les préférences de façon ciblée plutôt qu'une fois pour toutes les fonctionnalités d'un produit ou service (cette recommandation est également liée au caractère spécifique du consentement).

Le Groupe de travail international sur la protection des données dans les télécommunications de l'AMVP indique de plus que les entreprises ont un devoir de vulgarisation par rapport à l'impact des paramètres de protection[322]. Par exemple, elles gagneraient à expliquer aux parents et aux enfants pourquoi des paramètres de confidentialité élevés par défaut sont importants et à bien souligner les conséquences des changements de paramètres. Le groupe propose aussi qu'un consentement parental soit requis pour tout choix de réglage qui amoindrirait la protection des renseignements personnels.

Par ailleurs, certaines organisations soulignent l'importance d'assurer également la cybersécurité par défaut pour les produits s'adressant aux enfants, notamment les objets connectés (jouets, montres, etc.)[323].

---

[319] ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, précité, note 262, p. 11; INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, précité, note 254, par. 29-36; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 7; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, précité, note 254; REVEALING REALITY, précité, note 61, p. 10.

[320] ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 7.

[321] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, précité, note 254, recommandation 8; INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, précité, note 254, par. 36.

[322] INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, précité, note 254, par. 34 -36.

[323] CONSEIL DE L'EUROPE, précité, note 253, par. 3; Valérie MONTCALM, Alexandre PLOURDE et Elise THÉRIAULT, *Enfants sous écoute – La protection de la vie privée dans l'environnement des jouets intelligents*, Option consommateurs, 2018, p. 62, en ligne : <https://option-consommateurs.org/wp-content/uploads/2018/11/oc-jouets-i-rapport-final.pdf>.

4.1.2.3 Normes ou instruments souples

Enfin, une troisième catégorie de mesures misant sur les entreprises vise à établir des normes ou des instruments souples qui permettent de guider les actions des entreprises de façon plus directe.

Étant donné l'évolution rapide des possibilités technologiques et des pratiques, il n'est ainsi pas toujours possible de prévoir toutes les mesures nécessaires à même la législation. Par ailleurs, pour préserver la neutralité technologique, celle-ci ne peut être extrêmement détaillée.

Afin d'offrir un encadrement plus souple, des organisations proposent donc aux gouvernements ou aux autorités de protection des renseignements personnels d'élaborer des codes de pratiques[324]. Plus flexibles que les lois, ceux-ci peuvent être adaptés et revus plus fréquemment, et permettent également de donner des orientations plus précises aux entreprises. Ils peuvent être conçus en collaboration avec la société civile et d'autres acteurs importants, comme les organismes de protection des droits fondamentaux, et prendre en compte l'opinion des mineurs eux-mêmes via des consultations, dans le respect des principes de la Convention.

Les recommandations faites par les organismes internationaux font référence au modèle du *Children's Code* britannique[325]. L'Information Commissioner's Office (ci-après ICO) du Royaume-Uni, l'homologue de la Commission, a récemment adopté ce code de pratiques en matière de protection des renseignements personnels des enfants. Celui-ci, qui fait école à l'international, est présenté plus en détail à la section 4.2.1.2 et dans l'Annexe 2.

4.1.3 Réaffirmer la primauté des principes de la Convention

Outre les mesures visant les individus et les entreprises, on propose aussi de mieux asseoir les lois sur la protection des renseignements personnels sur les principes de la Convention.

En 2002, la Commission recommandait d'enchâsser dans la Loi sur l'accès une primauté de l'intérêt supérieur de l'enfant lors de l'évaluation des demandes d'accès à son dossier

---

[324] ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 7-8; COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, précité, note 258, p. 27; REVEALING REALITY, précité, note 61, p. 7, 10 et 11. Soulignons que le Commissaire à l'information et à la vie privée de la Colombie-Britannique, Michael McEvoy, préconise aussi une solution de ce genre pour mieux protéger les renseignements personnels des mineurs dans la province : Jeremy HAINSWORTH, « B.C. commissioner mulling over privacy code for children », *Vancouver Is Awesome* (22 mars 2022), en ligne : <https://www.vancouverisawesome.com/highlights/bc-commissioner-mulling-over-privacy-code-for-children-5182227> (consulté le 25 avril 2022).

[325] 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>.

par une personne y ayant droit[326]. Cette mesure visait à protéger l'enfant dans les cas où l'intérêt de ses parents pouvait être contraire au sien[327].

Cette situation peut encore se produire dans les juridictions où les lois donnent aux parents la responsabilité de consentir au nom de leurs enfants en dessous d'un certain seuil d'âge, comme le soulignait la CDPDJ dans son mémoire sur le projet de loi nº 64[328]. Soutenant que ces principes sont déjà intégrés notamment dans le *Code civil du Québec* et dans la *Loi sur la protection de la jeunesse*[329], la CDPDJ réitérait sa recommandation[330] de reconnaître, dans la Loi sur le privé et dans la Loi sur l'accès, l'intérêt supérieur de l'enfant, mais aussi le droit de celui-ci d'être entendu.

Ces ajouts permettraient non seulement de clarifier la pondération des intérêts dans certaines situations conflictuelles entre individus, mais donneraient également le ton aux organisations en ce qui concerne les décisions ayant un impact sur la protection des renseignements personnels des mineurs. Plusieurs organisations rappellent elles aussi la primauté à accorder à l'intérêt supérieur de l'enfant[331] et à son droit d'exprimer son opinion dans les affaires le concernant[332].

4.2 Mesures mises en œuvre ou envisagées dans la législation

À travers le monde, différents textes législatifs déjà en vigueur ou actuellement à l'étude concrétisent une partie des recommandations évoquées dans la section 4.1. En fonction des références faites à certaines juridictions dans les textes consultés ou de l'actualité législative, la Commission a sélectionné les lois suivantes pour une lecture approfondie :

---

326 COMMISSION D'ACCÈS À L'INFORMATION, *Une réforme de l'accès à l'information : le choix de la transparence*, 2002, p. 67, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_RQ_2002.pdf>. Voir aussi p. 59 de ce rapport.

327 Cette situation n'est pas que théorique. Dans une décision récente, la Commission a pris en compte cette notion dans l'analyse du préjudice qui serait causé à un enfant (un mineur de moins de 14 ans) si son père, faisant l'objet d'allégations d'agression sexuelle à son endroit, obtenait le droit d'accéder au rapport final d'une sexologue à la suite d'une thérapie suivie par l'enfant. Voir *X c. Centre d'expertise Marie-Vincent*, par. 46 et suivants, en ligne : <https://www.canlii.org/fr/qc/qccai/doc/2021/2021qccai203/2021qccai203.html>.

328 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, précité, note 262, p. 83-84.

329 *Loi sur la protection de la jeunesse*, RLRQ, c. P-34.1.

330 Claire BERNARD, *Les droits de l'enfant et des parents sur les dossiers qui concernent l'enfant : exposé descriptif*, Cat. 2. 176.5, Commission des droits de la personne et des droits de la jeunesse, 2003, p. 8, en ligne : <https://www.cdpdj.qc.ca/Publications/droits_enfants_parents_expose.pdf>.

331 J. BYRNE, E. DAY et L. RAFTREE, précité, note 233, p. 59-60; Observation générale nº 25, précité, note 11, par. 12-13; ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, précité, note 262, p. 8; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 5 et 7.

332 Observation générale nº 25, précité, note 11, par. 17, 18, 43 et 49; ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, précité, note 235, p. 5; ARTICLE 29 DATA PROTECTION WORKING PARTY, précité, note 268, p. 7.

#	Juridiction	Législation	Abréviation	Statut
1	Union européenne	*Règlement général sur la protection des données*[333]	RGPD	En vigueur
2	Union européenne	*Législation sur les services numériques*[334]	LSN	À l'étude[335]
3	Union européenne	*Législation sur l'intelligence artificielle*[336]	LIA	À l'étude
4	Royaume-Uni	*Data Protection Act 2018*[337]	DPA18	En vigueur
5	États-Unis (fédéral)	*Children's Online Privacy Protection Act*[338]	COPPA	En vigueur
6	États-Unis (fédéral)	*Kids' Online Safety Act*[339]	KOSA	À l'étude
7	Californie	*California Age-Appropriate Design Code Act*[340]	CAADCA	À l'étude
8	Colorado	*Colorado Privacy Act*[341]	CPA	Adopté
9	Washington (État)	*Washington Privacy Act*[342]	WPA	À l'étude
10	Canada (fédéral)	*Loi de 2022 sur la mise en œuvre de la Charte du numérique* (projet de loi C-27)[343]	C-27	À l'étude

[333] RGPD.

[334] *Proposition de Législation sur les services numériques*, 2020/0361 (COD) (1 février 2022), Conseil de l'Union européenne, en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CONSIL:ST_5620_2022_INIT&from=EN> (version consolidée temporaire du 11 février 2022).

[335] La LSN a été adoptée par le Parlement européen le 5 juillet 2022. Sa version finale sera publiée au Journal officiel de l'Union européenne à l'automne 2022. Voir « Procédure 2020/0361/COD », *EUR-Lex* (2020), en ligne : <https://eur-lex.europa.eu/legal-content/fr/HIS/?uri=COM:2020:825:FIN#> (consulté le 5 juillet 2022); COMMISSION EUROPÉENNE, « Digital Services Package: Commission welcomes the adoption by the European Parliament of the EU's new rulebook for digital services », *Commission européenne* (5 juillet 2022), en ligne : <https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_4313> (consulté le 5 juillet 2022).

[336] *Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union*, 2021/0106 (COD) (21 avril 2021), Commission européenne, en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0206&from=EN>.

[337] *Data Protection Act 2018*, 2018, c. 12, en ligne : <https://www.legislation.gov.uk/ukpga/2018/12> (consulté le 18 janvier 2022).

[338] *Children's Online Privacy Protection Act*, 15 U.S.C. c. 91 / 6501-6506, en ligne : <https://www.govinfo.gov/content/pkg/USCODE-2019-title15/html/USCODE-2019-title15-chap91.htm>.

[339] Richard BLUMENTHAL, *Kids Online Safety Act*, projet de loi n° S.3663, 117e (Sénat des États-Unis), en ligne : <https://www.congress.gov/bill/117th-congress/senate-bill/3663/text>.

[340] *Bill Text - AB-2273 The California Age-Appropriate Design Code Act.*, projet de loi n° AB2273 (16 février 2022), 2021-22 (Législature de Californie), en ligne : <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273> (version amendée du 26 avril 2022).

[341] *Colorado Privacy Act*, SB21-190, en ligne : <https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf>.

[342] *Establishing data privacy protections to strengthen a consumer's ability to access, manage, and protect their personal data*, projet de loi n°SB5813 (2021), 67e législature (Législature de l'État de Washington), en ligne : <https://app.leg.wa.gov/billsummary?BillNumber=5813&Initiative=false&Year=2021>.

[343] 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*

#	Juridiction	Législation	Abréviation	Statut
11	Ontario	Livre blanc sur une éventuelle loi provinciale sur la protection des renseignements personnels dans le secteur privé[344]	LBO	En projet
12	Inde	*Personal Data Protection Bill 2019*[345]	PDPB	Abandonné[346]
13	Brésil	*Lei Geral de Proteção de Dados Pessoais*[347]	LGPD	En vigueur

Les lois sur la protection des renseignements personnels de l'Australie[348], de la Nouvelle-Zélande[349], de la Colombie-Britannique[350] et de l'Alberta[351] ont aussi été consultées, mais elles ne contiennent pas de dispositions précises concernant les enfants, hormis des précisions sur l'âge auquel les droits peuvent être exercés de façon autonome. Tout au plus, la loi néo-zélandaise prévoit que le fait qu'une personne soit mineure doit faire partie des éléments analysés lors de l'examen du principe de loyauté/d'équité (*fairness*)[352].

Le tableau présenté à la page suivante constitue une synthèse des différentes mesures *spécifiques aux mineurs* proposées ou mises en place dans les textes législatifs consultés. 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

---

l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois, projet de loi n°C-27 (16 juin 2022), 44e lég., 1re sess. (Chambre des communes), en ligne : <https://www.parl.ca/DocumentViewer/fr/44-1/projet-loi/C-27/premiere-lecture>.

344 GOUVERNEMENT DE L'ONTARIO, précité, note 267.

345 *The Personal Data Protection Bill 2019*, projet de loi n°373-2019, 17e (Lok Sabha), en ligne : <https://prsindia.org/files/bills_acts/bills_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf>; voir la version amendée par le comité parlementaire JOINT COMMITTEE ON THE PERSONAL DATA PROTECTION BILL, 2019, *Report of the Joint Committee on the Personal Data Protection Bill, 2019*, Lok Sabha, 2021, en ligne : <https://www.ahlawatassociates.com/wp-content/uploads/2021/12/17-Joint-Committee-on-the-Personal-Data-Protection-Bill-2019.pdf> (consulté le 2 février 2022).

346 En août 2022, l'Inde a abandonné le PDPB, indiquant toutefois qu'un nouveau projet verrait le jour prochainement; Manish SINGH, « India withdraws personal data bill that alarmed tech giants », *TechCrunch* (4 août 2022), en ligne : <https://techcrunch.com/2022/08/03/india-government-to-withdraw-personal-data-protection-bill/> (consulté le 11 août 2022).

347 *Lei Geral de Proteção de Dados Pessoais*, loi nº 13.709 du 14 août 2018, en ligne : <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>; version anglaise : Ronaldo LEMOS, « Brazilian General Data Protection Law (LGPD, English translation) », *IAPP* (octobre 2020), en ligne : <https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/> (consulté le 28 avril 2022).

348 « Children and young people », *Office of the Australian Information Commissioner*, en ligne : <https://www.oaic.gov.au/privacy/your-privacy-rights/children-and-young-people> (consulté le 28 avril 2022).

349 « How does the Privacy Act deal with children and teenagers? », *New Zealand Privacy Commissioner*, en ligne : <https://privacy.org.nz/tools/knowledge-base/view/2> (consulté le 28 avril 2022).

350 *Personal Information Protection Act*, SBC 2003, c. 63, en ligne : <https://www.bclaws.ca/civix/document/id/complete/statreg/03063_01>. Voir aussi la note de bas de page 323 de ce rapport.

351 *Personal Information Protection Act*, S.O.A. 2003, c. P-6.5, en ligne : <https://www.qp.alberta.ca/documents/Acts/P06P5.pdf>.

352 « Principle 4 - Manner of collection », *New Zealand Privacy Commissioner*, en ligne : <https://www.privacy.org.nz/privacy-act-2020/privacy-principles/4/> (consulté le 28 avril 2022).

indication sur l'étendue des mesures implantées ou envisagées dans chaque régime et l'interaction entre elles.

Les pages subséquentes donnent plus de détails sur chacun des textes législatifs examinés. Dans plusieurs cas, les dispositions générales qui visent toute personne concernée peu importe son âge ne sont pas mentionnées, puisque ce rapport s'intéresse aux mesures particulières de protection des mineurs.

		Loi ou projet de loi												
		RGPD	LSN	LIA	DPA18	COPPA	KOSA	CAADCA	CPA	WPA	C-27	LBO	PDPB	LGPD
#	Mesures	1	2	3	4	5	6	7	8	9	10	11	12	13
A	Consentement parental jusqu'à un âge X	13-16	RGPD	RGPD	13	13	COPPA	CERT CCPA	13	13	PART	13-16	18	18
B	Adaptation des informations données à l'âge de l'enfant													
C	Droit au déréférencement													
D	Droit à la suppression							CCPA					CERT	
E	Interdiction (totale ou partielle) du profilage/des décisions automatisées	POT			CC			PART						
F	Interdiction (totale ou partielle) de la publicité ciblée							POT		SENS				
G	Interdiction (totale ou partielle) d'utiliser les RP d'enfants à des fins nuisibles				CC		IND							
H	Interdiction (totale ou partielle) d'utiliser des interfaces truquées				CC					CERT				
I	Interdiction (totale ou partielle) de communiquer les RP d'enfants				CC						IND			
J	Désignation explicite des RP d'enfants comme sensibles													
K	Réalisation d'une analyse d'impact si des RP d'enfants sont impliqués	LAPD			CC		IND							
L	Vérification d'âge par les fournisseurs de services	POT			CC									
M	Paramètres les plus protecteurs des RP par défaut													
N	Mise en place d'un code de pratiques		PART											
O	Mention de l'intérêt supérieur de l'enfant	IND			CC									

Légende

Chaque texte législatif a un acronyme/numéro issu de la liste de la page 68. Les mesures sont identifiées par des lettres stylisées (ex. A) pour faciliter les références faites dans la suite de l'avis. **Pour faciliter la navigation, les cases du tableau et les lettres dans le texte sont cliquables dans la version électronique de ce rapport.**

	Prévu dans la loi
	Potentiellement/partiellement
	Prévu ailleurs
CC	*Children's Code*
CCPA	*California Consumer Privacy Act*
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

4.2.1 Europe

Les règlements adoptés à l'échelle européenne ont souvent une résonnance internationale, du fait qu'ils s'appliquent à près d'une trentaine de pays comptant 450 millions d'habitants[353]. Ces dernières années, l'Union européenne a d'ailleurs adopté ou considéré des textes législatifs mettant en œuvre plusieurs dispositions concernant la protection des mineurs et de leurs renseignements personnels dans le monde numérique. Par ailleurs, cette question occupe également beaucoup de place dans la société britannique; le Royaume-Uni a donc lui aussi été étudié dans le cadre de la réalisation de ce rapport.

4.2.1.1 Union européenne

Le RGPD, qui est en vigueur depuis 2018, contient plusieurs références aux mineurs, tant dans ses considérants que dans ses dispositions. Il vise toutes les organisations, y compris les entreprises[354], et définit les renseignements personnels de façon large[355].

Le préambule explique que les enfants[356] ont besoin d'une protection particulière en ce qui a trait à leurs renseignements personnels[357] :

> (38) Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. […]

Ce souci se reflète également dans les considérants 58 (adaptation des informations pour les enfants), 65 (droit à l'oubli et à la suppression) et 71 (profilage et décisions automatisées). Conséquemment, les dispositions du RGPD prévoient plusieurs mesures de protection :

#	Détails
A	Les « services de la société de l'information » (produits et services numériques, pour simplifier) qui traitent des renseignements personnels en se fondant sur la base juridique du consentement[358] doivent obtenir le consentement d'un parent si l'enfant a moins de 16 ans. Cet âge peut être abaissé par des législations nationales, mais ne peut pas être inférieur à 13 ans[359].

353 « Vivre dans l'Union européenne: faits et chiffres », *Site de l'Union européenne*, en ligne : <https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/life-eu_fr> (consulté le 28 avril 2022).

354 RGPD, art. 2.

355 *Id.*, art. 4 (1).

356 Le RGPD ne contient aucune définition du terme « enfant ».

357 RGPD, considérant 38.

358 *Id.*, art. 6 (1) (a).

359 *Id.*, art. 8.

#	Détails
B	L'information fournie aux personnes concernées doit être concise, transparente, compréhensible, accessible et formulée en des termes simples et clairs, en particulier pour les enfants[360].
C D	Le RGPD prévoit un droit à la suppression des renseignements personnels suivant certaines situations[361]. Les entreprises doivent effacer ces renseignements et les déréférencer s'ils étaient diffusés publiquement[362].
E	Le considérant 71 du RGPD mentionne que le profilage et les décisions automatisées ne devraient pas concerner les enfants. Cependant, cette précision ne se retrouve pas dans le texte de loi lui-même. Le Comité européen de la protection des données estime toutefois dans ses lignes directrices sur la prise de décision automatisée et le profilage que bien que ces derniers ne soient pas interdits lorsqu'ils visent des enfants, les situations où ils sont légitimes devraient être très limitées[363].
K	Le RGPD prévoit la réalisation d'analyses d'impact sur la protection des données dans les cas où les traitements posent des risques particuliers pour les droits des personnes[364]. Des listes élaborées par les autorités nationales de protection des données prévoient certains cas où de telles analyses sont obligatoires. Dans plusieurs juridictions européennes, c'est le cas pour les projets impliquant des renseignements personnels de mineurs[365].
L	La mention d'un âge de consentement au traitement des renseignements personnels dans le RGPD suppose que des mécanismes de vérification d'âge soient mis en place, comme le rappelle le Comité européen de la protection des données dans ses lignes directrices sur le consentement[366]. Toutefois, il ne s'agit pas d'une exigence légale. Le projet euConsent, lancé récemment, vise à harmoniser les pratiques de vérification d'âge à l'échelle européenne[367]. Par ailleurs, compte tenu des technologies disponibles, les entreprises doivent investir des efforts raisonnables pour vérifier qu'un consentement parental est bien donné par une personne qui exerce la responsabilité parentale par rapport à un mineur donné[368].
M	Les entreprises doivent prévoir des mesures appropriées pour assurer la protection des renseignements personnels par défaut[369]. Par exemple, les

360 *Id.*, art. 12 (1).

361 *Id.*, art. 17 (1).

362 *Id.*, art. 17 (2).

363 COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, précité, note 283, p. 31-33.

364 RGPD, art. 35.

365 Voir par exemple la liste de l'autorité italienne, au point 6 : GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto*, 2018, en ligne : <https://www.gpdp.it/documents/10160/0/ALLEGATO+1+Elenco+delle+tipologie+di+trattamenti+soggetti+al+meccanismo+di+coerenza+da+sottoporre+a+valutazione+di+impatto.pdf/b9ceefa9-dd65-df86-fed4-df3c3570f59d?version=1.11>.

366 COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, précité, note 259, par. 132-135.

367 « euConsent: Electronic Identification and Trust Services for Children in Europe », *euConsent* (2021), en ligne : <https://euconsent.eu/> (consulté le 29 avril 2022).

368 RGPD, art. 8 (2).

369 *Id.*, art. 25.

#	Détails
	paramètres doivent empêcher que des renseignements personnels soient rendus accessibles à un nombre indéterminé d'autres personnes sans intervention concrète de la personne concernée[370].
O	Lorsque les entreprises se fondent sur leur « intérêt légitime » pour traiter des renseignements personnels, elles doivent s'assurer que les intérêts et les droits fondamentaux de la personne concernée ne prévalent pas, en particulier s'il s'agit d'un enfant[371].

Par ailleurs, le RGPD donne aux autorités de contrôle le mandat de veiller à la « sensibilisation du public et [à] sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement », en précisant que « [l] es activités destinées spécifiquement aux enfants font l'objet d'une attention particulière »[372].

Le RGPD est la loi maîtresse en matière de protection des renseignements personnels en Europe, mais deux projets de législation déposés en 2020 par la Commission européenne pourraient changer la donne en ce qui concerne la protection particulière des mineurs : la LSN et la LIA.

La LSN vise à encadrer les services numériques afin d'assurer le respect des droits fondamentaux, des droits des consommateurs et de la saine concurrence. À la date de finalisation du présent rapport, le texte législatif fait l'objet d'un accord politique[373], mais doit encore être entériné par les instances de l'Union européenne. D'application large, il prévoit des obligations pour tous les intermédiaires qui fournissent des services en Europe (ex. réseaux sociaux, hébergeurs infonuagiques, places de marché, etc.), avec un fardeau proportionnel à l'importance des entreprises. Selon la dernière version consolidée disponible du texte et les informations relayées à la suite de l'accord politique, la LSN contiendra les mesures de protection suivantes à l'égard des mineurs, dont il souligne la prédominance de l'intérêt supérieur[374] :

- Les entreprises devront adapter les informations fournies à l'âge des utilisateurs[375] (B);
- Il sera interdit d'utiliser les renseignements personnels des mineurs de moins de 16 ans pour leur présenter des publicités ciblées[376] (F).
- Il sera interdit d'utiliser des interfaces truquées[377] (H);

[370] *Id.*

[371] *Id.*, art. 6 (1) (f).

[372] *Id.*, art. 57 (1) (a).

[373] « Législation sur les services numériques: accord provisoire entre le Conseil et le Parlement pour faire de l'internet un espace plus sûr pour les citoyens européens », *Conseil de l'Union européenne* (23 avril 2022), en ligne : <https://www.consilium.europa.eu/fr/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/> (consulté le 29 avril 2022).

[374] LSN, considérant 3.

[375] *Id.*, art. 12.

[376] *Id.*, art. 24.

[377] *Id.*, art. 13.

- Les très grandes plateformes devront réaliser des analyses pour identifier les risques systémiques que posent leurs activités, notamment au regard de la protection des mineurs, et cibler des stratégies d'atténuation[378] (𝕂);
- Les entreprises devront adapter la conception de leurs fonctionnalités pour assurer un haut niveau de confidentialité et de sécurité par défaut pour les mineurs[379] (𝕄);
- La Commission européenne soutiendra le développement de normes volontaires sur la protection des mineurs par les organismes européens et internationaux de standardisation[380] (ℕ).

La LIA, quant à elle, vise à encadrer l'utilisation de l'intelligence artificielle de manière générale. Celle-ci étant souvent mise à contribution dans les systèmes de profilage ou de prise de décision automatisée, les nouvelles dispositions pourraient avoir un impact sur les mineurs. Entre autres, le projet de législation, toujours à l'étude, prévoit :

- L'interdiction des systèmes d'intelligence artificielle utilisant des techniques subliminales ou exploitant des vulnérabilités liées à l'âge pour susciter des comportements susceptibles de causer un préjudice physique ou psychologique à la personne concernée[381] (𝔾);
- Dans le processus de gestion des risques liés aux systèmes d'intelligence artificielle à haut risque, tenir compte de la probabilité qu'ils aient un impact sur les enfants ou que ceux-ci puissent y accéder[382] (𝕂).

4.2.1.2 Royaume-Uni

La loi sur la protection des renseignements personnels du Royaume-Uni, la DPA18, est une adaptation nationale du RGPD. Elle a été élaborée avant que le pays ne quitte l'Union européenne. Par conséquent, elle prévoit les mêmes protections que celles décrites dans la section 4.2.1.1 pour ce qui est du RGPD[383].

Toutefois, avant son adoption, la baronne Beeban Kidron, qui dirige également la 5Rights Foundation, a soumis des amendements visant à mandater l'Information Commissioner's Office (ICO) pour réaliser un code de pratiques contraignant visant la conception des « services de la société de l'information » auxquels les mineurs (**de moins de 18 ans**) sont susceptibles d'avoir accès[384] (ℕ). Ces amendements ayant été intégrés à la loi[385], le

---

[378] *Id.*, art. 26.

[379] *Id.*, art. 13a (3).

[380] *Id.*, art. 34 (1a).

[381] LIA, art. 5 (1), points (a) et (b).

[382] *Id.*, art. 9 (8); voir aussi considérant 28.

[383] Le 18 juillet 2022, le pays a toutefois déposé un projet de loi sur la refonte du DPA18, vu la sortie de l'Union européenne : *Data Protection and Digital Information Bill*, projet de loi n° 143 2022-23, 2022-2023 (Chambre des communes du Royaume-Uni), en ligne : <https://bills.parliament.uk/bills/3322>.

[384] « Age Appropriate Design Code, Data Protection Bill », *5Rights Foundation* (s.d.), en ligne : <https://5rightsfoundation.com/in-action/blog-age-appropriate-design-code-data-protection-bill.html> (consulté le 29 avril 2022).

[385] DPA18, art. 123-126.

ICO a donc rédigé et publié le *Age appropriate design code*, aussi connu sous le nom de *Children's Code*[386], qui est en vigueur depuis septembre 2020. Des consultations élargies ont accompagné le processus de rédaction, qui s'est échelonné sur 2 ans.

Ce code s'adresse essentiellement aux fournisseurs de produits et de services numériques qui sont susceptibles d'affecter les enfants, comme les applications, les logiciels, les jouets et les objets connectés, les moteurs de recherche, les jeux en ligne, les sites éducatifs ou informatifs, etc.[387]. Il vise à protéger les enfants *au sein* du monde numérique, et non pas *contre* celui-ci[388]. Ses 15 principes (présentés dans l'Annexe 2) constituent des obligations supplémentaires de protection des mineurs que ces fournisseurs doivent mettre en place. Le ICO peut tenir compte du non-respect du *Children's Code* au moment de faire enquête sur l'application du DPA18, et ajuster d'éventuelles sanctions en conséquence[389]. Autrement dit, le code de pratiques a un caractère quasi réglementaire[390].

Les principes du *Children's Code* complètent la DPA18. Dans le respect du principe de l'évolution des capacités consacré par la Convention, ceux-ci doivent être appliqués en tenant compte des tranches d'âge précises dans lesquelles se trouvent les enfants potentiellement visés[391]. Parmi les effets du code de pratiques, notons les précisions et ajouts suivants par rapport au DPA18 :

- Le profilage doit être désactivé par défaut, sauf rares exceptions, et ne doit être mis en place qu'avec des garanties appropriées pour protéger les mineurs des préjudices (surtout liés au contenu). Dans la plupart des cas, à moins qu'il ne constitue lui-même la caractéristique essentielle du service, le profilage devrait être paramétrable[392] (E);
- Les entreprises ne peuvent utiliser les renseignements personnels d'une façon qui nuit au bien-être des mineurs (de façon démontrée), ou qui contrevient à d'autres normes ou codes[393] (G, potentiellement F);
- Les entreprises ne peuvent utiliser des interfaces qui influencent indûment ses choix[394] (H);
- En général, les renseignements personnels de mineurs ne peuvent être communiqués à des tiers, sauf si leur intérêt supérieur le justifie[395] (I);
- Dans leurs analyses d'impact sur la protection des renseignements personnels, les entreprises doivent tenir compte plus largement des risques de l'utilisation

386 *Children's code*, précité, note 325.
387 *Id.*, p. 14.
388 *Id.*, p. 3.
389 DPA18, art. 127.
390 Il est également déposé au parlement britannique : *Id.*, art. 125.
391 *Children's code*, précité, note 325, p. 31 et suivantes.
392 *Children's code*, précité, note 325, principe 12.
393 *Id.*, principe 5.
394 *Id.*, principe 13.
395 *Id.*, principe 9.

projetée des renseignements personnels pour les droits du mineur au sens large (ex. à l'autonomie, à l'information, au bien-être, etc.)[396] (K);

- Pour savoir comment appliquer le *Children's Code*, les entreprises doivent soit vérifier l'âge des utilisateurs de leurs produits ou services, dans le respect des principes de protection des renseignements personnels, soit appliquer les principes du code à tous les utilisateurs sans égard à leur âge[397] (L);
- L'ensemble du *Children's Code* existe pour favoriser l'intérêt supérieur de l'enfant. Ce principe est à la base de tous les autres, et doit être considéré à toutes les étapes de conception d'un produit ou service numérique[398] (O).

Par ailleurs, le *Children's Code* précise plusieurs aspects liés à la transparence des pratiques pour les enfants, aux paramètres par défaut, aux contrôles parentaux ou à l'exercice des droits[399].

De l'avis de l'actuel commissaire du ICO, la communauté internationale gagnerait à développer des outils comme le *Children's Code* à une échelle plus globale, afin d'homogénéiser la protection dont bénéficient les mineurs à travers le monde dans l'environnement numérique[400]. Pour cette raison, le ICO appuie l'initiative californienne de la CAADCA (voir la section 4.2.2.1.2.1) et informe d'autres juridictions sur la mise en place de codes similaires.

Soulignons par ailleurs que le Royaume-Uni étudie actuellement un projet de loi d'application plus large, le *Online Safety Bill*[401], qui imposerait des normes supplémentaires aux entreprises numériques visant à assurer la sécurité en ligne. Entre autres, elles auraient un devoir de vigilance à l'égard des mineurs[402]. Ce projet de loi porte toutefois de manière prédominante sur le *contenu* hébergé en ligne plutôt que sur les renseignements personnels.

4.2.2 Amérique du Nord

Hors du Québec, jusqu'à récemment, peu de lois prévoyaient des dispositions étendues concernant la protection des renseignements personnels des mineurs, mais le vent tourne. Aux États-Unis, plusieurs nouveaux textes de loi, à l'échelle fédérale ou étatique, s'attaquent à cette question; au Canada, l'Ontario envisage une loi provinciale incluant

396 *Id.*, principe 2.

397 *Id.*, principe 3.

398 *Id.*, principe 1.

399 *Id.*, principes 4, 6, 7, 11 et 15.

400 John EDWARDS, « Blog: Why protecting children online in UK living rooms starts 5,000 miles away », *Information Commissioner's Office* (11 avril 2022), en ligne : <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2022/04/why-protecting-children-online-in-uk-living-rooms-starts-5-000-miles-away> (consulté le 10 mai 2022).

401 *Online Safety Bill*, projet de loi n° 004 2022-23, 2022-2023 (Chambre des communes du Royaume-Uni), en ligne : <https://bills.parliament.uk/bills/3137/publications>.

402 *Id.*, art. 10, 11, 25, 26, 31, 32, 33 et 53.

des protections pour les mineurs, et le gouvernement fédéral vient de déposer un projet de loi pour réformer la protection des renseignements personnels dans le secteur privé.

4.2.2.1 États-Unis

Aux États-Unis, à l'échelle fédérale, une loi spécifique à la protection des mineurs en ligne, la COPPA, a été adoptée en 1998 pour répondre aux enjeux liés à la vie privée des enfants qui se dessinaient avec l'expansion d'Internet[403]. D'autres initiatives récentes visent à la bonifier.

Le paysage de la protection des renseignements personnels aux États-Unis est toutefois de plus en plus morcelé : en l'absence de cadre fédéral américain d'application générale, les États adoptent de plus en plus de lois locales dans ce domaine. Quelques textes législatifs étatiques ont donc aussi été consultés.

4.2.2.1.1 Échelle fédérale

La COPPA assujettit les fournisseurs de services en ligne qui s'adressent aux mineurs de moins de 13 ans[404] – elle ne s'applique pas lorsque ces services visent la population générale, *y compris* les enfants[405]. Elle définit également les renseignements personnels de façon très restreinte : seuls sont concernés des identifiants précis, comme le nom, l'adresse, le courriel ou le numéro de téléphone, ou certains renseignements comme les photos ou les vidéos[406]. Pour l'essentiel, les renseignements qui peuvent être observés ou inférés sont donc hors portée.

La protection imposée par la COPPA repose surtout sur le mécanisme du consentement parental (A): pour recueillir des renseignements personnels concernant des enfants de moins de 13 ans, les entreprises doivent obtenir le consentement d'un parent[407]. Elles ont des obligations liées à la vérification de la validité de ce consentement, ce qui génère un certain nombre de problèmes d'application concrète[408], qui ont parfois pu mener à l'exclusion pure et simple des moins de 13 ans de plusieurs services en ligne[409]. Si le consentement n'est pas donné, le service peut être refusé à l'enfant[410]. En outre, les entreprises doivent :

---

403 FUTURE OF PRIVACY FORUM, précité, note 318, p. 6 -11.

404 Vu l'ancienneté de la COPPA et son applicabilité sur le territoire américain, où opèrent bon nombre de fournisseurs de services en ligne, ce seuil d'âge s'est graduellement établi comme un standard international. Il résulterait toutefois d'un compromis politique, puisque les premières versions de la COPPA le fixaient à 18, puis à 16 ans. Voir Milda MAČĖNAITĖ et Eleni KOSTA, « Consent for processing children's personal data in the EU: following in US footsteps? », (2017) 26-2 *Information & Communications Technology Law* 146-197, p. 182-185, DOI : 10.1080/13600834.2017.1321096.

405 COPPA, art. 6501 (1), (2) et (10).

406 *Id.*, art. 6501 (8); V. MONTCALM, A. PLOURDE et E. THÉRIAULT, précité, note 57, p. 55.

407 COPPA, art. 6501 (1), (2) et (10).COPPA, article 6502; FPF-01; GTCVP-01, p. 13-14; OC-01, p. 54-56.

408 Voir FUTURE OF PRIVACY FORUM, précité, note 318.

409 S. VAN DER HOF, précité, note 39, p. 114, note 61.

410 COPPA, art. 6502 (b) (3).

- Prévoir une politique de confidentialité, qui n'est pas nécessairement adaptée aux mineurs[411];
- Mettre en place des mesures de sécurité pour protéger les renseignements personnels des mineurs[412];
- Supprimer les renseignements personnels du mineur de moins de 13 ans à la demande d'un parent[413] (D).

La COPPA est complétée par un règlement d'application qui précise entre autres les mécanismes de vérification du consentement parental qui sont acceptables[414].

Plusieurs tentatives de bonifier la COPPA ont été faites au fil des ans. Récemment, des sénateurs ont déposé la KOSA, qui est toujours à l'étude. Celle-ci entend s'attaquer en général aux effets nuisibles du numérique sur les mineurs. Elle viserait les services électroniques commerciaux utilisés, ou susceptibles de l'être, par les mineurs de moins de 16 ans[415]. En plus d'obligations importantes de transparence[416], les mesures suivantes sont proposées pour renforcer la protection qui leur est offerte :

- Les entreprises doivent adapter les libellés des informations et des paramètres à l'âge des mineurs[417] (B);
- Des options facilement accessibles doivent permettre de supprimer un compte ou de demander l'effacement des renseignements personnels[418] (D);
- Les services numériques doivent prévoir des paramètres permettant entre autres de masquer le profil du mineur aux autres utilisateurs, de désactiver les fonctionnalités qui encouragent un engagement temporel accru et de désactiver les recommandations algorithmiques (G);
- Une fois par année, les entreprises doivent diffuser publiquement les résultats d'un audit des risques systémiques pour les mineurs, lequel comprend des mesures correctives[419] (K);
- Vu la complexité de la vérification d'âge, la loi prévoit la réalisation prochaine d'une recherche menée par différentes instances fédérales pour évaluer les meilleures options technologiques en tenant compte de la protection des renseignements personnels[420] (L);

---

411 *Id.*, art. 6502 (b) (1) (A) (i).
412 *Id.*, art. 6502 (b) (1) (D).
413 *Id.*, art. 6502 (b) (1) (A) (ii).
414 *Children's Online Privacy Protection Rule*, 16 CFR Part 312, en ligne : <https://www.ecfr.gov/current/title-16/part-312> (consulté le 11 janvier 2022).
415 KOSA, art. 2.
416 *Id.*, art. 5.
417 *Id.*, art. 4 (a) (3).
418 *Id.*, art. 4 (a) (1)(E).
419 *Id.*, art. 6.
420 *Id.*, art. 9.

- Les paramètres prévus doivent, par défaut, être réglés à l'option la plus protectrice pour les utilisateurs mineurs[421] (Ⓜ);
- Les entreprises ont le devoir d'agir dans l'intérêt supérieur de l'enfant et ont la responsabilité d'intervenir pour éviter les risques de préjudices physiques, émotionnels, développementaux ou matériels aux mineurs, dont plusieurs reflètent la typologie présentée dans la section 3.3.1[422] (Ⓞ).

4.2.2.1.2 Échelle étatique

Du côté des États, la Californie, le Colorado et l'État de Washington ont récemment adopté ou étudient actuellement des textes législatifs comportant des mesures visant spécifiquement les mineurs. Si d'autres États comme la Virgine, le Connecticut ou l'Utah ont également adopté récemment des lois sur la protection des renseignements personnels, celles-ci n'ont pas de particularités suffisamment importantes pour être considérées séparément dans le cadre de ce rapport.

4.2.2.1.2.1 Californie

De ces trois États, c'est la Californie – territoire où sont basées nombre de grandes entreprises du numérique – qui envisage actuellement l'encadrement le plus complet. Une loi d'application générale, la *California Consumer Privacy Act*[423] (la CCPA), prévoit déjà certaines protections : entre autres, les entreprises ne peuvent vendre ou partager les renseignements personnels d'un mineur de moins de 16 ans, sauf si celui-ci a donné son consentement explicite (s'il a plus de 13 ans) ou si son parent l'a exprimé en son nom (s'il a moins de 13 ans)[424] (Ⓐ). Les personnes concernées peuvent aussi demander la suppression des renseignements personnels qu'ils ont fournis[425] (Ⓓ). Ce droit à la suppression sera étendu aux renseignements recueillis auprès de tiers et inférés[426] lors de l'entrée en vigueur des modifications de la *California Privacy Rights Act*[427], une loi qui accroît la portée de la CCPA.

---

421 *Id.*, art. 4 (a) (2).

422 *Id.*, art. 3.

423 *California Consumer Privacy Act of 2018*, code civil de la Californie, 1798.100 - 1798.199.100, en ligne : <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5>.

424 *Id.*, art. 1798.120.

425 « Does the "right to be forgotten" under the California Consumer Privacy Act require that companies delete the same type of information as the "right to be forgotten" under the GDPR? », *Bryan, Cave, Leighton, Paisner*, en ligne : <https://ccpa-info.com/does-the-right-to-be-forgotten-under-the-california-consumer-privacy-act-require-that-companies-delete-the-same-type-of-information-as-the-right-to-be-forgotten-und/> (consulté le 2 mai 2022).

426 Jeffrey Dennis, Kyle Janecek, Iana Gaytandjieva, Angela Potter, Edidiong Udoh, Alexander Fetani, Marcello Ferraresi et Victoria Prescott, *Comparing privacy laws: GDPR v. CCPA & CPRA*, OneTrust DataGuidance / Newmeyer & Dillion LLP, 2022, p. 39-41, en ligne : <https://www.dataguidance.com/sites/default/files/20220127_onetrust_dataguidance_gdpr_v_ccpa_and_cpra_report.pdf>.

427 Les amendements sont intégrés au texte officiel de la CCPA.

Les instances législatives californiennes étudient actuellement la CAADCA, un projet de loi qui se concentre sur la protection des mineurs en ligne. Notamment inspirée par le *Children's Code* du ICO, la CAADCA s'appliquerait aux entreprises offrant un produit, un service ou une fonctionnalité en ligne auquel les enfants sont susceptibles d'accéder. Par ailleurs, la loi protégerait tous les mineurs de moins de 18 ans[428], et elle repose sur une définition large du renseignement personnel[429]. Elle prévoit les protections suivantes[430] :

#	Détails
B	Les entreprises assujetties devront adapter l'information à l'âge des mineurs susceptibles de la lire, peu importe le véhicule (conditions d'utilisation, politique de confidentialité, etc.)[431].
E	Le profilage devra être désactivé par défaut[432].
F	La loi interdira la collecte, la vente, la communication ou la conservation de tout renseignement personnel de mineur qui n'est pas nécessaire à la fourniture d'un produit, d'un service ou d'une fonctionnalité avec laquelle l'enfant est « activement et consciemment engagé »[433]. Combinée avec la désactivation par défaut du profilage, cette mesure pourrait limiter ou empêcher, dans les faits, la publicité ciblée.
G	La loi proscrira l'utilisation de renseignements personnels de mineurs à des fins nuisibles (de façon démontrée ou probable) à leur santé physique ou mentale ou à leur bien-être[434].
H	Explicitement, la CAADCA prévoit l'interdiction de recourir à des interfaces truquées si elles mènent les mineurs à fournir plus de renseignements personnels que nécessaire ou à abaisser leurs paramètres de protection, ou si elles causent des nuisances (démontrées ou probables) à leur santé ou à leur bien-être[435].
I	Les entreprises assujetties ne pourront communiquer ou vendre les renseignements personnels de mineurs que si cela est nécessaire pour fournir le service, le produit ou la fonctionnalité[436].
K	Pour tout produit, service ou fonctionnalité auxquels les mineurs peuvent accéder, les entreprises assujetties devront réaliser une analyse d'impact sur la protection des données qui permet de gérer les risques spécifiques aux mineurs[437]. Elles devront fournir un rapport à l'autorité de contrôle et le mettre à jour lors de l'ajout de fonctionnalités ou aux deux ans[438].

428 CAADCA, art. 1798.99.30 (a) (3).

429 CCPA, art. 1798.140.

430 Les protections présentées sont celles du texte du projet de loi amendé en date du 26 avril 2022 du projet de loi; voir note 340.

431 CAADCA, art. 1798.99.31 (a) (4).CAADCA, article 1798.99.31 (a) (4).

432 *Id.*, art. 1798.99.31 (b) (2).

433 *Id.*, art. 1798.99.31 (b) (3).

434 *Id.*, art. 1798.99.31 (b) (1).

435 *Id.*, art. 1798.99.31 (b) (9).

436 *Id.*, art. 1798.99.31 (b) (6).

437 *Id.*, art. 1798.99.31 (a) (1) et 1798.99.30 (a) (4).

438 *Id.*, art. 1798.99.31 (a) (1).

#	Détails
L	Les entreprises assujetties devront vérifier l'âge des consommateurs avec un degré de certitude « raisonnable » compte tenu des risques posés par leurs pratiques[439]; elles peuvent aussi appliquer la CAADCA à tous, indistinctement[440]. Si elles ne connaissent pas l'âge d'un consommateur, elles devront aussi limiter le traitement de ses renseignements personnels[441]. Les renseignements recueillis et utilisés pour vérifier l'âge ne pourront servir à aucune autre fin[442].
M	Par défaut, les paramètres devront être réglés pour offrir un « haut niveau de protection de la vie privée »[443].
N	La CAADCA créera un « groupe d'intervention spécial » sur la protection des renseignements personnels des mineurs[444]. Celui-ci devra faire des recherches, notamment sur les méthodes de vérification d'âge et les risques qui se posent en ligne pour les enfants, puis conseiller l'autorité de contrôle. Cette autorité devra adopter un règlement facilitant et clarifiant l'application de la CAADCA au plus tard le 1er avril 2024[445].
O	Les entreprises assujetties doivent considérer l'intérêt supérieur de l'enfant à travers leurs activités; par défaut, le besoin de sécurité, de bien-être et de vie privée des mineurs prime sur les intérêts commerciaux[446].

Outre les mesures prévues dans le tableau ci-haut, la CAADCA obligera également les entreprises à :

- Aviser clairement les mineurs de l'activation de la fonction de géolocalisation et à limiter la collecte et l'utilisation des renseignements de géolocalisation au strict nécessaire[447];
- Aviser clairement les mineurs de l'activation de fonctions de contrôle parental[448];
- Offrir aux mineurs et à leurs parents des mécanismes simples et accessibles d'exercice des droits[449].

4.2.2.1.2.2 Colorado

Le Colorado a de son côté adopté le CPA en 2021. La loi entrera en vigueur en juillet 2023; elle s'appliquera aux entreprises qui traitent un certain volume de renseignements

[439] *Id.*, art. 1798.99.31 (b) (10).
[440] *Id.*, art. 1798.99.31 (a) (2).
[441] *Id.*, art. 1798.99.31 (b) (4).
[442] *Id.*, art. 1798.99.31 (b) (10).
[443] *Id.*, art. 1798.99.31 (a) (3).
[444] *Id.*, art. 1798.99.32 (a).
[445] *Id.*, art. 1798.99.32 (d).
[446] *Id.*, art. 1798.99.29.
[447] *Id.*, art. 1798.99.31 (b)(7-8).
[448] *Id.*, art. 1798.99.31 (a) (5).
[449] *Id.*, art. 1798.99.31 (a) (7).

personnels[450]. Elle prévoit toutefois une définition potentiellement restrictive du renseignement personnel et définit « enfant » comme toute personne de moins de 13 ans[451]. La loi mise principalement sur le consentement parental comme mécanisme de protection : tout renseignement personnel concernant un mineur de moins de 13 ans est automatiquement considéré comme sensible, ce qui exige l'obtention d'un consentement explicite du parent.[452] (Ⓐ, Ⓙ)

4.2.2.1.2.3 État de Washington

L'Assemblée législative de l'État de Washington étudie actuellement la WPA. Ce projet de loi est divisé en quatre parties, dont l'une porte exclusivement sur la protection des renseignements personnels des enfants (de moins de 13 ans)[453] et des adolescents (de 13 à 18 ans)[454]. Il encadrerait les pratiques de toutes les entreprises, quelle que soit leur taille, par rapport aux renseignements personnels, qui sont définis de façon large[455]. Les mesures suivantes sont proposées :

- Les entreprises devront obtenir le consentement des parents pour traiter des renseignements personnels concernant des enfants[456] (Ⓐ). Les adolescents pourront consentir eux-mêmes; leur consentement devra être exprès et obtenu séparément. Ils devront donner un nouveau consentement exprès, séparément, pour tout ciblage publicitaire[457];
- En plus des droits d'accès et de rectification, un droit de suppression pourra être exercé par les parents au nom des enfants, par les adolescents eux-mêmes ou par un adulte, par rapport aux renseignements le concernant alors qu'il était mineur[458]; l'entreprise devra y donner suite, sauf exception précise[459] (Ⓓ);
- La loi interdira partiellement la publicité comportementale si elle se fonde sur des renseignements sensibles : en effet, les entreprises ne pourront utiliser des renseignements liés à l'origine ethnique et aux facteurs socioéconomiques, ou tout autre renseignement approximant ces derniers, pour cibler du contenu à un enfant, à un adolescent ou à des individus semblables à eux[460] (Ⓕ);
- La WPA interdira à une entreprise de traiter des renseignements personnels concernant des enfants ou des adolescents d'une façon nuisible, c'est-à-dire qui les désavantage injustement, qui résulte en un préjudice raisonnablement

---

450 CPA, art. 6-1-1304 (1).
451 *Id.*, art. 6-1-1303 (4) et (17).
452 *Id.*, art. 6-1-1303 (24) et 6-1-1308 (7).
453 WPA, art. 101 (5).
454 *Id.*, art. 101 (1).
455 *Id.*, art. 101 (13).
456 *Id.*, art. 102.
457 *Id.*
458 *Id.*, art. 105.
459 *Id.*, art. 109 (2).
460 *Id.*, art. 107 (7).

prévisible ou qui serait inattendue et « très choquante » pour une personne raisonnable[461] (Ⓖ);

- Les « pratiques commerciales abusives » liées au traitement des renseignements personnels des mineurs seront interdites[462] (Ⓗ); ces pratiques sont celles :
  - qui empêchent les mineurs de comprendre les conditions d'utilisation d'un service impliquant des renseignements personnels;
  - qui tirent injustement avantage ou qui ne tiennent pas suffisamment compte, de manière déraisonnable, d'une incompréhension du mineur des risques, des coûts ou des conditions du service, de son incapacité à protéger ses intérêts dans la sélection d'un service ou de sa confiance raisonnable envers l'entreprise afin qu'elle agisse dans son intérêt supérieur;
- Les entreprises devront réaliser des analyses d'impact sur la protection des données pour leurs activités impliquant des renseignements personnels sur des mineurs[463] (Ⓚ).

4.2.2.2 Canada

Bien qu'aucune loi sur le secteur privé actuellement en vigueur dans le reste du Canada ne prévoie de protections particulières pour les renseignements personnels des mineurs, tant le gouvernement fédéral que celui de l'Ontario envisagent actuellement des lois qui en introduiraient.

4.2.2.2.1 Échelle fédérale

Le 16 juin 2022, le gouvernement fédéral a déposé le projet de loi C-27, qui vise à remplacer l'actuelle *Loi sur la protection des renseignements personnels et les documents électroniques*[464].

En plus de prévoir la création d'un Tribunal de la protection des renseignements personnels et des données et une nouvelle législation sur l'intelligence artificielle, C-27 introduit différents mécanismes de protection pour les mineurs :

- Les droits et les recours prévus sont exercés par le parent ou le tuteur si le mineur n'a ni la capacité ni la volonté de les exercer personnellement[465] – on peut penser que cela inclut la possibilité de consentir à la collecte, à l'utilisation ou à la

---

461 *Id.*, art. 107 (1). Sans présumer de l'interprétation de « très choquant » (*highly offensive*), on peut noter que ce critère existe notamment dans la loi néo-zélandaise. Voir « What does highly offensive mean? », *New Zealand Privacy Commissioner* (23 mars 2022), en ligne : <https://www.privacy.org.nz/tools/knowledge-base/view/232> (consulté le 3 mai 2022).

462 WPA, art. 107 (9).

463 *Id.*, art. 108.

464 *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5.

465 C-27, art. 4 (a).

communication de renseignements personnels (Ⓐ)[466]. Ici, le gouvernement fédéral fait le choix de ne pas fixer de seuil d'âge;

- Les informations fournies par les organisations doivent être formulées de façon claire et raisonnablement compréhensible pour un individu visé par les activités de l'organisation (Ⓑ)[467];
- Les personnes concernées pourront demander le retrait (soit la suppression définitive et irréversible ou l'anonymisation[468]) d'un renseignement personnel par écrit dans certains cas[469], notamment si elles ont d'abord retiré leur consentement (Ⓓ). C-27 prévoit toutefois certaines exceptions à ce droit, mais tient compte du fait que les renseignements personnels concernent un mineur[470];
- C-27 pose des limites concernant la collecte ou l'utilisation de renseignements personnels en vue d'influencer le comportement ou les décisions d'un individu – spécifiquement, de telles activités ne sont permises qu'avec un consentement (Ⓔ)[471];
- Le projet de loi interdit explicitement l'utilisation de pratiques trompeuses ou mensongères, ou la fourniture d'informations de cette nature, pour obtenir un consentement, sans quoi celui-ci est invalide (Ⓗ)[472];
- C-27 indique clairement que les renseignements personnels concernant des mineurs sont sensibles, ce qui déclenche entre autres l'obligation d'obtenir un consentement exprès pour les recueillir, les utiliser ou les communiquer (Ⓙ, indirectement Ⓘ)[473].

Le projet de loi C-27 étant tout récent au moment de finaliser ce rapport, la Commission n'a pu en faire qu'une lecture rapide; il est possible que certaines autres protections ressortent de l'interaction entre différentes dispositions.

4.2.2.2.2 Ontario

Bien que seuls le Québec, l'Alberta et la Colombie-Britannique aient actuellement une loi provinciale sur la protection des renseignements personnels dans le secteur privé, l'Ontario envisage depuis deux ans d'adopter sa propre loi en cette matière. Le livre blanc du gouvernement sur le sujet[474] renseigne sur les intentions législatives, bien qu'aucun

---

466 Kirsten THOMPSON, « Canada's new federal privacy Bill C-27 – Summary of significant impacts and new proposals », *Dentons* (20 juin 2022), en ligne : <https://www.dentons.com/en/insights/articles/2022/june/20/canadas-new-federal-privacy-bill-c27-summary-of-significant-impacts-and-new-proposals> (consulté le 23 juin 2022).

467 C-27, art. 15 (4).

468 *Id.*, art. 2 (1).

469 *Id.*, art. 55 (1).

470 *Id.*, art. 55 (2).

471 *Id.*, art. 18 (1) et 18 (3).

472 *Id.*, art. 16.

473 *Id.*, art. 2 (2).

474 GOUVERNEMENT DE L'ONTARIO, précité, note 267.

projet de loi n'ait encore été déposé. En ce qui concerne les mesures pouvant protéger les renseignements personnels des mineurs, le document fait état :

- D'un mécanisme de consentement parental pour la collecte, l'utilisation et la communication de renseignements personnels d'un mineur de moins de 16 ans[475]; le livre blanc suggère aussi que les entreprises seraient tenues de vérifier la validité de ce consentement parental (Ⓐ);
    - Le gouvernement ontarien pourrait toutefois laisser aux adolescents de 13 à 16 ans l'occasion « de s'opposer au consentement de leur parent (ou tuteur) à fournir des renseignements personnels en leur nom ou, inversement, de s'opposer à la demande de leur parent (ou tuteur) de détruire ou de retirer des renseignements personnels les concernant »[476];
- D'un droit au déréférencement (ou à l'oubli) semblable à celui adopté dans la Loi 25 au Québec, permettant à des personnes de demander le déréférencement de certains renseignements personnels à leur sujet affichés par d'autres[477] – dans le cas des mineurs, ce droit serait exercé par les parents[478] (Ⓒ);
- D'un « droit à l'élimination », assimilable à un droit à la suppression, qui viserait au moins les renseignements fournis par une personne concernée elle-même[479] – dans le cas des mineurs, ce droit serait exercé par les parents[480] (Ⓓ);
- D'une interdiction de surveiller ou de profiler les mineurs de moins de 16 ans afin d'influencer leur comportement ou leurs décisions[481] (Ⓔ) et d'utiliser leurs renseignements personnels à des fins nuisibles aux personnes ou aux groupes de personnes[482] (Ⓖ);
- D'une consultation du Commissaire à l'information et à la protection de la vie privée de l'Ontario en vue d'élaborer des codes de pratiques et de conduite semblables au *Children's Code*[483] (Ⓝ).

4.2.3 Autres pays

Hors de l'Europe et de l'Amérique du Nord, les cas de l'Inde et du Brésil sont intéressants. Ces pays au poids démographique important se sont eux aussi penchés sur la protection des renseignements personnels des mineurs.

---

475 *Id.*, p. 32 -33.
476 *Id.*, p. 33.
477 *Id.*, p. 10.
478 *Id.*, p. 33.
479 *Id.*, p. 9.
480 *Id.*, p. 33.
481 *Id.*
482 *Id.*
483 *Id.*

4.2.3.1 Inde

L'Inde n'a pas actuellement de loi sur la protection des renseignements personnels; elle y réfléchit toutefois depuis 2019, date de dépôt du PDPB, un projet de loi d'application générale qui aurait protégé notamment les mineurs de façon spécifique. Avant d'être abandonné en août 2022[484], le PDPB a fait l'objet d'un premier rapport parlementaire suggérant des amendements[485]; c'est cette version qui a été consultée dans le cadre de ce rapport. Les mesures suivantes étaient notamment proposées :

- L'obligation d'obtenir un consentement parental pour traiter les renseignements personnels d'un mineur de moins de 18 ans[486] (Ⓐ), dont l'âge doit être dûment vérifié grâce à une méthode tenant compte de certains facteurs, comme le volume de renseignements personnels traités et les risques de préjudices posés par les activités de l'entreprise[487] (Ⓛ);
- Un droit au déréférencement d'application générale[488] (Ⓒ) et un droit à la suppression dans les cas où les renseignements personnels ne sont plus nécessaires à la finalité justifiant leur collecte[489] (Ⓓ);
- L'interdiction de plusieurs activités lorsqu'elles visent des mineurs, notamment tout profilage (Ⓔ), tout suivi comportemental, toute publicité ciblée (Ⓕ) et toute autre activité pouvant causer des préjudices importants au mineur[490] (Ⓖ);
    - Le projet de loi prévoit toutefois une exemption potentielle pour les services offrant des conseils ou du soutien à l'enfant;
- L'obligation de traiter les renseignements personnels dans le respect des droits de l'enfant (Ⓞ). À ce sujet, il faut noter la suppression de la mention de l'intérêt supérieur de l'enfant dans la version amendée par rapport à la version originale.

Le projet de loi indien était, de tous ceux qui ont été consultés, celui qui prévoyait les interdictions les plus fermes concernant le profilage, le suivi et la publicité ciblée. Il faisait d'ailleurs l'objet de certaines critiques en raison de cette radicalité[491].

4.2.3.2 Brésil

En 2020, le Brésil a adopté la LGPD, une loi nationale inspirée du RGPD européen. D'application générale, la LGPD vise toutes les entreprises et tous les renseignements personnels, ceux-ci jouissant d'une définition large[492]. Elle prévoit elle aussi que les

---

484 M. SINGH, précité, note 346.

485 JOINT COMMITTEE ON THE PERSONAL DATA PROTECTION BILL, 2019, précité, note 345, p. 69-74, recommandation 38.

486 PDPB, art. 16 (2) (dans la version telle qu'amendée).

487 *Id.*, art. 16 (3) (dans la version telle qu'amendée).

488 *Id.*, art. 20 (dans la version telle qu'amendée).

489 *Id.*, art. 18 (dans la version telle qu'amendée).

490 *Id.*, art. 16 (4) (dans la version telle qu'amendée).

491 Vrinda BHANDARI, « Facing the consequences of the Data Protection Bill on children's digital privacy », *Medianama* (16 février 2022), en ligne : <https://www.medianama.com/2022/02/223-consequences-data-protection-bill-children-digital-privacy/> (consulté le 28 février 2022).

492 LGPD, art. 3 et 5.

parents sont responsables de consentir au nom des mineurs[493], en matière de protection des renseignements personnels, jusqu'à leurs 18 ans[494] (Ⓐ). Les entreprises doivent faire des efforts raisonnables pour vérifier ce consentement parental[495].

En outre, la LGPD exige des entreprises qu'elles adaptent les informations concernant leurs pratiques en lien avec les renseignements personnels aux mineurs, en tenant compte de leurs caractéristiques propres et en ayant recours à des ressources audiovisuelles au besoin[496] (Ⓑ). Elle indique également que l'intérêt supérieur de l'enfant doit guider tout traitement de renseignements personnels concernant un mineur[497] (Ⓞ).

4.3 Mesures mises en œuvre ou proposées dans des normes

Au-delà des mécanismes législatifs exposés dans la section 4.2, certaines juridictions européennes se sont dotées de normes s'adressant aux entreprises et visant à mieux protéger les renseignements personnels des mineurs, inspirées du *Children's Code* britannique. L'Irlande et les Pays-Bas ont développé des codes de pratiques, à l'instar du ICO; en France, la Commission nationale de l'informatique et des libertés (ci-après CNIL) a structuré ces normes sous la forme de recommandations.

4.3.1 Irlande

L'autorité irlandaise de protection des données, la Data Protection Commission (ci-après DPC), a mené un processus très similaire à celui du ICO pour concevoir son code de pratiques *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing*[498] (ci-après les *Fundamentals*). Ainsi, elle a mené des consultations élargies auprès de différentes parties prenantes, notamment des groupes scolaires, et s'est appuyée sur une analyse juridique approfondie et des recherches académiques[499].

Les *Fundamentals*, contrairement au *Children's Code*, sont envisagés comme un document d'orientation : ils n'ont pas été élaborés en vertu d'un article de loi. La DPC a toutefois clairement indiqué qu'elle tiendrait compte du respect des *Fundamentals* dans ses activités de surveillance de l'application de la loi[500]. Les entreprises visées sont celles

---

493 *Id.*, art. 14 (1).

494 La LGPD ne contient pas de définition des mots « enfants » et « adolescents », et est donc muette sur l'âge; toutefois, une autre loi brésilienne indique que les enfants sont les personnes de moins de 12 ans, et les adolescents celles qui ont entre 12 et 18 ans. Voir Ana Carolina CAGNONI, « How Brazil regulates children's privacy and what to expect under the new data protection law », *International Association of Privacy Professionals* (29 octobre 2019), en ligne : <https://iapp.org/news/a/how-brazil-regulates-childrens-privacy-and-what-to-expect-under-the-new-data-protection-law/> (consulté le 29 avril 2022).

495 LGPD, art. 14(5).

496 *Id.*, art. 14 (6).

497 *Id.*, art. 14.

498 *Fundamentals*, précité, note 149.

499 « DPC publishes final version of Children's "Fundamentals" », *Data Protection Commission* (17 décembre 2021), en ligne : <https://www.dataprotection.ie/index.php/en/news-media/latest-news/dpc-publishes-final-version-childrens-fundamentals> (consulté le 3 mai 2022).

500 *Id.*

qui offrent des services s'adressant aux mineurs de moins de 18 ans[501], ou auxquels ceux-ci sont susceptibles d'accéder[502].

Le document comprend 14 principes similaires à ceux énoncés dans le *Children's Code*, et a d'ailleurs été conçus dans un esprit d'harmonisation normative, vu la proximité géographique avec le Royaume-Uni[503]. Entre autres, la DPC s'attend à ce que les entreprises :

- Appliquent les principes à tous leurs utilisateurs, ou vérifient l'âge selon une approche basée sur le risque[504];
- N'interfèrent pas avec l'intérêt supérieur de l'enfant[505];
- Adaptent l'information pour qu'elle soit compréhensible par les mineurs et les tiennent au courant de leurs pratiques[506];
- N'excluent pas les mineurs en dessous d'un certain âge de leurs services, ni ne nuisent à leur expérience[507];
- Réalisent des analyses d'impact accordant la préséance à l'intérêt supérieur de l'enfant[508];
- Prévoient des mesures de protection des renseignements personnels dès la conception et par défaut[509].
- N'aient pas recours au profilage ou à la prise de décision automatisée à des fins de marketing ou de publicité, sauf exception[510]; la DPC précise par ailleurs que[511] :

> Pour éviter toute confusion, la DPC ne considère pas qu'il est dans l'intérêt supérieur de l'enfant de leur montrer des publicités pour des jeux/services/produits/vidéos etc. qui peuvent les intéresser si ces publicités sont fondées sur le profilage.

Il faut noter que la *Data Protection Act 2018* de l'Irlande, qui adapte le RGPD au contexte national, prévoit une interdiction complète de profiler ou de microcibler un mineur[512]. Cet amendement au texte européen du RGPD dépasserait toutefois la latitude dont jouissent

---

501 *Fundamentals*, précité, note 149, p. 6; *Data Protection Act 2018*, 2018, c. 7, art. 29, en ligne : <https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/index.html>.

502 *Fundamentals*, précité, note 149, p. 15.

503 *Id.*, p. 70, note 12.

504 *Fundamentals*, précité, note 149, principe 1.

505 *Id.*, principe 3.

506 *Id.*, principes 5-6.

507 *Id.*, principes 10-11.

508 *Id.*, principe 13.

509 *Id.*, principe 14.

510 *Id.*, principe 12.

511 *Id.*, p. 57, notre traduction.

512 *Data Protection Act 2018*, précité, note 501, art. 30.

les états membres de l'Union européenne par rapport à l'adaptation du règlement, et est donc présentement inopérant[513].

4.3.2 Pays-Bas

Aux Pays-Bas, c'est le gouvernement plutôt que l'autorité de protection des données, en collaboration avec une université, qui a élaboré un code de pratiques non contraignant, le *Code Voor Kinderrechten*[514] (ci-après CVK), qui s'adresse aux développeurs et aux designers de services visant les moins de 18 ans[515].

Ancré dans la Convention, ce document regroupe 10 principes qui, à nouveau, sont similaires à ceux mis de l'avant dans le *Children's Code* et les *Fundamentals*. Il prévoit entre autres la désactivation du profilage, sauf lorsqu'il est fait dans l'intérêt supérieur de l'enfant, la réalisation d'analyses d'impact sur les droits des mineurs et l'adaptation des informations à l'âge des mineurs[516].

4.3.3 France

La CNIL, qui est l'autorité de protection des données en France, n'a pas développé de code de pratiques; elle a plutôt synthétisé sa position sous la forme de huit recommandations adressées au législateur et aux entreprises[517]. Celles-ci ont toutefois été soumises à des acteurs externes (y compris des enfants) pour consultation.

Fondamentalement, ces recommandations visent à considérer le besoin d'autonomie et les droits des mineurs, à renforcer la fonction d'accompagnement des adultes et à accroître la responsabilité des entreprises du numérique par rapport à la protection des renseignements personnels des mineurs[518]. Alors que le *Children's Code*, les *Fundamentals* et le CVK sont relativement semblables, les recommandations de la CNIL abordent d'autres aspects de la protection des renseignements personnels des mineurs et jettent un éclairage différent sur la question.

Fait intéressant, la CNIL a beaucoup réfléchi à l'interaction entre la capacité à contracter des mineurs, plus généralement traitée dans le droit des contrats, le droit civil et le droit de la consommation, et leur capacité à consentir au traitement de leurs renseignements

---

513 *Fundamentals*, précité, note 149, p. 73, note 77.

514 UNIVERSITY OF LEIDEN et WAAG ORGANISATION, *Code for Children's Rights*, Ministère de l'Intérieur et des Relations du Royaume, 2021, en ligne : <https://codevoorkinderrechten.nl/wp-content/uploads/2021/07/Code-voor-Kinderrechten-Wordversie_EN.pdf>.

515 *Id.*, p. 11-12.

516 *Id.*, principes 4, 5 et 7.

517 « Les droits numériques des mineurs », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/les-droits-numeriques-des-mineurs> (consulté le 6 décembre 2021).

518 « La CNIL publie 8 recommandations pour renforcer la protection des mineurs en ligne », *CNIL* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne> (consulté le 6 décembre 2021).

personnels[519]. Elle favorise une harmonisation des seuils d'âge et une reconnaissance de la capacité des adolescents à contracter eux-mêmes lorsque les services ont comme finalité principale le traitement de leurs renseignements personnels. Pour les mineurs de moins de 15 ans, elle recommande de confier le consentement aux parents (comme le prévoit la version française du RGPD), mais encourage ces derniers à s'assurer d'un co-consentement[520] :

> Cela signifie que le consentement pour des fonctionnalités supplémentaires telles que le choix d'un profil public ou privé sur un réseau social ou l'activation de la géolocalisation optionnelle sur une application doit théoriquement résulter d'un commun accord de l'enfant et du ou des titulaires de l'autorité parentale. Autrement dit, les parents ne peuvent, pour ces traitements, aller contre la volonté de l'enfant et l'enfant passer outre l'opposition de ses parents.

Puisque la question de l'âge du consentement autonome appelle celles de la vérification d'âge et de la vérification du consentement parental, la CNIL offre un tour d'horizon des méthodes actuelles utilisées à ces fins. Dans les cas où ces processus de vérification doivent être mis en œuvre, « il convient de préserver la capacité à naviguer en ligne librement, sans s'identifier »; par conséquent, l'autorité recommande des systèmes proportionnels, robustes, standardisés, simples, qui minimisent la collecte de renseignements personnels et, si possible, qui impliquent un tiers de confiance[521].

La CNIL met également l'accent sur l'exercice des droits par les mineurs eux-mêmes (recommandation 2), « sans préjudice de la possibilité pour les parents d'exercer les droits au nom de leur enfant et de l'accompagner dans cette démarche », précise-t-elle[522].

Si elle considère que les parents doivent soutenir leur enfant et mise sur la sensibilisation pour les y aider[523], la CNIL juge toutefois que les outils de contrôle parental mis à disposition par les plateformes présentent certains risques de mauvaise utilisation ou

---

519 « Recommandation 1 : encadrer la capacité d'agir des mineurs en ligne », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-1-encadrer-la-capacite-dagir-des-mineurs-en-ligne> (consulté le 6 décembre 2021).

520 « Recommandation 4 : rechercher le consentement d'un parent pour les mineurs de moins de 15 ans », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-4-rechercher-le-consentement-dun-parent-pour-les-mineurs-de-moins-de-15-ans> (consulté le 6 décembre 2021).

521 « Recommandation 7 : vérifier l'âge de l'enfant et l'accord des parents dans le respect de sa vie privée », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-7-verifier-lage-de-lenfant-et-laccord-des-parents-dans-le-respect-de-sa-vie-privee> (consulté le 6 décembre 2021).

522 « Recommandation 2 : encourager les mineurs à exercer leurs droits », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-2-encourager-les-mineurs-exercer-leurs-droits> (consulté le 6 décembre 2021).

523 « Recommandation 3 : accompagner les parents dans l'éducation au numérique », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-3-accompagner-les-parents-dans-leducation-au-numerique> (consulté le 6 décembre 2021).

d'habituation à la surveillance[524]. Par conséquent, elle souligne que ces outils doivent être proportionnés à l'intérêt de l'enfant et à son niveau de maturité, transparents et sécuritaires.

Comme les autres textes normatifs présentés dans ce rapport, la recommandation 6 de la CNIL appelle les entreprises à adopter un design vertueux, c'est-à-dire à éviter les interfaces truquées et à adapter la conception des services aux mineurs (ex. simplicité et format de l'information fournie)[525]. L'autorité fournit d'ailleurs de nombreux exemples de design problématique ou vertueux sur un site dédié aux développeurs[526]. Enfin, s'agissant toujours des conseils adressés aux entreprises, la CNIL recommande de prévoir des paramètres protecteurs par défaut, d'éviter le profilage des mineurs dans la plupart des cas (sauf lorsqu'il permet de les protéger) et d'éviter de communiquer leurs renseignements personnels à des fins commerciales, y compris publicitaires[527]. En ce sens, elle rejoint les autres textes normatifs présentés précédemment.

---

524 « Recommandation 5 : promouvoir des outils de contrôle parental respectueux de la vie privée et de l'intérêt de l'enfant », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-5-promouvoir-des-outils-de-controle-parental-respectueux-de-la-vie-privee-et-de> (consulté le 6 décembre 2021).

525 « Recommandation 6 : renforcer l'information et les droits des mineurs par le design », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-6-renforcer-linformation-et-les-droits-des-mineurs-par-le-design> (consulté le 6 décembre 2021).

526 « Données & Design - Études de cas », *Commission nationale de l'informatique et des libertés*, en ligne : <https://design.cnil.fr/etudes-de-cas/> (consulté le 4 mai 2022); voir par exemple « Fuzzy », « Konect », « Instap » et « BrawlCrush », qui visent des services fictifs s'adressant à des mineurs.

527 « Recommandation 8 : prévoir des garanties spécifiques pour protéger l'intérêt de l'enfant », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-8-prevoir-des-garanties-specifiques-pour-proteger-linteret-de-lenfant> (consulté le 6 décembre 2021).

5. ANALYSE DE LA LOI 25

Quoiqu'elle prévoie de nouvelles mesures de protection pour les renseignements personnels de toutes les personnes concernées, indépendamment de leur âge, la Loi 25 mise principalement sur le consentement parental pour ce qui est de la protection particulière des mineurs.

Du point de vue de la Commission, compte tenu des éléments présentés précédemment dans ce rapport, le mécanisme du consentement parental ne suffit pas. En cohérence avec les objectifs de cette réforme et en considérant les limites du consentement, d'ailleurs reconnues par les entreprises elles-mêmes, elle estime qu'il faut envisager des mesures supplémentaires visant à limiter certaines finalités et à responsabiliser davantage les entreprises afin de protéger les mineurs.

Dans cette section, la Commission résume d'abord les dispositions pertinentes de la Loi 25, puis les examine à la lumière du contexte présenté dans la section 3 et des lois, des normes et des travaux internationaux présentés dans la section 4.

Parmi les modifications substantielles que la Loi 25 apporte à la Loi sur le privé, plusieurs peuvent avoir un impact positif sur la protection plus particulière des mineurs. La Commission salue les avancées en cette matière. Toutefois, bien que variées, ces mesures n'ont peut-être pas toute l'efficacité voulue pour prévenir les risques pour les droits des mineurs mentionnés dans la section 3.3 de ce rapport. Au premier chef, la disposition principale qui vise les mineurs – le mécanisme de consentement parental – souffre d'importantes limites et gagnerait à être complétée par d'autres mesures.

5.1 Présentation du cadre juridique modernisé

Adoptée en septembre 2021, la Loi 25 constitue une modernisation importante du cadre de protection des renseignements personnels. À bien des égards, elle propulse le Québec à l'avant-garde internationale en la matière.

Par rapport à celles d'autres juridictions, la législation québécoise s'applique de façon large : la Loi sur le privé est prépondérante et assujettit toute personne qui exploite une entreprise au sens de l'article 1525 du *Code civil du Québec*[528]. De plus, elle repose sur une définition large du renseignement personnel[529].

Le tableau suivant, qui reflète celui de la page 71, présente les mesures qui touchent les mineurs dans le cadre juridique québécois tel que modifié par la Loi 25.

[528] Loi sur le privé, art. 1. Lorsqu'applicable, les références faites à cette loi dans la suite du texte concernent les articles tels qu'ajoutés ou amendés par la Loi 25.

[529] *Id.*, art. 2.

	Mesures	LP
A	Consentement parental jusqu'à un âge X	14
B	Exigence explicite d'adaptation des informations données à l'âge de l'enfant	
C	Droit au déréférencement	
D	Droit à la suppression	CERT
E	Interdiction explicite (totale ou partielle) du profilage/des décisions automatisées	PART
F	Interdiction explicite (totale ou partielle) de la publicité ciblée	
G	Interdiction explicite (totale ou partielle) d'utiliser les RP d'enfants à des fins nuisibles	
H	Interdiction explicite (totale ou partielle) d'utiliser des interfaces truquées	
I	Interdiction explicite (totale ou partielle) de communiquer les RP d'enfants	
J	Désignation explicite des RP d'enfants comme sensibles	
K	Réalisation d'une analyse d'impact si des RP d'enfants sont impliqués	
L	Vérification d'âge par les fournisseurs de services	
M	Paramètres les plus protecteurs des RP par défaut	PART
N	Mise en place d'un code de pratiques	
O	Mention de l'intérêt supérieur de l'enfant	

Légende

	Prévu dans la loi
	Partiellement
CERT	Seulement dans certains cas
PART	Partiellement
RP	Renseignements personnels

Le législateur a opté pour le consentement parental comme mécanisme principal de protection des renseignements personnels des mineurs dans la Loi 25 (Ⓐ). En ce sens, il a étendu la responsabilité parentale déjà prévue par exemple pour l'accès aux dossiers médicaux[530]. Jusqu'à l'âge de 14 ans, c'est donc le titulaire de l'autorité parentale ou le tuteur du mineur qui pourra consentir à la collecte de renseignements personnels auprès de ce dernier, à leur utilisation à d'autres fins que celles prévues ou à leur communication[531]. 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, l'utilisation ou la communication sont manifestement au bénéfice du mineur. Cette mesure est la seule qui vise spécifiquement les mineurs. Elle s'applique tant dans le monde physique que numérique.

La législation québécoise prévoit aussi un droit au déréférencement (Ⓒ). Ainsi, sous réserve du respect de certains critères, la Loi 25 prévoit qu'une personne concernée peut

[530] *Id.*, art. 38.

[531] *Id.*, art. 4.1 et 14.

exiger d'une entreprise qu'elle cesse la diffusion d'un renseignement personnel la concernant ou que soit désindexé tout hyperlien rattaché à son nom et permettant d'accéder à ce renseignement par un moyen technologique[532]. L'un des critères dont doit tenir compte l'entreprise dans l'analyse de la demande est le fait que le renseignement concerne la personne alors qu'elle est ou était mineure, ce qui témoigne d'un souci particulier pour les mineurs, qui sont en processus de construction identitaire et d'exploration. Par ailleurs, si la Loi sur le privé ne prévoit pas de droit à la suppression large, comme la WPA par exemple, elle offre toutefois un droit à la rectification[533] fondé sur le *Code civil du Québec*[534] (ci-après C.c.Q.) (D). Une personne concernée peut donc faire supprimer un renseignement lorsque celui-ci est périmé ou non justifié par l'objet du dossier.

La Loi 25 n'interdit pas le profilage, mais impose une obligation de transparence aux entreprises qui y ont recours[535]. Elle prévoit aussi sa désactivation par défaut[536] (E). Ces dispositions visent aussi les technologies d'identification et de localisation.

Les produits et services technologiques recueillant des renseignements personnels, s'ils disposent de paramètres de confidentialité, devront par défaut être réglés pour assurer le plus haut niveau de confidentialité possible[537] en vertu de la Loi 25 (M). Les témoins de connexion sont toutefois exclus de la portée de cette obligation.

Au-delà de ces mesures, d'autres sont pertinentes, même si elles ne correspondent pas exactement aux libellés du tableau :

- Les entreprises devront fournir des informations supplémentaires aux personnes concernées au moment de recueillir des renseignements personnels[538] et rendre publiques des politiques de confidentialité[539]. Elles devront utiliser des « termes simples et clairs » pour transmettre ces informations, tout comme pour les demandes de consentement[540]. La Loi 25 ne prévoit toutefois pas d'adaptation particulière pour les mineurs (B);
- Si elles utilisent des renseignements personnels pour rendre une décision fondée exclusivement sur un traitement automatisé, les entreprises devront en informer la personne concernée au plus tard au moment de l'informer de cette décision. Elles

---

532 *Id.*, art. 28.1.

533 *Id.*, art. 28.

534 *Code civil du Québec*, RLRQ, c. CCQ-1991, art. 40.

535 Loi sur le privé, art. 8.1.

536 Pour la disposition miroir de la Loi sur l'accès, voir SECRÉTARIAT À LA RÉFORME DES INSTITUTIONS DÉMOCRATIQUES, À L'ACCÈS À L'INFORMATION ET À LA LAÏCITÉ, « Identification, localisation et profilage », *Québec. ca* (25 janvier 2022), en ligne : <https://www.quebec.ca/gouvernement/travailler-gouvernement/services-employes-etat/conformite/protection-des-renseignements-personnels/technologie-et-droit-a-la-protection-des-renseignements-personnels/identification-localisation-profilage> (consulté le 6 avril 2022).

537 Loi sur le privé, art. 9.1.

538 *Id.*, art. 8.

539 *Id.*, art. 8.2.

540 *Id.*, art. 14.

devront aussi expliquer la décision (par ex. renseignements utilisés, facteurs pris en compte dans la décision) et donner l'occasion à la personne concernée de présenter ses observations à un employé en mesure de réviser la décision[541] (lien avec E);

- La Loi 25 prévoit une définition pour les renseignements sensibles, lesquels font l'objet d'une protection renforcée (par exemple, les entreprises doivent obtenir un consentement explicite pour les utiliser à d'autres fins ou les communiquer). Même si les renseignements personnels des mineurs ne font pas partie des exemples explicites mentionnés dans le texte législatif[542] (lien avec J), ils pourraient être considérés comme tels dans certains contextes;
- La Loi 25 n'impose pas de vérification de l'âge (lien avec L), quoique cette exigence pourrait être implicite, comme dans le cas du RGPD[543]; la Commission ne s'est pas prononcée à cet égard;
- Dans plusieurs situations, les entreprises devront réaliser des évaluations des facteurs relatifs à la vie privée tenant compte entre autres de la sensibilité des renseignements impliqués[544] (lien avec K). Celles-ci mèneront à une réflexion en amont des projets qui permettra souvent d'envisager l'impact d'une activité projetée sur la protection des renseignements personnels en général. Le fait qu'un projet implique les renseignements personnels de mineurs n'est pas en soi un critère menant à l'obligation de réaliser une telle évaluation.

5.2 Analyse de la protection accordée aux mineurs

Bien que la Loi sur le privé telle que modifiée par la Loi 25 soit une législation d'avant-garde en matière de protection des renseignements personnels de manière générale, la protection particulière qu'elle accorde aux mineurs n'est pas suffisante, selon la Commission, compte tenu des considérations énoncées précédemment dans ce rapport.

La Loi 25 vise à impliquer davantage le parent pour assurer une protection supplémentaire au mineur jusqu'à ce qu'il atteigne un âge où on estime qu'il est en mesure de faire ses propres choix avec discernement. *A priori*, on peut voir dans ce choix une extension de la responsabilité parentale traditionnelle vers le monde numérique, et une mise en œuvre du principe d'évolution des capacités de l'enfant consacré dans la Convention[545]. Il est également clair que cette mesure de protection est désormais presque systématique dans les lois sur la protection des renseignements personnels[546].

Toutefois, le consentement ne saurait constituer le seul mécanisme spécifique de protection des mineurs : même exercé par le parent, il souffre d'importantes limites,

---

[541] *Id.*, art. 12.1.

[542] *Id.*, art. 12-13.

[543] Voir la ligne L du tableau de la page 71 de ce rapport.

[544] Loi sur le privé, art. 3.3, 17 et 21.

[545] K. McCULLAGH, précité, note 183, p. 127.

[546] Voir le tableau de la page 72.

surtout dans le contexte numérique[547], que la Commission explore ci-après. Elle revient également sur l'adéquation de certaines autres mesures de protection évoquées ci-haut.

5.2.1 Nécessité, intérêt légitime, licéité de la collecte et consentement

La Loi sur le privé, telle que modifiée par la Loi 25, pose plusieurs conditions pour la collecte d'un renseignement personnel par une entreprise :

1. L'entreprise doit avoir un intérêt sérieux et légitime pour recueillir ce renseignement et doit aussi déterminer la fin de la collecte au préalable[548];
2. La collecte doit être faite par des moyens licites[549];
3. Elle doit se faire auprès de la personne concernée[550], sauf :
    a. Dans le cas où celle-ci a moins de 14 ans (vu les changements apportés par la Loi 25) – la collecte se fait alors auprès du parent, ou auprès du mineur si le parent y consent ou si elle est manifestement au bénéfice du mineur[551];
    b. Si la personne concernée consent à ce que le renseignement soit recueilli auprès d'un tiers, ou si les conditions prévues par la loi sont respectées[552];
4. L'entreprise ne peut recueillir que les renseignements nécessaires aux fins qu'elle a identifiées[553];
5. L'entreprise doit respecter ses obligations d'information envers la personne concernée[554].

5.2.1.1 Critère de nécessité

Le critère de **nécessité** est fondamental. En vertu de celui-ci, une entreprise ne peut recueillir un renseignement que si[555] :

- Elle poursuit un objectif légitime, important et réel;
- La collecte est proportionnelle compte tenu de cet objectif, c'est-à-dire :
    - Elle est rationnellement liée à l'objectif;
    - L'atteinte à la vie privée est minimisée;
    - La collecte est nettement plus utile à l'entreprise que préjudiciable à la personne concernée.

En théorie, ce principe-maître à lui seul devrait suffire à équilibrer beaucoup de situations problématiques. Par exemple, lorsque l'intérêt supérieur de l'enfant serait gravement mis

---

547 COMMISSION D'ACCÈS À L'INFORMATION, précité, note 62, p. 35-37; COMMISSION D'ACCÈS À L'INFORMATION, précité, note 307, p. 89-90.

548 Loi sur le privé, art. 4.

549 *Id.*, art. 5.

550 *Id.*, art. 6.

551 *Id.*, art. 4.1.

552 *Id.*, art. 6.

553 *Id.*, art. 5.

554 *Id.*, art. 7 à 8.2.

555 *Laval (Société de transport de la Ville de)* c. *X*, [2003] C.A.I. 667 (C.Q.).

en cause par une collecte commerciale projetée de renseignements personnels, la collecte ne serait pas « nettement plus utile à l'entreprise que préjudiciable à la personne concernée ». Dans un tel cas, une entreprise devrait s'abstenir d'aller de l'avant.

En pratique, la nécessité est rarement bien comprise par les entreprises. Elle demande une analyse approfondie et, dans bien des cas, une forme de retenue que l'environnement commercial actuel ne favorise pas. Par ailleurs, dans certains cadres juridiques, comme le RGPD ou la LGPD, elle ne constitue pas la seule base juridique permettant de recueillir des renseignements personnels; par exemple, le consentement à lui seul permet selon ces lois de justifier une collecte dans certains cas[556]. Il en résulte que des pratiques courantes hors du Québec ont cours également sur son territoire, sans toujours être forcément conformes au droit local.

5.2.1.2 Rôle du consentement

Le consentement est aussi l'une des pierres angulaires des lois québécoises sur la protection des renseignements personnels. Il est associé à la notion de contrôle de l'individu sur la circulation et l'utilisation de ses informations. **Toutefois, il ne permet pas, au Québec, de contourner le principe de nécessité**. Autrement dit, l'obtention d'un consentement ne libère pas les entreprises de leur responsabilité de réaliser une analyse sérieuse de la nécessité de la collecte. Dans les faits, cependant, comme le soulignait la Commission dans son rapport quinquennal de 2016, cette nuance n'est pas bien comprise par les assujettis, entre autres en raison du libellé de certains articles des lois[557]. Le consentement est donc *perçu* comme une autorisation à recueillir tout renseignement, indépendamment de sa nécessité. Dans certains cas, les entreprises s'en servent même pour justifier des pratiques inacceptables.

Le consentement joue aussi un rôle central en ce qui concerne l'utilisation et la communication de ces renseignements. Dans ce cas, il constitue la principale base juridique permettant l'utilisation et la communication à d'autres fins que celles de la collecte, si celles-ci ne sont pas prévues par la loi. Il revêt par conséquent une importance capitale par rapport à la protection des renseignements personnels. Les paramètres qui en assurent la validité peuvent toutefois être compromis par certaines caractéristiques de l'environnement numérique actuel (voir la section 5.2.2).

5.2.1.3 Utilisation et communication sans consentement

Dans certains cas, l'utilisation et la communication sont possibles même sans le consentement de la personne concernée. Ainsi, la Loi sur le privé telle que modifiée autorise entre autres les entreprises à utiliser des renseignements personnels sans solliciter de consentement si elles jugent que cette utilisation est à des fins compatibles avec la finalité initiale de la collecte[558]. Considérant la difficulté d'évaluer le critère de

---

[556] COMMISSION D'ACCÈS À L'INFORMATION, précité, note 62, p. 35.

[557] COMMISSION D'ACCÈS À L'INFORMATION, précité, note 307, p. 92.

[558] Loi sur le privé, art. 12, alinéa 2, paragraphe 1°.

nécessité mentionnée ci-haut, l'interprétation de la « compatibilité » pourrait être plus large que voulu, malgré les balises posées dans la loi[559].

La Loi 25 a également ajouté à la Loi sur le privé un droit explicite de retirer son consentement[560]. Cependant, ce droit ne couvre pas les situations où une entreprise utilise ou communique un renseignement personnel sans consentement, suivant une exception permise par la loi. Autrement dit, la Loi sur le privé telle que modifiée n'offre aucun droit d'opposition au mineur ou à ses parents par rapport à certaines utilisations ou communications ne reposant pas sur le consentement.

Les éléments présentés précédemment militent pour des modifications permettant de rendre la Loi sur le privé plus claire et plus explicite. C'est ce que propose Option consommateurs dans son mémoire sur le projet de loi nº 64[561] en faisant référence à l'interdiction explicite de certaines pratiques commerciales problématiques :

> Bien que des dispositions légales actuellement en vigueur pourraient être invoquées pour baliser certaines de ces pratiques, il reste qu'il nous apparaît hasardeux de s'en remettre uniquement au patient travail des tribunaux pour en venir à déterminer ce que peuvent faire ou non les entreprises avec nos données.

5.2.2 Caractère libre et éclairé du consentement

Le caractère libre et éclairé[562] du consentement peut être remis en question[563], qu'il soit donné par le parent pour un mineur de moins de 14 ans, ou le mineur lui-même lorsqu'il est âgé de 14 à 17 ans.

Pour être libre, le consentement ne doit être influencé par aucune contrainte ou pression indue. Or, dans l'environnement numérique et commercial, plusieurs problèmes nuisent à cette liberté :

- **Les interfaces ne sont pas neutres :** Les entreprises ont le contrôle entier sur les outils mis en place pour recueillir le consentement. Elles y incluent souvent des interfaces truquées qui peuvent orienter les choix en générant, par exemple, une asymétrie dans leur mise en valeur (voir l'Annexe 1)[564]. Celles-ci peuvent être bonifiées au fil du temps, puisque les entreprises peuvent tester leur efficacité sur de grandes quantités d'utilisateurs[565].

---

559 *Id.*, art. 12, alinéa 3.

560 *Id.*, art. 8.

561 OPTION CONSOMMATEURS, précité, note 223, p. 11.

562 *Id.*, art. 14.

563 COMMISSION D'ACCÈS À L'INFORMATION, précité, note 62, p. 34-39; M. MAČĖNAITĖ et E. KOSTA, précité, note 404, p. 185-186.

564 REVEALING REALITY, précité, note 61; M. MAČĖNAITĖ et E. KOSTA, précité, note 404, p. 185; COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, précité, note 301, p. 13 -22.

565 REVEALING REALITY, précité, note 61, p. 29; Jennifer KING, *Dark Patterns & Manipulative Design*, Présentation PowerPoint, Sacramento (Californie), California Privacy Protection Agency Pre-Rulemaking

- **Le consentement répété perd de son sens :** Le consentement devrait être un acte significatif, négocié avec l'autre partie au besoin. En le demandant constamment à travers toutes les activités en ligne, on mine son sens. Il peut alors se créer une « fatigue du consentement », qui pousse à le donner sans vraiment considérer le contexte ou les informations reçues[566].
- **Refuser, c'est s'exclure :** Puisque le consentement à la collecte, à l'utilisation, à la communication et à la conservation de renseignements personnels est souvent une condition d'utilisation des produits et services numériques ou d'accès à toutes leurs fonctionnalités, refuser de consentir revient à s'abstenir d'y avoir recours. Un tel choix a de très importantes conséquences pour la socialisation d'un mineur[567], vu la popularité et le rôle central des produits et services numériques dans la vie des mineurs et leur sensibilité à la pression des pairs[568]. Comme le souligne aussi la Commission européenne, « l'abstinence numérique n'est pas une option pour les enfants d'aujourd'hui, qui dépendent de plus en plus de l'internet pour avoir accès à des informations, à certaines activités scolaires, aux contacts sociaux et à des activités récréatives »[569].

Le consentement doit aussi être éclairé, ce qui implique « que la personne dispose d'informations suffisantes pour poser un jugement sur la situation et évaluer la portée du consentement qu'elle s'apprête à donner ou non. Elle doit donc connaître avec suffisamment de détails ce qui se passera si elle accepte et quelles seront les conséquences d'un refus »[570]. Le respect de ce critère peut lui aussi être compromis par plusieurs facteurs :

- **Les pratiques sont opaques et complexes** : Les informations contenues dans les conditions d'utilisation, les politiques de confidentialité, les consentements ou les interfaces sont souvent complexes, partielles ou incomplètes[571]. Les nouvelles dispositions de la Loi sur le privé qui prévoient l'utilisation de termes simples et clairs pour communiquer l'information aux personnes concernées[572] contribueront à une meilleure compréhension de leur part. Toutefois, elles ne sont peut-être pas suffisantes pour permettre de présumer d'un consentement éclairé en toutes circonstances. En particulier, la complexité de l'environnement numérique en

---

Informational Sessions, 29 mars 2022, p. 15, en ligne : <https://cppa.ca.gov/meetings/materials/20220329_30_day_1_item_2c_king.pdf>.

566 M. MAČĖNAITĖ et E. KOSTA, précité, note 404, p. 186.

567 REVEALING REALITY, précité, note 118, p. 9; M. MAČĖNAITĖ et E. KOSTA, précité, note 404, p. 185; M. JOHNSON, V. STEEVES, L. R. SHADE et G. FORAN, précité, note 122, p. 26.

568 Voir la section 3.4 de ce rapport.

569 COMMISSION EUROPÉENNE, *Une décennie numérique pour les enfants et les jeunes : la nouvelle stratégie européenne pour un internet mieux adapté aux enfants*, COM (2022) 212 final, 2022, en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=COM:2022:212:FIN>, section 3.

570 COMMISSION D'ACCÈS À L'INFORMATION, précité, note 307, p. 91.

571 *Id.*, p. 109; 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, Éditions Yvon Blais, 2019, p. 35-66, aux pages 51-59.

572 Loi sur le privé, art. 3.2, 8, 8.2 et 14.

général – pour des raisons qui dépassent bien souvent les pratiques d'une seule entreprise[573] – est telle qu'il peut être ardu de bien l'expliquer tant aux mineurs qu'à leurs parents dans des informations touchant un produit, un service ou une fonctionnalité. Dans ces circonstances, lorsque les mineurs sont exposés à des risques importants pour leurs droits fondamentaux, le recours au consentement pour autoriser certaines pratiques est inapproprié.

- **Les choix doivent être faits dans l'instantanéité** : La nature dématérialisée des services numériques cantonne l'acte du consentement à une courte période temporelle. Beaucoup d'informations sont données en même temps et plusieurs incitatifs encouragent la prise d'une décision rapide, ce qui ne favorise pas la réflexion sur la portée du consentement. Par ailleurs, celui-ci est demandé la plupart du temps par une interface et non par un humain, ce qui empêche de poser des questions pour bien comprendre. La Loi 25 obligera certes les entreprises à prêter assistance aux personnes concernées au moment de consentir, à leur demande[574], mais ce geste exigera des efforts et du temps que tous les mineurs ou leurs parents ne pourront ou ne voudront pas investir, même s'ils ont des questions.
- **Les mineurs et leurs parents ont une littératie numérique limitée** : Comme le montrent les sections 3.2.2.2 et 3.2.3.2 de ce rapport, tant les mineurs que leurs parents ont une compréhension limitée de l'écosystème numérique et de sa complexité. Pour une bonne partie, cela s'explique par l'opacité des pratiques impliquant des renseignements personnels. De même, ils se concentrent surtout sur la dimension interpersonnelle de la vie privée et sur les renseignements fournis, laissant de côté les enjeux commerciaux et les risques liés aux renseignements observés ou inférés. Dans ce contexte, sans égard à la qualité de l'information fournie par l'entreprise, la compréhension réelle nécessaire à un consentement n'est pas toujours assurée.

5.2.3 Choix du seuil d'âge et vérifications

Le mécanisme du consentement parental implique également de fixer un seuil d'âge au-delà duquel celui-ci n'est plus requis, et potentiellement de mener des vérifications de l'âge du mineur et de sa relation avec le parent.

Le moment auquel un mineur acquiert suffisamment de discernement pour être en mesure de donner un consentement valide à la collecte, à l'utilisation ou à la communication de ses renseignements personnels varie d'une personne à l'autre, en fonction de paramètres dépassant l'âge à lui seul[575]. Idéalement, dans l'esprit du respect de l'évolution des capacités de l'enfant *individuel*, principe consacré dans la Convention, les entreprises devraient vraisemblablement faire une analyse au cas par cas de la capacité à consentir d'un mineur.

---

[573] Voir le concept de « surveillance croisée », qui engendre de la complexité, dans D. LYON, précité, note 63, p. 8.

[574] Loi sur le privé, art. 14.

[575] M. STOILOVA, S. LIVINGSTONE et R. NANDAGIRI, précité, note 39, p. 28 -29.

Or en pratique, une telle analyse demande beaucoup de temps et d'informations que les entreprises offrant des produits et services numériques n'ont pas, et son résultat variable d'une personne à l'autre n'offre pas beaucoup de sécurité juridique[576]. Pour ces raisons, comme la Loi 25, la plupart des législations qui introduisent un consentement parental fixent un seuil pour « l'âge de consentement numérique »[577]. Ce choix opérationnel se justifie, mais comporte sa part d'arbitraire et risque tantôt de surprotéger, tantôt de sous-protéger certains mineurs.

De façon corollaire, l'ajout d'un seuil d'âge dans la loi, 14 ans en l'occurrence au Québec, amène à réfléchir sur la nécessité de vérifier cet âge. En effet, pour être conforme à la loi, faut-il s'assurer que l'utilisateur inconnu d'un service numérique a bel et bien moins de 14 ans, en quel cas son parent doit être sollicité? Ce rapport ne s'y penche pas en détail, **mais la Commission souligne que la question de la vérification d'âge est éminemment complexe et présente des enjeux de protection des renseignements personnels**. Elle requiert généralement d'en collecter davantage[578], et potentiellement sur tous les utilisateurs plutôt que sur les mineurs seuls[579].

Enfin, si l'entreprise établit que le consentement du parent est requis, d'autres difficultés pratiques se posent. S'il est relativement facile de confirmer qu'une personne a plus de 18 ans, il est en revanche beaucoup plus ardu de démontrer sa relation effective avec le mineur concerné[580]. En d'autres termes, aucun moyen véritablement satisfaisant n'existe à l'heure actuelle pour démontrer que l'adulte sollicité pour consentir détient bel et bien l'autorité parentale ou la fonction de tuteur par rapport au mineur[581].

5.2.4 Consentement parental et autonomie du mineur

Au-delà de ces considérations, confier le consentement au parent lorsqu'il s'agit des renseignements personnels d'un mineur peut nuire à l'autonomie de ce dernier.

Comme le soulignait la Commission en 2002, « les intérêts des enfants ne sont pas nécessairement identiques à ceux de ses parents ou des adultes qui vivent dans leur milieu »[582]. Elle indiquait par exemple que dans des cas d'abus ou de violence familiale, il serait périlleux de s'en remettre entièrement au parent sans considérer l'intérêt supérieur de l'enfant[583]. Même si la réflexion présentée à l'époque portait sur le droit du parent à accéder aux renseignements personnels concernant son enfant mineur, elle illustrait un problème qui s'étend au consentement parental. La protection exercée par le parent peut

---

576 K. MCCULLAGH, précité, note 183, p. 125-127.

577 Voir le tableau de la page 72.

578 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, précité, note 521.

579 5RIGHTS FOUNDATION, précité, note 241; INFORMATION COMMISSIONER'S OFFICE, précité, note 313; COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, précité, note 259, p. 32; INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, précité, note 254, par. 16.

580 K. MCCULLAGH, précité, note 183, p. 129-130.

581 FUTURE OF PRIVACY FORUM, précité, note 318.

582 COMMISSION D'ACCÈS À L'INFORMATION, précité, note 326, p. 66.

583 *Id.*

parfois se muer en contrôle, ce qui peut nuire aux droits du mineur, notamment celui à la liberté d'expression[584].

À ce chapitre, le fait que le consentement parental ne soit pas requis par la Loi 25 si la collecte, l'utilisation ou la communication de renseignements personnels est manifestement au bénéfice du mineur est une protection utile. Elle peut permettre au mineur d'aller chercher de l'aide en ligne dans une situation de violence familiale, par exemple, sans en informer son parent. Cependant, elle ne constitue pas une solution à toutes les facettes du problème.

Par ailleurs, la Loi 25 permet aux enfants de 14 à 17 ans de consentir de manière autonome, mais permet aussi aux entreprises de recueillir un consentement parental pour l'adolescent. Elle est toutefois muette sur une éventuelle prédominance à accorder à la volonté du mineur par rapport à celle de son parent.

5.2.5 Consentement, individualisation de la réflexion et effets de groupe

Le consentement est un acte de contrôle individuel. Fondamentalement, il confie à la personne concernée (ou à la personne qui la représente) une responsabilité importante quant à la protection de ses droits. Si cela peut être approprié dans de nombreuses situations, ce l'est de moins en moins en matière de protection des renseignements personnels.

En effet, plusieurs des risques auxquels sont confrontés les mineurs dans le monde numérique sont de nature systémique. Ils dépassent la relation individuelle qu'ont les mineurs avec une entreprise, et résultent plutôt de choix de conception ou de modèles d'affaires entiers. Autrement dit, ils sont générés par les entreprises. Dès lors, confier le fardeau de la protection aux parents ou aux adolescents représente une forme de déséquilibre[585], alors qu'il existe une forte asymétrie de pouvoir dans leur relation avec les entreprises[586]. De la même façon, en droit de la consommation, cette asymétrie a mené à l'interdiction de pratiques commerciales jugées préjudiciables, déplaçant le poids de la protection des épaules de l'individu à celles de l'entreprise, comme le rappelle le juriste Alexandre Plourde[587] :

> Depuis longtemps, le droit de la consommation s'est d'ailleurs affranchi de la prédominance du principe de liberté contractuelle pour laisser plus de place à des normes d'équité. Comme l'exposait le juriste Claude Masse, les bouleversements induits par la naissance de la société de consommation au Québec ont exposé les limites de la liberté contractuelle qui permettait, en pratique, à la partie la plus forte d'un contrat d'imposer sa volonté. Des mesures de protection qui écartent la

[584] M. MAČĖNAITĖ et E. KOSTA, précité, note 404, p. 186-187; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, précité, note 262, p. 45-46 et 83.

[585] V. STEEVES, précité, note 10, p. 12.

[586] D. LYON, précité, note 63, p. 8; COMMISSION D'ACCÈS À L'INFORMATION, précité, note 62, p. 37.

[587] A. PLOURDE, précité, note 571, p. 58.

> primauté du consentement ont permis de rétablir l'équité dans ces contrats, notamment à l'aide de dispositions interdisant la lésion et les clauses abusives, ou encadrant les frais pouvant être imposés à un consommateur.
>
> [Références omises]

Paradoxalement, même s'il pouvait être exercé sans les problèmes mentionnés précédemment dans cette section, le consentement n'a pas qu'une portée *individuelle* :

- Le refus de consentir à une utilisation de renseignements personnels jugée risquée, par exemple, concerne un seul mineur, mais n'affecte pas les pratiques de l'entreprise et leur effet sur les mineurs en tant que groupe[588];
- À l'inverse, consentir peut avoir un effet sur d'autres mineurs. Par exemple, accepter d'être identifié dans une photo où on apparaît peut permettre d'inférer la présence d'un ami sur celle-ci, même s'il n'est pas à son tour identifié. Activer la personnalisation des contenus en fonction des intérêts peut aussi permettre à l'entreprise de raffiner son modèle et de changer la manière dont elle présente les informations à d'autres mineurs ayant le même profil[589].

Le professeur Daniel Solove vulgarise de façon imagée cette interrelation des informations concernant les individus[590] :

> Le jeu *Clue* démontre l'interrelation des renseignements personnels et la façon dont les inférences à propos d'une personne peuvent être faites à partir des renseignements d'autres personnes. […]
>
> Supposez que le tueur soit le colonel Moutarde dans la bibliothèque avec le couteau. Avec chaque élément d'information révélé, comme le fait que M. Green ou le professeur Plum ne sont pas les coupables, on en apprend davantage à propos du colonel Moutarde. Éventuellement, en procédant par élimination, un joueur peut être certain que le tueur est le colonel Moutarde.
>
> *Clue* est une excellente démonstration que beaucoup de renseignements personnels ne sont pas seulement *relationnels* parce qu'ils impliquent plusieurs personnes dans une relation quelconque, mais aussi parce que l'information à propos de certaines personnes peut être utilisée pour faire des inférences à propos d'autres personnes. […]

En somme, de plus en plus, il convient d'envisager les risques concernant la protection des renseignements personnels non pas dans leur seule dimension individuelle, mais aussi dans leur dimension collective[591]. En ce sens, le renforcement de la responsabilité

---

588 Voir A. YOUNG, précité, note 233.

589 *Id.*, p. 4.

590 D. J. SOLOVE, précité, note 233, p. 15-16, notre traduction.

591 *Id.*, p. 12-17; J. BYRNE, E. DAY et L. RAFTREE, précité, note 233, p. 31; I. COFONE, précité, note 232, p. 53-58.

des entreprises par la Loi 25 est une piste porteuse. Dans le cas particulier des mineurs, il faut toutefois aller plus loin.

5.2.6 Autres dispositions de la Loi 25

Certaines autres dispositions de la Loi 25 souffrent de limites qui empêchent de protéger au mieux les renseignements personnels des mineurs :

- L'obligation de désactiver par défaut le profilage est enchâssée dans un article qui concerne une obligation d'information. C'est donc par déduction que s'interprète cette obligation. Vu son importance, elle devrait être plus claire, compte tenu des importantes sanctions auxquelles s'exposeront les entreprises;
- Les témoins de connexion ne sont pas visés par l'obligation d'adopter des paramètres de confidentialité élevés par défaut. Or, même si le secteur privé tente petit à petit de s'en affranchir[592], ils sont l'un des véhicules les plus communs utilisés par les entreprises pour recueillir des renseignements (observés) au sujet des mineurs. Le fait que les témoins de connexion puissent être « primaires » ou provenir de tiers risque d'entraîner un flou pour les entreprises qui auront à interpréter ces dispositions. À nouveau, il serait utile de préciser cette disposition[593];
- Malgré l'exigence d'utiliser des termes simples et clairs lors de la transmission d'informations aux personnes concernées, la Loi 25 mériterait de préciser que celles-ci doivent être adaptées aux capacités et à l'âge des mineurs.

Par ailleurs, bien que la Loi 25 ait étendu la définition de renseignement personnel[594], celle-ci n'inclut pas explicitement les renseignements inférés. Ces renseignements sont pourtant une des catégories les plus importantes pour les entreprises, et leur statut juridique incertain nuit à la protection des mineurs.

---

592 Carlós Raúl SÁNCHEZ SÁNCHEZ, Audrey PORTES et Steffie GALLIN, « La fin des "cookies tiers" ne répond pas au besoin de contrôle des internautes sur leurs données », *La Conversation* (6 avril 2022), en ligne : <https://theconversation.com/la-fin-des-cookies-tiers-ne-repond-pas-au-besoin-de-controle-des-internautes-sur-leurs-donnees-180612> (consulté le 9 avril 2022).

593 Pour la disposition miroir de la Loi sur l'accès, voir l'interprétation du SECRÉTARIAT À LA RÉFORME DES INSTITUTIONS DÉMOCRATIQUES, À L'ACCÈS À L'INFORMATION ET À LA LAÏCITÉ, « Protection par défaut », *Québec.ca* (8 avril 2022), en ligne : <https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/technologie-et-droit-a-la-protection-des-renseignements-personnels/protection-defaut> (consulté le 5 mai 2022).

594 Loi sur le privé, art. 2.

6. RECOMMANDATIONS ET PERSPECTIVES

Au terme de l'analyse présentée dans ce rapport, la Commission peut répondre à la question à l'origine de ce rapport[595], compte tenu des ajustements mentionnés dans la section 2.4 :

Oui, des mesures supplémentaires, au-delà du consentement parental, devraient être envisagées dans la Loi sur le secteur privé afin de protéger davantage les mineurs dans le contexte d'une collecte, d'une utilisation, d'une communication ou d'une conservation de leurs renseignements personnels à des fins commerciales ou à des fins de profilage commercial.

Dans cette section, la Commission formule ses recommandations quant aux mesures qui devraient être mises en place, en s'attardant aux critères qui peuvent permettre de les circonscrire. Elle offre enfin quelques perspectives conclusives.

6.1 Recommandations

Comme toute une variété d'acteurs[596], la Commission croit en l'importance des mesures visant les individus (renforcement du consentement, droits, etc.), particulièrement en matière d'éducation et de sensibilisation.

Toutefois, celles-ci ne suffisent pas pour diminuer efficacement à elles seules les risques auxquels les mineurs sont exposés dans le monde numérique. La Commission considère qu'il faut renverser le fardeau de la protection[597] et responsabiliser davantage les entreprises qui tirent profit de ces renseignements, compte tenu de l'impact majeur de leurs pratiques sur les mineurs. Cette façon de faire a l'avantage d'offrir une protection « plancher » à tous les mineurs, indépendamment de leur littératie numérique personnelle ou de celle de leurs parents; c'est une approche systémique qui mise sur les entreprises, selon la typologie présentée au début de la section 4.

La Loi 25 est déjà fermement orientée dans cette direction. Elle vise à diminuer la prépondérance du consentement, tout en le renforçant dans les situations où il est significatif. Elle étend également de manière significative les obligations incombant aux

---

595 Mandat du ministre, p. i de ce rapport.

596 En font foi les propos consensuels à cet égard tenus par des intervenants de tous horizons lors d'une conférence sur la protection de la vie privée des jeunes en ligne organisée par le Commissaire à l'information et à la protection de la vie privée de l'Ontario : Patricia KOSSEIM, « Une étoile pour la Journée de la protection des données : Former une nouvelle génération de citoyens numériques », *Commissaire à l'information et à la protection de la vie privée de l'Ontario* (3 février 2022), en ligne : <https://www.ipc.on.ca/une-etoile-pour-la-journee-de-la-protection-des-donnees-former-une-nouvelle-generation-de-citoyens-numeriques/?lang=fr> (consulté le 7 février 2022).

597 Voir J. BYRNE, E. DAY et L. RAFTREE, précité, note 233, p. 63-65; en matière de sécurisation des objets connectés, voir COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, précité, note 39, p. 19-20; voir aussi, en général D. J. SOLOVE, précité, note 233; M. MAČĖNAITĖ et E. KOSTA, précité, note 404, section 7.2; V. STEEVES, précité, note 10, p. 12.

entreprises, notamment en matière de protection de la vie privée dès la conception et par défaut. **Le principe de responsabilité appuie lui aussi l'idée que les entreprises sont celles qui doivent agir de manière à protéger, puisque ce sont elles qui génèrent les risques pour les mineurs en raison de leurs finalités commerciales.**

En ce sens, suivre les recommandations formulées ci-bas serait un prolongement logique de l'intention législative derrière la Loi 25, et permettrait de placer le Québec comme chef de file en matière de protection des renseignements personnels des mineurs dans l'environnement numérique. Par ailleurs, cela inscrirait le Québec dans le mouvement international de renforcement de la protection des mineurs en ligne, illustré par les nombreux documents et textes légaux récents recensés dans la section 4.

6.1.1 Interdire la collecte, l'utilisation et la communication de renseignements personnels de mineurs pour certaines finalités

En ce moment, la Loi sur le privé n'impose aucune restriction explicite aux finalités pouvant justifier la collecte, l'utilisation et la communication de renseignements personnels. Bien que le principe de nécessité doive être respecté pour la collecte et que la Commission a maintes fois eu l'occasion de le rappeler dans ses décisions, elle constate qu'il cède souvent la place au consentement en pratique[598]. En parallèle, la loi prévoit qu'un consentement suffit à légitimer l'utilisation ou à la communication à une autre finalité que celle justifiant la collecte (en plus de prévoir des cas où le consentement n'est pas requis pour l'utilisation ou la communication). Les entreprises jouissent donc d'une grande marge de manœuvre, pour autant qu'elles respectent leurs obligations de transparence[599].

Puisque le consentement parental n'est pas suffisant pour protéger les mineurs, la Commission est d'avis que la Loi sur le privé doit interdire explicitement certaines finalités. Celles-ci ne pourront alors plus justifier la collecte, l'utilisation ou la communication de renseignements personnels, avec ou sans consentement.

En ce sens, la Commission précise une recommandation déjà formulée dans son mémoire sur le projet de loi nº 64, où elle proposait de limiter ou d'interdire l'utilisation des renseignements personnels en certaines circonstances préjudiciables aux individus ou portant atteinte à leurs droits fondamentaux[600]. Comme le montre l'étalonnage présenté dans la section 4.2, cette voie a été retenue dans plusieurs juridictions.

Il s'agit là d'un choix de société, tout comme l'interdiction de faire de la publicité commerciale destinée à des mineurs de moins de 13 ans enchâssée dans la LPC[601]. Dans le cas de la protection des renseignements personnels des mineurs, il faut notamment prioriser l'interdiction des fins de profilage et de publicité comportementale et aux autres

---

598 Voir la section 5.2.1 de ce rapport.

599 OPTION CONSOMMATEURS, précité, note 223, p. 10 -12.

600 COMMISSION D'ACCÈS À L'INFORMATION, précité, note 62, p. 37 -38.

601 Il pourrait même prolonger l'esprit de cette interdiction; voir la p. 48 de ce rapport.

fins nuisibles de façon explicite. Cette clarté est requise pour éviter toute équivoque, notamment compte tenu des sanctions importantes prévues par la Loi 25.

Voici des exemples concrets d'interdictions à prévoir (dans l'environnement numérique, mais aussi de façon plus large) :

- La publicité comportementale fondée sur les renseignements personnels d'un mineur et adressée à ce mineur ou à ses proches[602];
- L'utilisation des habitudes de connexion ou de navigation d'un enfant pour personnaliser le moment où lui sont envoyées les notifications d'une application;
- Le profilage d'un adolescent avant l'embauche afin de prédire son potentiel de rendement au travail et de déterminer une proposition salariale personnalisée en conséquence.

Le profilage en particulier devrait toutefois rester possible dans les cas où il protège le mineur, comme lorsqu'il permet d'adapter le contenu qui lui est présenté pour éviter qu'il soit inapproprié à son âge. De même, il peut parfois servir à concevoir des outils éducatifs, ou être mobilisé par des OBNL. La Commission reconnaît en outre l'importance de s'assurer ne pas empêcher des activités légitimes, qui contribuent dans certains cas à permettre aux enfants de réaliser leurs droits.

Par conséquent, la Commission s'inspire en partie de la proposition ontarienne[603] pour trouver un équilibre dans les interdictions.

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.).

---

602 À ce sujet, voir la section 3.4.2 de ce rapport.

603 GOUVERNEMENT DE L'ONTARIO, précité, note 267.

Par ailleurs, en toutes circonstances, les entreprises ne devraient pas pouvoir vendre les renseignements personnels concernant des mineurs, et ce, afin de les préserver de toute exploitation économique.

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.

6.1.2 Inclure explicitement les renseignements inférés dans la portée de la loi

Puisqu'une bonne partie des activités commerciales des entreprises qui proposent des produits et des services numériques repose sur l'inférence de renseignements, il est primordial que ceux-ci soient protégés au même titre que tout autre renseignement personnel.

S'il est clair pour la Commission que les renseignements inférés sont déjà inclus dans la portée de la loi, cela ne semble pas être le cas pour les entreprises. S'inspirant d'une recommandation formulée dans son mémoire sur le projet de loi nº 64[604], la Commission recommande par conséquent de les mentionner explicitement dans la Loi sur le privé. Cet ajout éviterait toute ambigüité, ce qui est primordial compte tenu notamment des importantes sanctions prévues par la Loi 25. Par ailleurs, il clarifierait l'application des obligations des entreprises et les droits et recours des citoyens de tous âges lorsque ces renseignements sont en cause.

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.

6.1.3 Inscrire certains droits de l'enfant dans la loi

Pour les motifs présentés dans la section 4.1.3, la Commission estime que l'intérêt supérieur de l'enfant, son droit d'exprimer son opinion sur les questions l'intéressant et son droit d'être entendu dans toutes les procédures qui le concernent doivent être enchâssés dans la Loi sur le privé, comme le recommandait la CDPDJ dans son mémoire sur le projet de loi nº 64[605].

Ces ajouts refléteraient les valeurs du Québec, qui s'expriment déjà dans le texte d'autres lois adoptées par l'Assemblée nationale[606]. Ils enverraient un message clair aux

---

[604] COMMISSION D'ACCÈS À L'INFORMATION, précité, note 62, p. 12; voir aussi la réflexion sous-jacente aux pages 7 à 11.

[605] COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, précité, note 262, p. 83 -84.

[606] Voir par exemple, récemment, l'ajout fait par la *Loi modernisant la Loi sur la protection de la jeunesse et d'autres dispositions législatives*, L.Q. 2022, c. 11, art. 1 et 5.

entreprises qui recueillent, utilisent, communiquent ou conservent des renseignements personnels concernant des mineurs. Ils permettraient également d'arbitrer certains conflits potentiels entre un mineur et son parent et servir de principes pour guider l'interprétation des dispositions de la loi, notamment les interdictions recommandées ci-haut.

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.**

6.1.4 Garantir des protections pour tous les mineurs, adaptées à leur âge

Comme cela a transparu tout au long de ce rapport, les adolescents sont eux aussi exposés à des risques accrus. Comme le préconise l'UNICEF[607], tous les moins de 18 ans méritent une protection particulière à l'égard de leurs renseignements personnels.

Or, le mécanisme de consentement parental mis en place au Québec vise surtout les moins de 14 ans. Il laisse supposer qu'à partir de cet âge, les renseignements des adolescents peuvent, pour l'essentiel, être traités comme ceux des adultes. Du point de vue de la Commission, il est donc souhaitable que la Loi sur le privé reconnaisse à tous les mineurs, enfants comme adolescents, des besoins particuliers et le droit d'être protégés adéquatement, en accord avec l'évolution de leurs capacités. Ainsi, la protection offerte devrait toujours être accrue pour les mineurs, vu leur vulnérabilité particulière, mais devrait être adaptée à leur âge et à leurs capacités.

En matière de transparence, par exemple, les entreprises devraient avoir l'obligation de communiquer les informations aux mineurs d'une façon qui leur permette de bien comprendre ce qui sera fait de leurs renseignements personnels avant d'accepter d'utiliser un produit, un service ou une fonctionnalité. Elles pourraient entre autres recourir à des formats audiovisuels ou fournir l'information juste à temps. Une entreprise s'adressant à la fois aux enfants de 10 à 13 ans et aux adolescents de 14 à 17 ans pourrait proposer de courtes vidéos animées sur différents aspects de son utilisation des renseignements personnels pour les plus jeunes, et des textes plus détaillés entrecoupés de vidéos explicatives pour les adolescents. Même dans le cas où ce sont les parents qui consentent, puisque ceux-ci devraient toujours chercher à associer leur enfant à leur décision, l'adaptation des informations à l'âge et aux capacités du mineur est primordiale. Cet élément de transparence permettrait aussi de renforcer la littératie numérique pour le futur.

---

[607] J. BYRNE, E. DAY et L. RAFTREE, précité, note 233, p. 34 -36.

À ce chapitre, la Commission suggère de s'inspirer des catégories d'âge utilisées dans le *Children's Code*, présentées dans l'Annexe 2. Celles-ci, élaborées après des consultations avec des experts, permettent de préciser l'application de certains des principes du code selon le stade de développement des mineurs.

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.).

6.1.5 Accorder une préséance à l'opinion de l'adolescent

Avec l'âge, l'enfant accède à de plus en plus d'autonomie décisionnelle. Il accède conséquemment à de plus en plus de droits à mesure qu'il grandit. À 14 ans, notamment, les lois québécoises lui reconnaissent entre autres le droit de consentir seul à des soins médicaux le concernant[608], de demander un changement de nom[609] (ou de s'opposer seul à une telle demande)[610] ou d'accéder aux renseignements contenus dans son dossier médical[611]; plusieurs dispositions de la *Loi sur la protection de la jeunesse* lui accordent aussi une autonomie renforcée à partir de cet âge[612].

Par ailleurs, comme mentionné dans la section 5.2.4, l'intérêt du parent et celui du mineur ne sont pas toujours concordants. S'il peut être utile que le parent d'un mineur de 14 ans et plus puisse consentir en son nom lorsque leurs intérêts s'alignent, il serait important en revanche que la loi prévoie quelle opinion doit prévaloir dans le cas contraire.

S'inspirant entre autres de ce qu'envisage l'Ontario[613], mais aussi des dispositions de la Convention, la Commission estime pertinent d'accorder la préséance à l'opinion de l'adolescent dans le cas où celle-ci diverge de celle du parent. Cette mesure permettrait également d'assurer une meilleure cohérence de la Loi sur le privé avec les lois susmentionnées.

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.

---

608 C.c.Q., art. 14.

609 *Id.*, art. 60.

610 *Id.*, art. 66.

611 *Loi sur les services de santé et les services sociaux*, RLRQ, c. S-4.2, art. 17.

612 *Loi sur la protection de la jeunesse*, précité, note 329, art. 45.2, 47 à 47.3, 51.4, 51.5, 64, entre autres.

613 GOUVERNEMENT DE L'ONTARIO, précité, note 267, p. 33.

6.1.6 Étendre la protection par défaut

L'article 8.1 de la Loi sur le privé telle que modifiée par la Loi 25 concerne principalement la transparence. Or, puisque son objectif est aussi que les fonctions de profilage, de localisation ou d'identification soient désactivées par défaut, il serait souhaitable de le reformuler. Ce faisant, on éviterait toute ambigüité et on s'assurerait que les mineurs ne soient pas automatiquement soumis à un profilage autorisé, à une identification ou à une localisation sans avoir eu l'occasion de consentir (ou sans que leur parent ait eu cette occasion). La Commission recommande donc de revoir la Loi sur le privé pour affirmer plus clairement que ces fonctions doivent être désactivées par défaut.

La Commission précise ici encore qu'en clarifiant l'obligation, cette mesure bénéficierait aussi aux adultes et aux entreprises.

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.

Par ailleurs, étant donné le rôle prépondérant des témoins de connexion tiers[614] dans l'écosystème commercial, la Commission estime qu'ils ne devraient pas être exclus de l'obligation de paramétrage protecteur par défaut prévue à l'article 9.1 de la Loi sur le privé telle que modifiée par la Loi 25, à tout le moins lorsqu'ils sont utilisés sur des services fréquentés par les mineurs. La Commission revient sur ce thème dans la section 6.2.

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.

6.1.7 Exiger des analyses d'impact sur les droits des mineurs au sens large

L'article 3.3 de la Loi sur le privé telle que modifiée par la Loi 25 prévoit la réalisation d'évaluations des facteurs relatifs à la vie privée dès qu'une entreprise entame un projet d'acquisition, de développement ou de refonte d'un système d'information ou de prestation électronique de services. De l'avis de la Commission, ce libellé permet de couvrir la plupart des produits et services numériques. Afin de tenir compte des recommandations internationales concernant les analyses d'impact sur les droits des mineurs, il serait pertinent de préciser que ces évaluations doivent tenir compte également des facteurs liés à d'autres droits fondamentaux des mineurs lorsque le projet implique des renseignements personnels concernant des moins de 18 ans. En effet, tout impact sur les droits fondamentaux des mineurs résultant de la collecte, de l'utilisation, de la

[614] Voir la note 95.

communication ou de la conservation de renseignements personnels devrait être identifié et amoindri ou éliminé.

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.

6.1.8 Encadrer la conception des produits et services numériques

La façon dont sont conçus les produits et services numériques influe de manière importante sur la réalisation des droits des mineurs et sur les risques auxquels ils sont exposés. Inspirée par les recommandations et les travaux de ses homologues[615], entre autres, la Commission estime qu'il est opportun de baliser la conception de ces produits et services. Cela va également dans le sens de la protection de la vie privée dès la conception, déjà mise de l'avant dans la Loi 25.

D'abord, bien qu'elles aient probablement déjà pour effet de contrevenir aux dispositions sur le consentement ou sur la transparence, par exemple, les interfaces truquées devraient être interdites explicitement dans la Loi sur le privé[616]. Ici encore, la Commission milite pour une clarté renforcée, car ces interfaces minent la validité du consentement, qu'il soit donné par le mineur ou par un parent, et peuvent inciter à fournir plus de renseignements personnels que nécessaire.

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.

Par ailleurs, les entreprises devraient avoir l'obligation de concevoir leurs produits et services d'une façon qui respecte le droit des mineurs à la protection de leurs renseignements personnels. Par exemple, elles pourraient faciliter l'exercice des droits par des moyens techniques simples et faciles d'accès, comme l'illustre l'exemple fictif ci-contre, préparé par la CNIL[617].

---

615 *Children's code*, précité, note 325; *Fundamentals*, précité, note 149; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, précité, note 517; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, précité, note 526.

616 La Commission estime que ces interfaces contreviennent déjà à l'esprit de plusieurs dispositions de la Loi sur le privé, mais constate qu'elles sont néanmoins déployées à large échelle.

617 LABORATOIRE D'INNOVATION NUMÉRIQUE DE LA CNIL, « Konect [Tableau de bord] », *Données & Design*, en ligne : <https://design.cnil.fr/etudes-de-cas/konect/> (consulté le 4 mai 2022). Image utilisée selon les termes de la licence CC BY 3.0 FR.

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.

6.1.9 Renforcer l'éducation et la sensibilisation des mineurs et de leurs parents

La Commission conserve la conviction que la littératie numérique et la connaissance des droits en matière de renseignements personnels sont des éléments clés permettant de protéger les mineurs dans l'environnement numérique. Elle encourage le gouvernement à faire plus de place à ces notions dans le programme d'enseignement général. À ce sujet, elle réitère les recommandations formulées dans son mémoire sur la refonte du programme d'études Éthique et culture religieuse[618]. En particulier, les sujets abordés ne devraient pas se limiter à la prévention des risques interpersonnels (ex. cyberintimidation, sextorsion, etc.); il est également nécessaire d'aborder le droit à la vie privée dans toutes ses dimensions, y compris commerciale.

De son côté, la Commission entend poursuivre ses efforts de sensibilisation et de promotion de la protection des renseignements personnels auprès des jeunes. Elle a cependant besoin d'un financement rehaussé pour que ces activités puissent avoir toute l'ampleur voulue et mieux atteindre leur cible.

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.

6.2 Critères

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, la Commission reconnaît qu'il ne serait pas proportionnel de demander à toutes les entreprises, quel que

[618] COMMISSION D'ACCÈS À L'INFORMATION, précité, note 46.

soit leur secteur d'activités, d'adapter les informations aux enfants ou de changer la conception de leurs services, par exemple.

Le critère de la « probabilité d'accès », qui est repris dans quelques normes et législations internationales, est déjà présent, en quelque sorte, dans la législation québécoise. Il existe en deux principales versions :

- **Absolue (probabilité de 100 %)** : Les entreprises qui offrent des produits et services directement aux mineurs sont visées. Deux autres variantes consistent à viser a) celles qui offrent des produits et services *destinés* à des mineurs et b) celles qui ont connaissance de recueillir des renseignements personnels sur des mineurs. Cette version du critère est notamment utilisée dans la COPPA[619].
- **Relative (probabilité de plus de 50 %)** : Les entreprises couvertes sont celles qui offrent des produits et services auxquels les mineurs sont *susceptibles* d'accéder. Cette version vise à donner des obligations supplémentaires aux entreprises en fonction de l'impact réel de leurs activités sur les mineurs. On la retrouve dans la DPA18 du Royaume-Uni[620], dans la CAADCA[621], dans le CVK[622] et dans les *Fundamentals*[623]. Le ICO précise que le mot « susceptible » doit être interprété comme révélant une probabilité majoritaire (50 % +1)[624].

La version relative de ce critère est beaucoup plus forte. Elle permet de couvrir tant les produits et services visant directement les mineurs que ceux qui s'adressent à une population générale, mais qui, dans les faits, sont également utilisés par des mineurs. Ce faisant, elle évite certains problèmes constatés aux États-Unis avec la COPPA : l'expérience montre que des entreprises indiquent dans leurs conditions d'utilisation que leurs services sont interdits aux moins de 13 ans, ou s'assurent de ne jamais demander la date de naissance de l'utilisateur, et évitent ainsi d'être soumises à la loi[625]. Cette version couvre les bons produits et services et évite d'assujettir à des obligations supplémentaires toute entreprise offrant un service auquel un enfant pourrait *théoriquement* accéder.

Pour déterminer si les mineurs sont susceptibles d'accéder à un produit ou à un service, le *Children's Code* et les *Fundamentals* proposent entre autres d'en évaluer la nature, le contenu et l'attrait pour les mineurs[626]. Ces critères sont déjà enchâssés dans la LPC[627], qui prévoit que :

---

619 COPPA, art. 6501 (10) et 6502 (a) (1).

620 DPA18, art. 123.

621 CAADCA, art. 1798.99.30 (f) et 1798.99.31.

622 CVK, précité, note 514, p. 8.

623 *Fundamentals*, précité, note 149, p. 15.

624 *Children's code*, précité, note 325, p. 16.

625 M. MAČĖNAITĖ et E. KOSTA, précité, note 404, p. 168-169.

626 *Children's code*, précité, note 325, p. 17; *Fundamentals*, précité, note 149, p. 15. Les *Fundamentals* suggèrent en outre de prendre en compte l'âge des utilisateurs de produits ou services similaires et les recherches indépendantes.

627 LPC, art. 249.

> **249**. Pour déterminer si un message publicitaire est ou non destiné à des personnes de moins de treize ans, on doit tenir compte du contexte de sa présentation et notamment :
>
> **a)** de la nature et de la destination du bien annoncé;
> **b)** de la manière de présenter ce message publicitaire;
> **c)** du moment ou de l'endroit où il apparaît.
>
> […]

En somme, de l'avis de la Commission, ce critère pourrait être avantageusement utilisé dans la Loi sur le privé, puisque les éléments permettant de l'apprécier sont déjà opérants en droit québécois.

D'autres critères pertinents et complémentaires pourraient inclure l'impact potentiel d'une activité sur les mineurs, tel que proposé par l'UNICEF pour les systèmes d'intelligence artificielle[628], le niveau de risque envisagé, comme proposé dans la LIA, et l'importance des activités de l'entreprise, telle que prise en compte dans la LSN. Dans ce dernier cas, les obligations sont modulées en fonction de la taille de l'entreprise. Le défaut d'une telle approche est de laisser un angle mort pour les petites entreprises dont les produits et services rejoignent beaucoup de mineurs, comme cela peut être le cas pour une jeune pousse, par exemple[629].

6.3 Limites et perspectives

Pour clore ce rapport, la Commission souhaite attirer l'attention sur certaines limites de l'exercice auquel elle s'est livrée, qui soulèvent à leur tour des pistes de réflexion.

Premièrement, la Commission s'est appuyée sur une recherche documentaire approfondie pour produire ce rapport. Or, afin de respecter le droit des mineurs d'exprimer leur opinion sur les sujets qui les concernent, plusieurs organisations internationales recommandent de consulter les mineurs eux-mêmes avant de concevoir des politiques et des réglementations qui les touchent. La Commission souligne donc que d'éventuelles concrétisations de ses recommandations devraient être discutées avec des enfants et des adolescents, de même que des groupes représentant leurs intérêts. Par exemple, à l'international, les processus d'élaboration de codes comme le *Children's Code* ou les *Fundamentals* ont inclus des phases de consultation des mineurs.

Deuxièmement, ce rapport mentionne à de nombreuses reprises les droits fondamentaux des mineurs tels que consacrés par la Convention, ceux-ci trouvant aussi écho dans la législation québécoise. La Commission estime que 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 de mettre en œuvre certaines des recommandations formulées dans ce rapport. L'opinion de l'Office de la protection du

[628] UNICEF et MINISTÈRE DES AFFAIRES ÉTRANGÈRES DE LA FINLANDE, précité, note 55, p. 17.
[629] REVEALING REALITY, précité, note 61, p. 11.

consommateur pourrait également être sollicitée. Comme le souligne le professeur de droit Pierre Trudel, de plus en plus de questions liées à l'utilisation des données touchent à la fois la protection des renseignements personnels, la protection du consommateur et les droits fondamentaux[630].

Troisièmement, la Commission ne s'est pas penchée sur l'interaction entre l'exercice des droits liés aux renseignements personnels, le consentement, l'âge des mineurs et le droit contractuel. Comme le souligne la CNIL, ces différents éléments méritent une considération particulière afin d'assurer un arrimage entre les domaines du droit[631]. La question reste donc à explorer plus avant.

Quatrièmement, la Commission ne s'est concentrée que sur les enjeux liés aux activités commerciales impliquant des renseignements personnels de mineurs. Ce rapport ne traite donc pas de ce qui concerne le secteur public, alors que les organismes publics sont susceptibles eux aussi d'utiliser ou de communiquer des renseignements personnels à des fins préjudiciables aux mineurs[632]. Le déploiement de l'intelligence artificielle dans le système scolaire, entre autres, soulève des questions liées à la protection des renseignements personnels et aux droits des mineurs. De même, la Commission ne s'est pas penchée sur les partenariats public-privé, alors que de plus en plus d'organismes publics concluent avec le secteur privé des contrats[633] qui sont susceptibles d'avoir un impact sur la protection des renseignements personnels des mineurs. On peut penser à l'inclusion grandissante des appareils et des applications en salle de classe, à l'adhésion à différentes technologies éducatives[634] (services de gestion de classe, outils de suivi des apprentissages, etc.) ou à des systèmes de surveillance[635]. Ces questions méritent un examen plus attentif.

Enfin, ce rapport ne traite pas en détail de la question de la vérification d'âge et de la vérification du consentement parental. Très complexes, celles-ci font encore l'objet de travaux internationaux. Les recommandations de la Commission auraient pour effet de renforcer les obligations de certaines entreprises à l'égard des mineurs – elles pourraient donc souhaiter ou devoir vérifier l'âge de leurs utilisateurs en certaines circonstances afin

---

630 Pierre TRUDEL, « Sortir les États de leurs vases clos », *Le Devoir* (17 mai 2022), en ligne : <https://www.ledevoir.com/opinion/chroniques/711945/chronique-sortir-les-etats-de-leurs-silos> (consulté le 17 mai 2022).

631 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, précité, note 519; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, précité, note 522. Voir aussi les résultats d'un sondage international sur l'exercice des droits mené auprès des autorités de protection des renseignements personnels : INTERNATIONAL WORKING GROUP ON DIGITAL EDUCATION*, Cadre légal et pratiques des autorités de protection des données relatifs à l'exercice des droits des mineurs – Mise en perspective d'autres initiatives internationales sur la question des droits des mineurs*, 2020, en ligne : <https://globalprivacyassembly.org/wp-content/uploads/2020/12/Synhtese-enquete-fr-DEWG-Cadres-legaux-et-Perspectives-internationales-des-droits-des-mineurs-15.09.pdf>.

632 Toute la dimension *institutionnelle* de la vie privée, telle que décrite dans la section 2.3, était ainsi hors de la portée de ce rapport.

633 D. LYON, précité, note 63, p. 12.

634 M. GOLLOM, précité, note 43; voir aussi HUMAN RIGHTS WATCH, précité, note 43.

635 COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, *Priorités stratégiques du CIPVP 2021-2025*, 2021, p. 9-10, en ligne : <http://www.ipc.on.ca/wp-content/uploads/2021/04/ipc-strategic-priorities-2021-2025-f.pdf>; COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, précité, note 39, p. 7-9.

d'appliquer la loi ou la réglementation, l'autre option étant de l'appliquer auprès de toutes les personnes physiques[636]. En l'état, même si les recommandations de la Commission n'étaient pas suivies, l'ajout d'un seuil d'âge pour le consentement autonome du mineur dans la Loi sur le privé soulève lui-même implicitement la possibilité que soient déployés des mécanismes de vérification. Étant donné les enjeux de minimisation des données et de préservation de l'anonymat en ligne, la Commission continuera de suivre ces sujets de près. L'impact d'une éventuelle identité numérique québécoise permettant de ne révéler que certains attributs d'identité, par exemple, reste à évaluer.

[636] *Children's code*, précité, note 325, principe 3; *Fundamentals*, précité, note 149, principe 1.

RÉFÉRENCES

Textes légaux fédéraux

CHAMPAGNE, F.-P., *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 nº C-27 (16 juin 2022), 44e lég., 1re sess. (Chambre des communes), en ligne : <https://www.parl.ca/DocumentViewer/fr/44-1/projet-loi/C-27/premiere-lecture>

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, c. 5

Textes légaux québécois

Loi concernant la lutte contre le tabagisme, RLRQ, c. L-6.2

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, L.Q. 2021, c. 25

Loi modernisant la Loi sur la protection de la jeunesse et d'autres dispositions législatives, L.Q. 2022, c. 11

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

Loi sur la protection de la jeunesse, RLRQ, c. P-34.1

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

Loi sur la protection du consommateur, RLRQ, c. P-40.1

Loi sur le cinéma, RLRQ, c. C-18.1

Loi sur les infractions en matière de boissons alcooliques, RLRQ, c. I-8.1

Loi sur les services de santé et les services sociaux, RLRQ, c. S-4.2

Textes légaux internationaux

Bill Text – AB-2273 The California Age-Appropriate Design Code Act., projet de loi nº AB2273 (16 février 2022), 2021-22 (Législature de Californie), en ligne : <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273>

BLUMENTHAL, Richard, *Kids Online Safety Act*, projet de loi nº S.3663, 117e (Sénat des États-Unis), en ligne : <https://www.congress.gov/bill/117th-congress/senate-bill/3663/text>

California Consumer Privacy Act of 2018, code civil de la Californie, 1798.100 - 1798.199.100, en ligne : <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5>

Children's Online Privacy Protection Act, 15 U.S.C. c. 91 / 6501-6506, en ligne : <https://www.govinfo.gov/content/pkg/USCODE-2019-title15/html/USCODE-2019-title15-chap91.htm>

Children's Online Privacy Protection Rule, 16 CFR Part 312, en ligne : <https://www.ecfr.gov/current/title-16/part-312> (consulté le 11 janvier 2022)

Code civil du Québec, RLRQ, c. CCQ-1991

Colorado Privacy Act, SB21-190, en ligne : <https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf>

Data Protection Act 2018, 2018, c. 12, en ligne : <https://www.legislation.gov.uk/ukpga/2018/12> (consulté le 18 janvier 2022)

Data Protection Act 2018, 2018, c. 7, en ligne : <https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/index.html>

Data Protection and Digital Information Bill, projet de loi nº 143 2022-23, 2022-2023 (Chambre des communes du Royaume-Uni), en ligne : <https://bills.parliament.uk/bills/3322>

Establishing data privacy protections to strengthen a consumer's ability to access, manage, and protect their personal data, projet de loi nº SB5813 (2021), 67e législature (Législature de l'État de Washington), en ligne : <https://app.leg.wa.gov/billsummary?BillNumber=5813&Initiative=false&Year=2021>

Lei Geral de Proteção de Dados Pessoais, loi nº 13.709 du 14 août 2018, en ligne : <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>

Online Safety Bill, projet de loi nº 004 2022-23, 2022-2023 (Chambre des communes du Royaume-Uni), en ligne : <https://bills.parliament.uk/bills/3137/publications>

ORGANISATION DES NATIONS UNIES, *Convention relative aux droits de l'enfant*, (1989), traité nº 27531, en ligne : <https://www.ohchr.org/FR/ProfessionalInterest/Pages/CRC.aspx>

Personal Information Protection Act, S.O.A. 2003, c. P-6.5, en ligne : <https://www.qp.alberta.ca/documents/Acts/P06P5.pdf>

Personal Information Protection Act, SBC 2003, c. 63, en ligne : <https://www.bclaws.ca/civix/document/id/complete/statreg/03063_01>

Proposition de Législation sur les services numériques, 2020/0361(COD) (1 février 2022), Conseil de l'Union européenne, en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CONSIL:ST_5620_2022_INIT&from=EN>

Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, 2021/0106(COD) (21 avril 2021), Commission européenne, en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0206&from=EN>

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) (Texte présentant de l'intérêt pour l'EEE), (2016), OOJ 2016 L 119/1, en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679>

The Personal Data Protection Bill 2019, projet de loi nº373-2019, 17e (Lok Sabha), en ligne : <https://prsindia.org/files/bills_acts/bills_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf>

Affaires

Enquête à l'égard de Clearview AI Inc., dossier 1023158-S, 14 décembre 2021, en ligne : <https://decisions.cai.gouv.qc.ca/cai/ss/fr/item/518218/index.do> (consulté le 31 mars 2022)

Laval (Société de transport de la Ville de) c. *X*, [2003] C.A.I. 667 (C.Q.)

Irwin Toy Ltd. c. Québec (Procureur général), [1989] 1 RCS 927, en ligne : <https://scc-csc.lexum.com/scc-csc/scc-csc/fr/item/443/index.do>

M.C. c. R.S., 2022 QCCS 1260, en ligne : <https://www.canlii.org/fr/qc/qccs/doc/2022/2022qccs1260/2022qccs1260.html> (consulté le 10 mai 2022)

X c. Centre d'expertise Marie-Vincent, en ligne : <https://www.canlii.org/fr/qc/qccai/doc/2021/2021qccai203/2021qccai203.html>

Monographies

DIANA PAOLA ALVAREZ BAUTISTA, *Vie privée des mineurs en ligne: protection des données personnelles. Étude comparée entre le droit canadien, américain et celui de l'Union européenne*, mémoire de maîtrise, Montréal, Université de Montréal, 2021, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/25850/Alvarez_Bautista_Diana_Paola_2021_memoire.pdf>

ZUBOFF, S., *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, New York (É-U), PublicAffairs, 2019

Articles de revue, actes de conférences et chapitres de livre

BINNS, R., U. LYNGS, M. VAN KLEEK, J. ZHAO, T. LIBERT et N. SHADBOLT, « Third Party Tracking in the Mobile Ecosystem », dans *Proceedings of the 10th ACM Conference on Web Science*, Amsterdam Netherlands, ACM, 2018, p. 23-31, DOI : 10.1145/3201064.3201089

BOCK, M. et M. WIENER, « Towards a Taxonomy of Digital Business Models – Conceptual Dimensions and Empirical Illustrations », dans *ICIS 2017 Proceedings*, Séoul (Corée du Sud), 2017, en ligne : <https://www.researchgate.net/profile/Maximilian-Bock/publication/325627453_Towards_a_Taxonomy_of_Digital_Business_Models_-_Conceptual_Dimensions_and_Empirical_Illustrations/links/5b1950eea6fdcca67b635a99/Towards-a-Taxonomy-of-Digital-Business-Models-Conceptual-Dimensions-and-Empirical-Illustrations.pdf>

CITRON, D. K. et D. J. SOLOVE, « Privacy Harms », *SSRN Journal* 2021, DOI : 10.2139/ssrn.3782222

COFONE, I., « Privacy Standing », *University of Illinois Law Review* (à paraître), en ligne : <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782887>

DESIMPELAERE, L., L. HUDDERS et D. V. de SOMPEL, « Children's and Parents' Perceptions of Online Commercial Data Practices: A Qualitative Study », (2020) 8-4 *Media and Communication* 163-174, DOI : 10.17645/mac.v8i4.3232

DONOVAN, S., « "Sharenting": The Forgotten Children of the GDPR », (2020) 4-03/2020 *Peace Human Rights Governance* 35-59, DOI : 10.14658/pupj-phrg-2020-1-2

EKAMBARANATHAN, A., J. ZHAO et M. VAN KLEEK, « "Money makes the world go around": Identifying Barriers to Better Privacy in Children's Apps From Developers' Perspectives », dans *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, Yokohama Japan, ACM, 2021, p. 1-15, DOI : 10.1145/3411764.3445599

GAUTRAIS, V. et A. PORCIN, « Les 7 péchés de la L.p.c. : actions et omissions applicables au commerce électronique », (2009) 43-3 *Revue juridique Thémis* 45

GRAßL, P., H. SCHRAFFENBERGER, F. Z. BORGESIUS et M. BUIJZEN, « Dark and Bright Patterns in Cookie Consent Requests », (2021) 3-1 *Journal of Digital Social Research* 1-38, DOI : 10.33621/jdsr.v3i1.54

KING, D. L., P. H. DELFABBRO, S. M. GAINSBURY, M. DREIER, N. GREER et J. BILLIEUX, « Unfair play? Video games as exploitative monetized services: An examination of game patents from a consumer protection perspective », (2019) 101 *Computers in Human Behavior* 131-143, DOI : 10.1016/j.chb.2019.07.017

KING, J. *Dark Patterns & Manipulative Design*, présentation, Sacramento (Californie), California Privacy Protection Agency Pre-Rulemaking Informational Sessions, 29 mars 2022

LIVINGSTONE, S. et M. STOILOVA, « The 4Cs: Classifying Online Risk to Children », *CO:RE Short Report Series on Key Topics* 2021, DOI : 10.21241/SSOAR.71817

LUPTON, D. et B. WILLIAMSON, « The datafied child: The dataveillance of children and implications for their rights », (2017) 19-5 *New Media & Society* 780-794, DOI : 10.1177/1461444816686328

MAČĖNAITĖ, M., « Protecting Children Online: Combining the Rationale and Rules of Personal Data Protection Law and Consumer Protection Law », dans Mor BAKHOUM, Beatriz CONDE GALLEGO, Mark-Oliver MACKENRODT et Gintarė SURBLYTĖ-NAMAVIČIENĖ (dir.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?*, coll. MPI Studies on Intellectual Property and Competition Law, Berlin, Heidelberg, Springer, 2018, p. 331-375, en ligne : <https://doi.org/10.1007/978-3-662-57646-5_13> (consulté le 6 décembre 2021)

MAČĖNAITĖ, M. et E. KOSTA, « Consent for processing children's personal data in the EU: following in US footsteps? », (2017) 26-2 *Information & Communications Technology Law* 146-197, DOI : 10.1080/13600834.2017.1321096

MASCHERONI, G., « Researching datafied children as data citizens », *Journal of Children and Media* 2018.1-7, DOI : 10.1080/17482798.2018.1521677

MCCULLAGH, K., « The General Data Protection Regulation: A Partial Success for Children on Social Network Sites? », dans Tobias BRÄUTIGAM et Samuli MIETTINEN (dir.), *Data Protection, Privacy and European Regulation in the Digital Age*, Helsinki, Unigrafia, 2016, p. 110-139, en ligne : <https://papers.ssrn.com/abstract=2985724>

NARAYANAN, A., A. MATHUR, M. CHETTY et M. KSHIRSAGAR, « Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces », (2020) 18-2 *Queue* Pages 10:67-Pages 10:92, DOI : 10.1145/3400899.3400901

PLOURDE, A., « 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, Éditions Yvon Blais, 2019, p. 35-66

PRIOR, S. et N. COULL, « Parents Unwittingly Leak Their Children's Data: A GDPR Time Bomb? », dans Abbas MOALLEM (dir.), *HCI for Cybersecurity, Privacy and Trust*, coll. Lecture Notes in Computer Science, Cham, Springer International Publishing, 2020, p. 471-486, DOI : 10.1007/978-3-030-50309-3_31

SOLOVE, D. J., « The Limitations of Privacy Rights », (à paraître) 98 *Notre Dame Law Review*, DOI : 10.2139/ssrn.4024790

STAKSRUD, E. et S. LIVINGSTONE, « Children and online risk: Powerless victims or resourceful participants? », (2009) 12-3 *Information, Communication & Society* 364-387

VAN DER HOF, S., « 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

WALDMAN, A. E., « Cognitive biases, dark patterns, and the 'privacy paradox' », (2020) 31 *Current Opinion in Psychology* 105-109, DOI : 10.1016/j.copsyc.2019.08.025

ZHAO, J., G. WANG, C. DALLY, P. SLOVAK, J. EDBROOKE-CHILDS, M. VAN KLEEK et N. SHADBOLT, « "I make up a silly name": Understanding Children's Perception of Privacy Risks Online », dans *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, Glasgow Scotland Uk, ACM, 2019, p. 1-13, DOI : 10.1145/3290605.3300336

Rapports et documents gouvernementaux

5RIGHTS FOUNDATION, *Tick to Agree - Age appropriate presentation of published terms*, 2021, en ligne : <https://5rightsfoundation.com/TicktoAgree-Age_appropriate_presentation_of_published_terms.pdf>

———, *But how do they know it's a child?*, 2021, en ligne : <https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf>

ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE, *La famille numérique (2021)*, 2022, en ligne : <https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/2022-03-la-famille-numerique>

———, *Portrait numérique des foyers québécois (2021)*, 2022, en ligne : <https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/2022-01-portrait-numerique-des-foyers-quebecois>

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Avis 2/2009 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles)*, 398/09/EN WP 160, 2009, en ligne : <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_fr.pdf>

ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE, *Résolution sur les droits numériques des enfants*, Mexico, 2021, en ligne : <https://globalprivacyassembly.org/wp-content/uploads/2021/12/Resolution-sur-les-droits-numeriques-des-enfants-GPA-finale-le-21.10.2021.FR_.pdf>

AUXIER, B., M. ANDERSON, A. PERRIN et E. TURNER, *Parenting Children in the Age of Screens*, Pew Research Center, 2020, en ligne : <https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2020/07/PI_2020.07.28_kids-and-screens_FINAL.pdf>

BERNARD, C., *Les droits de l'enfant et des parents sur les dossiers qui concernent l'enfant : exposé descriptif,* Cat. 2. 176.5, Commission des droits de la personne et des droits de la jeunesse, 2003, en ligne : <https://www.cdpdj.qc.ca/Publications/droits_enfants_parents_ expose.pdf>

BRISSON-BOIVIN, K., *Le bien-être numérique des familles canadiennes*, Ottawa, HabiloMédias, 2018, en ligne : <https://habilomedias.ca/sites/mediasmarts/files/publication-report/full/numerique-familles-canadiennes.pdf>

BRISSON-BOIVIN, K. et S. MCALEESE, *Averti aux algorithmes : Les jeunes Canadiens discutent l'intelligence artificielle et la confidentialité*, HabiloMédias, 2021, en ligne : <https://habilomedias.ca/recherche-et-politique/averti-aux-algorithmes%C2%A0-les-jeunes-canadiens-discutent-l%E2%80%99intelligence-artificielle-et-la>

BYRNE, J., E. DAY et L. RAFTREE, *UNICEF Global Insight Data Governance Manifesto*, 2021, en ligne : <https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf>

CHAUDRON, S., R. DI GIOIA et M. GEMO, *Young children (0-8) and digital technology: a qualitative study across Europe.*, European Commission – Joint Research Centre, Luxembourg, Publications Office, 2018, en ligne : <https://data.europa.eu/doi/10.2760/294383> (consulté le 25 mars 2022)

COMITÉ DES DROITS DE L'ENFANT DE L'ORGANISATION DES NATIONS UNIES, *Observation générale n° 14 (2013) sur le droit de l'enfant à ce que son intérêt supérieur soit une considération primordiale*, 2013, en ligne : <http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2f5F0vEAXPu5AtSWvliDPBvwUDNUcLY%2bjlY9LwV%2bqu%2f76ghnFz5ngXgCakqefOzjKZHk9XN8vDnGlPnxGqaEEn4Buo1n> (consulté le 16 décembre 2021)

———, *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%2fPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2f5F0vEG%2bcAAx34gC78FwvnmZXGFsdFXGQsWU46nx%2b5vAg3QbGXlnOwo3Oquj8nN7ltX6yUYoRpe7N%2b7Q6mEUIz2mfWi> (consulté le 16 décembre 2021)

COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679*, WP251rev.01, 2018, en ligne : <https://ec.europa.eu/newsroom/article29/items/612053>

———, *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>

———, *Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognise and avoid them*, 2022, en ligne : <https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf>

COMMISSAIRE À L'ENFANCE DU ROYAUME-UNI, *Who knows what about me? A Children's Commissioner report into the collection and sharing of children's data*, 2018, en ligne : <https://dera.ioe.ac.uk//32673/1/who-knows-what-about-me.pdf>

COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, *Commentaires du CIPVP sur le livre blanc du gouvernement de l'Ontario intitulé Modernisation de la protection de la vie privée en Ontario*, 2021, en ligne : <http://www.ipc.on.ca/wp-content/uploads/2021/09/2021-09-03-commentaires-du-cipvp-le-livre-blanc-du-gouv-on-modernisation-protection-vie-privee-en-on.pdf>

———, *Priorités stratégiques du CIPVP 2021-2025*, 2021, en ligne : <http://www.ipc.on.ca/wp-content/uploads/2021/04/ipc-strategic-priorities-2021-2025-f.pdf>

COMMISSAIRES À LA PROTECTION DE LA VIE PRIVÉE ET RESPONSABLES DE LA SURVEILLANCE DE LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *La vie privée des enfants en ligne – Résolution des commissaires à la protection de la vie privée et responsables de la surveillance de la protection de la vie privée du Canada*, Regina, Saskatchewan, 2008, en ligne : <https://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_080604/?wbdisable=true>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, COMMISSION D'ACCÈS À L'INFORMATION, BUREAU DU COMMISSAIRE À L'INFORMATION ET À LA VIE PRIVÉE DE L'ABERTA, et BUREAU DU COMMISSAIRE À L'INFORMATION ET À LA VIE PRIVÉE DE LA COLOMBIE-BRITANNIQUE, *Rapport de conclusions - Enquête conjointe sur le Groupe TDL Corporation (exploitant franchiseur de Tim Hortons au Canada)*, 2022, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_TDL_RF_FR.pdf> (consulté le 31 mars 2022)

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Rapport de conclusions d'enquête en vertu de la LPRPDE nº 2018-001 : Un manufacturier de jouets connectés améliore les mesures de sécurité pour protéger adéquatement les renseignements d'enfants », *Commissariat à la protection de la vie privée du Canada* (8 janvier 2018), en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2018/lprpde-2018-001/> (consulté le 9 décembre 2021)

COMMISSION D'ACCÈS À L'INFORMATION, *Une réforme de l'accès à l'information : le choix de la transparence* (rapport quinquennal 2002), 2002, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_RQ_2002.pdf>

———, *Technologies et vie privée à l'heure des choix de société* (rapport quinquennal 2011), 2011, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_RQ_2011.pdf>

———, *Rétablir l'équilibre* (rapport quinquennal 2016), Québec, 2016, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf>

———, *Révision du programme d'études Éthique et culture religieuse – Mémoire de la Commission d'accès à l'information présenté au Secteur de l'éducation préscolaire et de l'enseignement primaire et secondaire du ministère de l'Éducation et de l'Enseignement supérieur*, 2020, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_M_ECR_MEES_vf.pdf>

———, *Projet de loi nº 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*, Québec, 2020, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_M_projet_loi_64_modernisation_PRP.pdf>

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 nº 64, Loi modernisant les dispositions législatives en matière de protection des renseignements personnels*, Cat. 2.412.42.8, 2020, en ligne : <https://www.cdpdj.qc.ca/storage/app/media/publications/memoire_PL64_renseignements-personnels.pdf>

COMMISSION EUROPÉENNE, *Une décennie numérique pour les enfants et les jeunes : la nouvelle stratégie européenne pour un internet mieux adapté aux enfants*, COM(2022) 212 final, 2022, en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=COM:2022:212:FIN>

CONSEIL DE L'EUROPE, *Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique*, Recommandation CM/Rec(2018)7 du Comité des Ministres, 2018, en ligne : <https://rm.coe.int/lignes-directrices-relatives-au-respect-a-la-protection-et-a-la-realis/16808d881b>

———, *Recommandation CM/Rec(2021)8 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre du profilage*, Strasbourg, Editions du Conseil de l'Europe, 2021, en ligne : <https://search.coe.int/cm/pages/result_details.aspx?ObjectId=0900001680a46148>

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>

DENNIS, J., K. JANECEK, I. GAYTANDJIEVA, A. POTTER, E. UDOH, A. FETANI, M. FERRARESI et V. PRESCOTT, *Comparing privacy laws: GDPR v. CCPA & CPRA*, OneTrust DataGuidance / Newmeyer & Dillion LLP, 2022, en ligne : <https://www.dataguidance.com/sites/default/files/20220127_onetrust_dataguidance_gdpr_v_ccpa_and_cpra_report.pdf>

FORUM ÉCONOMIQUE MONDIAL, *Artificial Intelligence for Children - Toolkit*, 2022, en ligne : <https://www3.weforum.org/docs/WEF_Artificial_Intelligence_for_Children_2022.pdf>

FRÉCHETTE, J., *Être parent à l'ère du numérique – Le partage de renseignements personnels sur les réseaux sociaux et ses conséquences sur le droit à la vie privée et à l'image des enfants*, Option consommateurs, 2019, en ligne : <https://option-consommateurs.org/wp-content/uploads/2019/09/parentalite-numerique-oc.pdf>

FUTURE OF PRIVACY FORUM, *The State of Play: Verifiable Parental Consent and COPPA (Discussion draft)*, 2021, en ligne : <https://fpf.org/wp-content/uploads/2021/11/FPF-The-State-of-Play-Verifiable-Parental-Consent-and-COPPA.pdf> (consulté le 6 décembre 2021)

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto*, 2018, en ligne : <https://www.gpdp.it/documents/10160/0/ALLEGATO+1+Elenco+delle+tipologie+di+trattamenti+soggetti+al+meccanismo+di+coerenza+da+sottoporre+a+valutazione+di+impatto.pdf/b9ceefa9-dd65-df86-fed4-df3c3570f59d?version=1.11>

GOUVERNEMENT DE L'ONTARIO, *Modernisation de la protection de la vie privée en Ontario - Autonomiser les Ontariens et favoriser l'économie numérique*, 2020, en ligne : <https://www.ontariocanada.com/registry/showAttachment.do?postingId=37468&attachmentId=49464>

GROUPE DE TRAVAIL DES COMMISSAIRES À LA VIE PRIVÉE ET DES DÉFENSEURS CANADIENS DES ENFANTS ET DES JEUNES SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DES ENFANTS EN LIGNE, *Il devrait y avoir une loi : Les sauts périlleux de la vie privée des enfants au 21e siècle*, 2009, en ligne : <https://www.bibliotheque.assnat.qc.ca/DepotNumerique_v2/AffichageFichier.aspx?idf=32966>

HUMAN RIGHTS WATCH, *"How Dare They Peep into My Private Life?" Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic*, 2022, en ligne : <https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments> (consulté le 8 juin 2022)

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>

———, *Age Assurance for the Children's Code*, 2021, en ligne : <https://ico.org.uk/media/about-the-ico/documents/4018659/age-assurance-opinion-202110.pdf>

———, *Information Commissioner's opinion: Age Assurance for the Children's Code*, 2021, en ligne : <https://ico.org.uk/media/about-the-ico/documents/4018659/age-assurance-opinion-202110.pdf>

INSTITUT FRANÇAIS D'OPINION PUBLIQUE, *Les comportements digitaux des enfants - Regards croisés parents et enfants*, Commission nationale de l'informatique et des libertés, 2020, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/sondage_ifop_-_comportements_digitaux_des_enfants_-_fevrier_2020.pdf>

INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS, *Resolution on Children's Online Privacy*, Strasbourg, 2008, en ligne : <http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Childrens-Online-Privacy-.pdf>

INTERNATIONAL CONSUMER PROTECTION AND ENFORCEMENT NETWORK, *Best Practice Principles for Marketing Practices Directed Towards Children Online*, 2020, en ligne : <https://icpen.org/sites/default/files/2020-06/ICPEN%20-

%20Best%20Practice%20Principles%20for%20Marketing%20Practices%20Directed%20Towards%20Children%20Online%202020.pdf>

INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, *Protecting the Privacy of Children in Online Services - Working paper*, 2019, en ligne : <https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2019/2019-IWGDPT-Working_Paper_Online_Services_for_Children.pdf>

INTERNATIONAL WORKING GROUP ON DIGITAL EDUCATION, *Cadre légal et pratiques des autorités de protection des données relatifs à l'exercice des droits des mineurs – Mise en perspective d'autres initiatives internationales sur la question des droits des mineurs*, 2020, en ligne : <https://globalprivacyassembly.org/wp-content/uploads/2020/12/Synhtese-enquete-fr-DEWG-Cadres-legaux-et-Perspectives-internationales-des-droits-des-mineurs-15.09.pdf>

JOHNSON, M., V. STEEVES, L. R. SHADE et G. FORAN, *Partager ou ne pas partager : Comment les adolescents prennent des décisions en matière de vie privée à propos des photos sur les réseaux sociaux*, HabiloMédias, 2017, en ligne : <https://habilomedias.ca/sites/mediasmarts/files/publication-report/full/partager-ou-ne-pas-partager.pdf>

JOINT COMMITTEE ON THE PERSONAL DATA PROTECTION BILL, 2019, *Report of the Joint Committee on the Personal Data Protection Bill, 2019*, Lok Sabha, 2021, en ligne : <https://www.ahlawatassociates.com/wp-content/uploads/2021/12/17-Joint-Committee-on-the-Personal-Data-Protection-Bill-2019.pdf> (consulté le 2 février 2022)

KIDRON, B., A. EVANS et J. AFIA, *Disrupted Childhood: The Cost of Persuasive Design*, 5Rights Foundation, 2018, en ligne : <https://5rightsfoundation.com/static/5Rights-Disrupted-Childhood.pdf>

LAUZON, J., M. J. SIMKIN et M.-H. BEAULIEU, *La publicité destinée aux enfants : Identifier la meilleure protection possible*, Option consommateurs, 2008, en ligne : <https://www.option-consommateurs.org/documents/principal/fr/File/rapports/pratiques_commerciales/oc_ic_publicite_enfant_200804.pdf>

LIVINGSTONE, S., M. STOILOVA et R. NANDAGIRI, *Children's data and privacy online – Growing up in a digital age. An evidence review*, London School of Economics and Political Sciences, 2019, en ligne : <https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review.pdf>

LUPIÁÑEZ-VILLANUEVA, F., A. BOLUDA, F. BOGLIACINO, G. LIVA, L. LECHARDOY et T. 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, en ligne : <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418>

LYON, D., *Au-delà de la surveillance des mégadonnées - Liberté et équité. Rapport pour tous les Canadiens et Canadiennes*, Surveillance Studies Centre / Queen's University, 2022, en ligne : <https://www.sscqueens.org/sites/sscqueens.org/files/bds_rapport_fr_2022-05-17.pdf>

MCALEESE, S., M. JOHNSON et M. LADOUCEUR, *Les jeunes Canadiens s'expriment : une recherche qualitative sur la protection de la vie privée et le consentement*, Ottawa,

HabiloMédias, 2020, en ligne : <https://habilomedias.ca/sites/default/files/publication-report/full/rapport_jeunes_canadiens_sexpriment.pdf>

MONTCALM, V., A. PLOURDE et E. THÉRIAULT, *Enfants sous écoute – La protection de la vie privée dans l'environnement des jouets intelligents*, Option consommateurs, 2018, en ligne : <https://option-consommateurs.org/wp-content/uploads/2018/11/oc-jouets-i-rapport-final.pdf>

———, *Enfants sous écoute – La protection de la vie privée dans l'environnement des jouets intelligents*, Option consommateurs, 2018, en ligne : <https://option-consommateurs.org/wp-content/uploads/2018/11/oc-jouets-i-rapport-final.pdf>

OCDE, *Children in the digital environment - Revised typology of risks*, OCDE Digital Economy Papers, 302, 2021, en ligne : <https://www.oecd-ilibrary.org/science-and-technology/children-in-the-digital-environment_9b8f222e-en;jsessionid=-6yCMDDpCH2dHXQIOUo_-TiV.ip-10-240-5-51>

OFFICE DE LA PROTECTION DU CONSOMMATEUR, *Vos enfants et la pub*, 2008, en ligne : <https://www.opc.gouv.qc.ca/fileadmin/media/documents/consommateur/sujet/publicite-pratique-illegale/EnfantsPub.pdf>

———, *Publicité destinée aux enfants de moins de 13 ans – Guide d'application des articles 248 et 249, Loi sur la protection du consommateur*, 2012, en ligne : <https://cdn.opc.gouv.qc.ca/media/documents/consommateur/bien-service/index-sujet/guide-application.pdf?1379440600>

OPTION CONSOMMATEURS, *Projet de loi n^{o} 64 – Loi modernisant des dispositions législatives en matière de protection des renseignements personnels - Commentaires d'Option consommateurs présentés à la Commission des institutions*, 2020, en ligne : <https://option-consommateurs.org/wp-content/uploads/2020/09/option-consommateurs-pl64-memoire.pdf>

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *Recommandation du Conseil sur les enfants dans l'environnement numérique*, OCDE/LEGAL/0389, Organisation de coopération et de développement économiques, 2021, en ligne : <https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0389%20> (consulté le 16 décembre 2021)

PLOURDE, A., *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, en ligne : <https://option-consommateurs.org/wp-content/uploads/2017/06/option-consommateurs-2014-2015-gratuite-rapport.pdf>

REVEALING REALITY, *Towards a better digital future – Informing the Age Appropriate Design Code*, Information Commissioner's Office, 2019, en ligne : <https://ico.org.uk/media/about-the-ico/consultations/2614763/ico-rr-report-0703.pdf>

———, *Pathways: How digital design puts children at risk*, 5Rights Foundation, 2021, en ligne : <https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf>

STEEVES, V., *Jeunes Canadiens dans un monde branché, Phase III : Tendances et recommandations*, Ottawa, HabiloMédias, 2015, en ligne : <https://habilomedias.ca/sites/mediasmarts/files/publication-report/full/jcmbiii_tendances_recommandations_rapport.pdf>

———, *It's Time for a Change: Rethinking Policies to Protect Children's Rights in a Datafied World*, coll. Kids & Technology Essay Series, 2021, en ligne : <https://www.mediatechdemocracy.com/s/Steeves_Nov21.pdf>

STOILOVA, M., S. LIVINGSTONE et R. 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>

THE CENTER FOR INDUSTRY SELF-REGULATION, *A Roadmap for Considering Teen Privacy & Safety*, 2022, en ligne : <https://bbbnp-bbbp-stf-use1-01.s3.amazonaws.com/docs/librariesprovider5/default-document-library/tapp_roadmap.pdf>

UNICEF et MINISTÈRE DES AFFAIRES ÉTRANGÈRES DE LA FINLANDE, *Policy guidance on AI for children*, UNICEF, 2020, en ligne : <https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf>

UNIVERSITY OF LEIDEN et WAAG ORGANISATION, *Code for Children's Rights*, Ministère de l'Intérieur et des Relations du Royaume, 2021, en ligne : <https://codevoorkinderrechten.nl/wp-content/uploads/2021/07/Code-voor-Kinderrechten-Wordversie_EN.pdf>

YOUNG, A., *Responsible group data for children*, UNICEF, 2020, en ligne : <https://www.unicef.org/globalinsight/media/1251/file/UNICEF-Global-Insight-DataGov-group-data-issue-brief-2020.pdf>

Articles de journaux ou de magazines

DUHAMEL, F.-X., « Plus de temps d'écran pour les adolescents, dont beaucoup sont tannés », *La Presse* (18 mai 2022), en ligne : <https://www.lapresse.ca/actualites/2022-05-18/plus-de-temps-d-ecran-pour-les-adolescents-dont-beaucoup-sont-tannes.php> (consulté le 25 mai 2022)

BHANDARI, V., « Facing the consequences of the Data Protection Bill on children's digital privacy », *Medianama* (16 février 2022), en ligne : <https://www.medianama.com/2022/02/223-consequences-data-protection-bill-children-digital-privacy/> (consulté le 28 février 2022)

GOLLOM, M., « Educational tech, including CBC Kids, harvested personal data from children, new report claims », *CBC News* (25 mai 2022), en ligne : <https://www.cbc.ca/news/canada/cbc-kids-personal-data-educational-technology-1.6465739> (consulté le 2 juin 2022)

HAINSWORTH, J., « B.C. commissioner mulling over privacy code for children », *Vancouver Is Awesome* (22 mars 2022), en ligne : <https://www.vancouverisawesome.com/highlights/bc-commissioner-mulling-over-privacy-code-for-children-5182227> (consulté le 25 avril 2022)

HARRIS, R., « 72M data points collected on children in spite of COPPA », *App Developer Magazine* (27 décembre 2017), en ligne : <https://appdevelopermagazine.com/72m-data-points-collected-on-children-in-spite-of-coppa/> (consulté le 9 mars 2022)

HILL, K., « The Secretive Company That Might End Privacy as We Know It », *The New York Times* (18 janvier 2020), en ligne : <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> (consulté le 31 mars 2022)

KEEGAN, J. et A. NG, « The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users – The Markup », *The Markup* (6 décembre 2021), en ligne : <https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user> (consulté le 8 décembre 2021)

LE MONDE et AGENCE FRANCE-PRESSE, « Une lanceuse d'alerte accuse Facebook de "choisir le profit plutôt que la sécurité" de ses utilisateurs », *Le Monde.fr* (3 octobre 2021), en ligne : <https://www.lemonde.fr/pixels/article/2021/10/03/facebook-se-defend-d-avoir-contribue-a-l-assaut-du-capitole-le-6-janvier_6096981_4408996.html> (consulté le 31 mars 2022)

LELOUP, D., « Santé mentale des adolescents : Instagram mis en difficulté par les sénateurs américains », *Le Monde.fr* (30 septembre 2021), en ligne : <https://www.lemonde.fr/pixels/article/2021/09/30/sante-mentale-des-adolescents-audition-a-haut-risque-pour-instagram-au-senat-americain_6096605_4408996.html> (consulté le 31 mars 2022)

SINGH, M., « India withdraws personal data bill that alarmed tech giants », *TechCrunch* (4 août 2022), en ligne : <https://techcrunch.com/2022/08/03/india-government-to-withdraw-personal-data-protection-bill/> (consulté le 11 août 2022)

TRUDEL, P., « Sortir les États de leurs vases clos », *Le Devoir* (17 mai 2022), en ligne : <https://www.ledevoir.com/opinion/chroniques/711945/chronique-sortir-les-etats-de-leurs-silos> (consulté le 17 mai 2022)

Pages Web

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

AGENCE DE LA SANTÉ PUBLIQUE DU CANADA, « Alerte COVID : L'appli canadienne d'avis d'exposition à la COVID-19 » (31 juillet 2020), en ligne : <https://www.canada.ca/fr/sante-publique/services/publications/maladies-et-affections/appli-alerte-covid.html> (consulté le 10 août 2020)

CAGNONI, A. C., « How Brazil regulates children's privacy and what to expect under the new data protection law », *International Association of Privacy Professionals* (29 octobre 2019), en ligne : <https://iapp.org/news/a/how-brazil-regulates-childrens-privacy-and-what-to-expect-under-the-new-data-protection-law/> (consulté le 29 avril 2022)

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Les technologies de surveillance appliquées aux enfants », *Commissariat à la protection de la vie privée du Canada* (14 mars 2013), 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/2012/opc_201210/> (consulté le 31 janvier 2022)

COMMISSION EUROPÉENNE, « Digital Services Package: Commission welcomes the adoption by the European Parliament of the EU's new rulebook for digital services »,

Commission européenne (5 juillet 2022), en ligne : <https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_4313> (consulté le 5 juillet 2022)

DAY, E., « Data governance for children: An emerging priority area for privacy professionals », *Unicef* (19 mai 2022), en ligne : <https://www.unicef.org/globalinsight/stories/data-governance-children-emerging-priority-area-privacy-professionals> (consulté le 25 mai 2022)

ÉDITIONS LAROUSSE, « Définitions : médiatiser - Dictionnaire de français Larousse », *Dictionnaire Larousse en ligne*, en ligne : <https://www.larousse.fr/dictionnaires/francais/m%C3%A9diatiser/50110> (consulté le 9 mars 2022)

EDWARDS, J., « Blog: Why protecting children online in UK living rooms starts 5,000 miles away », *Information Commissioner's Office* (11 avril 2022), en ligne : <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2022/04/why-protecting-children-online-in-uk-living-rooms-starts-5-000-miles-away> (consulté le 10 mai 2022)

HABILOMÉDIAS, « HabiloMédias.ca », en ligne : <https://habilomedias.ca/> (consulté le 16 mai 2022)

JOHNSTON, A., « Big Tech, Individuation, and why Privacy must become the Law of Everything », *Salinger Privacy - Big Tech blog* (22 mars 2022), en ligne : <https://www.salingerprivacy.com.au/2022/03/22/big-tech-blog/?utm_source=pocket_mylist> (consulté le 31 mars 2022)

KOSSEIM, P., « Une étoile pour la Journée de la protection des données : Former une nouvelle génération de citoyens numériques », *Commissaire à l'information et à la protection de la vie privée de l'Ontario* (3 février 2022), en ligne : <https://www.ipc.on.ca/une-etoile-pour-la-journee-de-la-protection-des-donnees-former-une-nouvelle-generation-de-citoyens-numeriques/?lang=fr> (consulté le 7 février 2022)

LABORATOIRE D'INNOVATION NUMÉRIQUE DE LA CNIL, « Konect [Tableau de bord] », *Données & Design*, en ligne : <https://design.cnil.fr/etudes-de-cas/konect/> (consulté le 4 mai 2022)

LE CROSNIER, H., « Publicité ciblée : l'économie de l'attention », *L'observatoire mesdatasetmoi.fr* (27 mars 2017), en ligne : <https://www.mesdatasetmoi-observatoire.fr/article/l-economie-de-lattention> (consulté le 17 mars 2022)

LEMOS, R., « Brazilian General Data Protection Law (LGPD, English translation) », *IAPP* (octobre 2020), en ligne : <https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/> (consulté le 28 avril 2022)

OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Grand dictionnaire terminologique - mise en données », *Grand dictionnaire terminologique* (2014), en ligne : <https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26523020> (consulté le 9 mars 2022)

———, « Grand dictionnaire terminologique - notification poussée », *Grand dictionnaire terminologique* (2014), en ligne : <https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26527127> (consulté le 17 mars 2022)

———, « interface truquée », *Grand dictionnaire terminologique* (2018), en ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26544648> (consulté le 20 septembre 2020)

———, « Grand dictionnaire terminologique - mégadonnées », *Grand dictionnaire terminologique* (2020), en ligne : <https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26507313> (consulté le 9 mars 2022)

SÁNCHEZ SÁNCHEZ, C. R., A. PORTES et S. GALLIN, « La fin des “cookies tiers” ne répond pas au besoin de contrôle des internautes sur leurs données », *La Conversation* (6 avril 2022), en ligne : <https://theconversation.com/la-fin-des-cookies-tiers-ne-repond-pas-au-besoin-de-controle-des-internautes-sur-leurs-donnees-180612> (consulté le 9 avril 2022)

SCHWAB, K., « The Fourth Industrial Revolution: what it means and how to respond », *World Economic Forum* (14 janvier 2016), en ligne : <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> (consulté le 9 mars 2022)

SECRÉTARIAT À LA RÉFORME DES INSTITUTIONS DÉMOCRATIQUES, À L'ACCÈS À L'INFORMATION ET À LA LAÏCITÉ, « Identification, localisation et profilage », *Québec.ca* (25 janvier 2022), en ligne : <https://www.quebec.ca/gouvernement/travailler-gouvernement/services-employes-etat/conformite/protection-des-renseignements-personnels/technologie-et-droit-a-la-protection-des-renseignements-personnels/identification-localisation-profilage> (consulté le 6 avril 2022)

———, « Protection par défaut », *Québec.ca* (8 avril 2022), en ligne : <https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/technologie-et-droit-a-la-protection-des-renseignements-personnels/protection-defaut> (consulté le 5 mai 2022)

STEEVES, V. et J. BAILEY, « Our project », *eQuality Project*, en ligne : <https://www.equalityproject.ca/our-project/> (consulté le 17 mars 2022)

THOMPSON, K., « Canada's new federal privacy Bill C-27 – Summary of significant impacts and new proposals », *Dentons* (20 juin 2022), en ligne : <https://www.dentons.com/en/insights/articles/2022/june/20/canadas-new-federal-privacy-bill-c27-summary-of-significant-impacts-and-new-proposals> (consulté le 23 juin 2022)

WIEWIÓROWSKI, W., « It is time to target online advertising », *European Data Protection Supervisor* (14 mars 2022), en ligne : <https://edps.europa.eu/press-publications/press-news/blog/it-time-target-online-advertising_en> (consulté le 16 mars 2022)

« Les renseignements personnels des enfants et Internet », *Commission d'accès à l'information* (17 septembre 2015), en ligne : <https://www.cai.gouv.qc.ca/les-renseignements-personnels-des-enfants-et-internet/> (consulté le 26 janvier 2022)

« Vous recueillez des renseignements auprès des enfants? Voici dix conseils sur les services destinés aux enfants et aux jeunes », *Commissariat à la protection de la vie privée du Canada* (14 décembre 2015), en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/bus_kids/02_05_d_62_tips/> (consulté le 17 janvier 2022)

« Children Online: Research and Evidence - A knowledge base on children and youth in the digital world », *CORDIS (Commission européenne)* (2020), en ligne : <https://cordis.europa.eu/project/id/871018/fr> (consulté le 29 mars 2022)

« Procédure 2020/0361/COD », *EUR-Lex* (2020), en ligne : <https://eur-lex.europa.eu/legal-content/fr/HIS/?uri=COM:2020:825:FIN#> (consulté le 5 juillet 2022)

« euConsent: Electronic Identification and Trust Services for Children in Europe », *euConsent* (2021), en ligne : <https://euconsent.eu/> (consulté le 29 avril 2022)

« Démographie : la population du Québec et les familles », *Ministère de la Famille du Québec* (12 février 2021), en ligne : <https://www.mfa.gouv.qc.ca/fr/Famille/chiffres-famille-quebec/chiffres-famille/Pages/demographie-population-familles.aspx> (consulté le 17 mars 2022)

« Étude détaillée du projet de loi nº 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels », *Journal des débats de la Commission des institutions de l'Assemblée nationale du Québec* (12 mai 2021), en ligne : <http://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/ci-42-1/journal-debats/CI-210512.html#16h30> (consulté le 4 avril 2022)

« La CNIL publie 8 recommandations pour renforcer la protection des mineurs en ligne », *CNIL* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne> (consulté le 6 décembre 2021)

« Les droits numériques des mineurs », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/les-droits-numeriques-des-mineurs> (consulté le 6 décembre 2021)

« Recommandation 1 : encadrer la capacité d'agir des mineurs en ligne », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-1-encadrer-la-capacite-dagir-des-mineurs-en-ligne> (consulté le 6 décembre 2021)

« Recommandation 2 : encourager les mineurs à exercer leurs droits », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-2-encourager-les-mineurs-exercer-leurs-droits> (consulté le 6 décembre 2021)

« Recommandation 3 : accompagner les parents dans l'éducation au numérique », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-3-accompagner-les-parents-dans-leducation-au-numerique> (consulté le 6 décembre 2021)

« Recommandation 4 : rechercher le consentement d'un parent pour les mineurs de moins de 15 ans », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-4-rechercher-le-consentement-dun-parent-pour-les-mineurs-de-moins-de-15-ans> (consulté le 6 décembre 2021)

« Recommandation 5 : promouvoir des outils de contrôle parental respectueux de la vie privée et de l'intérêt de l'enfant », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-5-promouvoir-des-outils-de-controle-parental-respectueux-de-la-vie-privee-et-de> (consulté le 6 décembre 2021)

« Recommandation 6 : renforcer l'information et les droits des mineurs par le design », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-6-renforcer-linformation-et-les-droits-des-mineurs-par-le-design> (consulté le 6 décembre 2021)

« Recommandation 7 : vérifier l'âge de l'enfant et l'accord des parents dans le respect de sa vie privée », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-7-verifier-lage-de-lenfant-et-laccord-des-parents-dans-le-respect-de-sa-vie-privee> (consulté le 6 décembre 2021)

« Recommandation 8 : prévoir des garanties spécifiques pour protéger l'intérêt de l'enfant », *Commission nationale de l'informatique et des libertés* (9 juin 2021), en ligne : <https://www.cnil.fr/fr/recommandation-8-prevoir-des-garanties-specifiques-pour-proteger-linteret-de-lenfant> (consulté le 6 décembre 2021)

« Position de principe sur la publicité comportementale en ligne », *Commissariat à la protection de la vie privée du Canada* (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 31 janvier 2022)

« DPC publishes final version of Children's "Fundamentals" », *Data Protection Commission* (17 décembre 2021), en ligne : <https://www.dataprotection.ie/index.php/en/news-media/latest-news/dpc-publishes-final-version-childrens-fundamentals> (consulté le 3 mai 2022)

« Friends Suggestions », *Risky-By-Design* (2022), en ligne : <https://www.riskyby.design/friend-suggestions> (consulté le 31 mars 2022)

« Recommendation Systems », *Risky-By-Design* (février 2022), en ligne : <https://www.riskyby.design/recommendation-systems> (consulté le 31 mars 2022)

« L'entreprise de 2025 pilotée par les données », *Ministère de l'Économie et de l'Innovation* (23 mars 2022), en ligne : <https://www.economie.gouv.qc.ca/objectifs/informer/vecteurs/entreprise-entrepreneuriat-et-croissance-des-pme-html/lentreprise-de-2025-pilotee-par-les-donnees/> (consulté le 25 mars 2022)

« What does highly offensive mean? », *New Zealand Privacy Commissioner* (23 mars 2022), en ligne : <https://www.privacy.org.nz/tools/knowledge-base/view/232> (consulté le 3 mai 2022)

« Législation sur les services numériques: accord provisoire entre le Conseil et le Parlement pour faire de l'internet un espace plus sûr pour les citoyens européens », *Conseil de l'Union européenne* (23 avril 2022), en ligne : <https://www.consilium.europa.eu/fr/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/> (consulté le 29 avril 2022)

« Age Appropriate Design Code, Data Protection Bill », *5Rights Foundation* (s.d.), en ligne : <https://5rightsfoundation.com/in-action/blog-age-appropriate-design-code-data-protection-bill.html> (consulté le 29 avril 2022)

« Children and young people », *Office of the Australian Information Commissioner*, en ligne : <https://www.oaic.gov.au/privacy/your-privacy-rights/children-and-young-people> (consulté le 28 avril 2022)

« Convention relative aux droits de l'enfant », *Commission des droits de la personne et des droits de la jeunesse*, en ligne : <https://www.cdpdj.qc.ca/fr/vos-droits/lois-qui-protegent-vos-droits/convention-relative-aux-droits-de-lenfant> (consulté le 4 mars 2022)

« Cookie – Définition », *Commission nationale de l'informatique et des libertés*, en ligne : <https://www.cnil.fr/fr/definition/cookie> (consulté le 3 juin 2022)

« Does the "right to be forgotten" under the California Consumer Privacy Act require that companies delete the same type of information as the "right to be forgotten" under the GDPR? », *Bryan, Cave, Leighton, Paisner*, en ligne : <https://ccpa-info.com/does-the-right-to-be-forgotten-under-the-california-consumer-privacy-act-require-that-companies-delete-the-same-type-of-information-as-the-right-to-be-forgotten-und/> (consulté le 2 mai 2022)

« Données & Design - Études de cas », *Commission nationale de l'informatique et des libertés*, en ligne : <https://design.cnil.fr/etudes-de-cas/> (consulté le 4 mai 2022)

« Espace jeunesse », *Commission d'accès à l'information*, en ligne : <https://www.cai.gouv.qc.ca/jeunes/> (consulté le 6 avril 2022)

« How does the Privacy Act deal with children and teenagers? », *New Zealand Privacy Commissioner*, en ligne : <https://privacy.org.nz/tools/knowledge-base/view/2> (consulté le 28 avril 2022)

« Index du Journal des débats - 29e législature, 1re session (9 juin 1970 - 19 décembre 1970) – 45 - Loi de la protection du consommateur (le ministre de la Justice) », *Assemblée nationale du Québec*, en ligne : <http://www.assnat.qc.ca/fr/travaux-parlementaires/journaux-debats/index-jd/recherche.html?cat=sv&Session=jd29l1se&Section=projlois&Requete=45+-+Loi+de+la+protection+du+consommateur+(le+ministre+de+la+Justice)> (consulté le 27 janvier 2022)

« Index du Journal des débats - 30e législature, 4e session (16 mars 1976 - 18 octobre 1976) – 7 - Loi sur la protection du consommateur (le ministre des Consommateurs, des Coopératives et des Institutions financières) », *Assemblée nationale du Québec*, en ligne : <http://www.assnat.qc.ca/fr/travaux-parlementaires/journaux-debats/index-jd/recherche.html?cat=sv&Session=jd30l4se&Section=projlois&Requete=7+-+Loi+sur+la+protection+du+consommateur+(le+ministre+des+Consommateurs%2c+des+Coop%c3%a9ratives+et+des+Institutions+financi%c3%a8res)> (consulté le 27 janvier 2022)

« Index du Journal des débats - 31e législature, 3e session (21 février 1978 - 20 février 1979) – 72 - Loi sur la protection du consommateur (le ministre des Consommateurs, des Coopératives et des Institutions financières) », *Assemblée nationale du Québec*, en ligne : <http://www.assnat.qc.ca/fr/travaux-parlementaires/journaux-debats/index-jd/recherche.html?cat=sv&Session=jd31l3se&Section=projlois&Requete=72+-+Loi+sur+la+protection+du+consommateur+(le+ministre+des+Consommateurs%2c+des+Coop%c3%a9ratives+et+des+Institutions+financi%c3%a8res)> (consulté le 27 janvier 2022)

« Principle 4 - Manner of collection », *New Zealand Privacy Commissioner*, en ligne : <https://www.privacy.org.nz/privacy-act-2020/privacy-principles/4/> (consulté le 28 avril 2022)

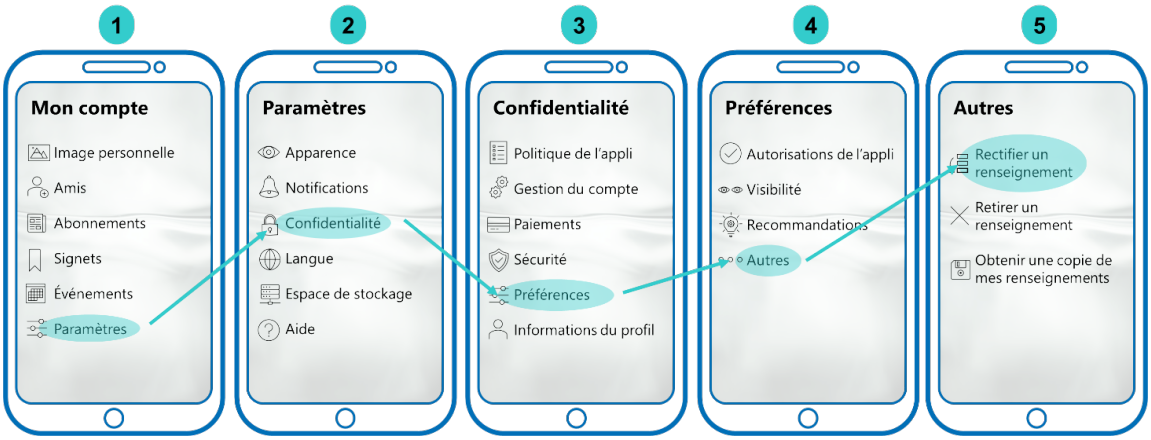
« Vivre dans l'Union européenne: faits et chiffres », *Site de l'Union européenne*, en ligne : <https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/life-eu_fr> (consulté le 28 avril 2022)

ANNEXE 1 – EXEMPLES D'INTERFACES TRUQUÉES

Les exemples fictifs suivants illustrent quelques-unes des interfaces truquées déployées par les fournisseurs de services en ligne pour orienter les choix ou les comportements des utilisateurs (y compris mineurs) en matière de renseignements personnels. Ils sont inspirés ou adaptés des travaux de la 5Rights Foundation[637], du ICO[638], de la CNIL[639], du CEPD[640] et de la professeure Jennifer King[641], et classés suivant la typologie du CEPD. Leur inclusion n'implique pas que la Commission se prononce quant à leur conformité ou non-conformité à l'égard de la législation québécoise actuelle sur la protection des renseignements personnels ou d'autres lois québécoises.

Surcharge : labyrinthe de vie privée

Dans cet exemple, le mineur doit naviguer dans plusieurs menus dont le vocabulaire est quelque peu confus pour parvenir enfin à l'option qu'il recherche, celle de rectifier un renseignement.



637 5RIGHTS FOUNDATION, précité, note 201.

638 *Children's code*, précité, note 325.

639 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, précité, note 526.

640 COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, précité, note 301.

641 J. KING, précité, note 565; Arvind NARAYANAN, Arunesh MATHUR, Marshini CHETTY et Mihir KSHIRSAGAR, « Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces », (2020) 18-2 *Queue* Pages 10:67-Pages 10:92, DOI : 10.1145/3400899.3400901; Ari Ezra WALDMAN, « Cognitive biases, dark patterns, and the 'privacy paradox' », (2020) 31 *Current Opinion in Psychology* 105-109, DOI : 10.1016/j.copsyc.2019.08.025; Paul GRAßL, Hanna SCHRAFFENBERGER, Frederik Zuiderveen BORGESIUS et Moniek BUIJZEN, « Dark and Bright Patterns in Cookie Consent Requests », (2021) 3-1 *Journal of Digital Social Research* 1-38, DOI : 10.33621/jdsr.v3i1.54.

Orientation : orientation visuelle

Dans cet exemple (à gauche), l'application sollicite le consentement du mineur à la collecte de données de géolocalisation. Elle oriente son choix en mettant le bouton « OK » en évidence, au centre et coloré. Le bouton « Non » est grisé et placé en retrait.

Orientation : orientation émotive

Dans cet exemple (à droite), le mineur tente de supprimer son compte. Au moment de lui demander de confirmer son action, ce qui est normal, l'application de jeu fait appel à ses émotions pour l'inciter à ne pas compléter le processus. Une icône de personnage triste est même ajoutée de façon à jouer sur la culpabilité du mineur. Par ailleurs, une orientation visuelle apparaît ici encore (le bouton « Non » est plus en évidence).

Entrave : processus plus long que nécessaire

Dans cet exemple (à gauche), le mineur qui souhaite obtenir une copie de ses renseignements est bloqué par un mécanisme qui le ralentit. Le service le force à confirmer son intention en clavardant avec un agent, et propose un temps d'attente déraisonnable pour faire la demande d'exercice du droit. Ces éléments découragent le mineur de poursuivre.

Surcharge : demandes persistantes

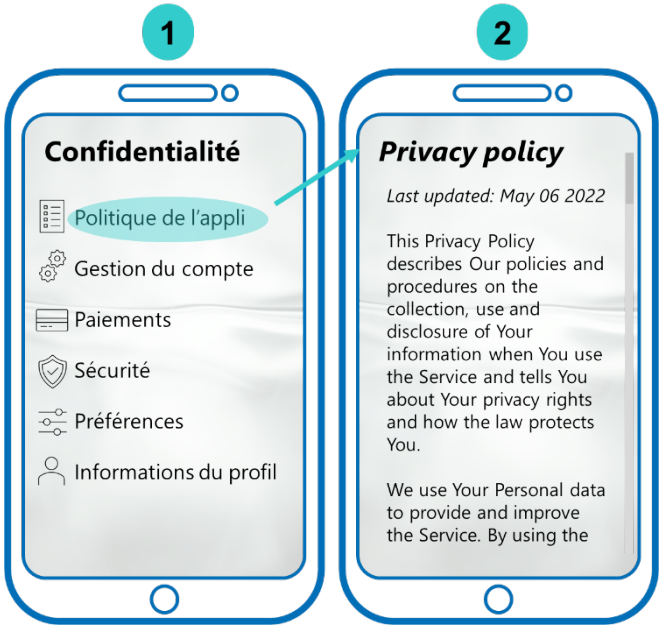
Dans cet exemple (à droite), le service d'écoute de musique en continu propose au mineur d'obtenir des recommandations personnalisées via un profilage. Il lui est impossible de refuser ce paramètre (mécanisme de type entrave : cul-de-sac), puisqu'il ne peut cliquer que sur « Plus tard » pour refuser. Ce faisant, une nouvelle alerte se déclenche quelques heures plus tard, le forçant à choisir de nouveau dans l'objectif qu'il cède.

Entrave : information trompeuse

Dans cet exemple (à gauche), le mineur souhaitant paramétrer la personnalisation de ses vidéos reçoit des explications biaisées par rapport à l'effet du paramètre. Le texte oriente clairement son choix vers l'activation des recommandations.

Obscurité : discontinuité linguistique

Dans cet exemple (à droite), le mineur qui souhaite prendre connaissance de la politique de confidentialité de l'application, offerte en français, ne peut la consulter que dans une autre langue. Cela l'empêche d'obtenir les informations recherchées.



ANNEXE 2 – PRINCIPES ET CATÉGORIES D'ÂGE DU *CHILDREN'S CODE*

Le *Children's Code* du ICO contient 15 principes qui sont reproduits ci-après (notre traduction).

1. **Intérêt supérieur de l'enfant.** L'intérêt supérieur de l'enfant devrait être une considération primordiale lorsque les entreprises conçoivent et développent des services en ligne auxquels les mineurs sont susceptibles d'accéder.

2. **Analyses d'impact sur la protection des données.** Les entreprises doivent mener une analyse d'impact sur la protection des données pour évaluer et atténuer les risques pour les droits et libertés des mineurs susceptibles d'accéder à leurs services qui émergent du traitement de données. Elles doivent tenir compte des différences d'âge, de capacités et de besoins développementaux et s'assurer que leur analyse inclut toutes les mesures pertinentes pour se conformer au *Children's Code*.

3. **Application appropriée à l'âge.** Les entreprises doivent adopter une approche fondée sur le risque pour évaluer l'âge des utilisateurs individuels et s'assurer d'appliquer efficacement les principes du *Children's Code* aux utilisateurs mineurs. Elles doivent soit établir l'âge avec un degré de certitude approprié aux risques pour les droits et libertés des mineurs qui émergent de leur traitement de données ou appliquer l'ensemble des principes du *Children's Code* à tous leurs utilisateurs.

4. **Transparence**. L'information sur la protection des renseignements personnels que les entreprises fournissent aux utilisateurs, tout comme leurs conditions d'utilisation, leurs politiques et leurs normes de communauté, doit être concise, mise en évidence et rédigée en langage clair, adapté à l'âge de l'enfant. De courtes explications supplémentaires spécifiques concernant la façon d'utiliser les renseignements personnels doivent être données au moment où une fonctionnalité précise est activée.

5. **Utilisations nuisibles des données.** Les entreprises ne doivent pas utiliser les données de façons dont on sait qu'elles nuisent au bien-être des mineurs ou qui contreviennent aux codes de pratiques de l'industrie, à d'autres règlements ou à des avis gouvernementaux.

6. **Politiques et normes de communauté.** Les entreprises doivent respecter leurs propres conditions d'utilisation, politiques et normes de communauté, notamment mais non limitativement leurs politiques de confidentialité, leurs restrictions liées à l'âge, leurs règles de comportement et leurs politiques sur le contenu.

7. **Paramètres par défaut.** Par défaut, les paramètres doivent prévoir une « haute confidentialité », sauf si les entreprises peuvent démontrer une raison impérieuse de faire autrement, en tenant compte de l'intérêt supérieur de l'enfant.

8. **Minimisation des données.** Les entreprises doivent recueillir et conserver uniquement le minimum de renseignements personnels qui leur sont nécessaires pour fournir les fonctionnalités de leur service avec lesquelles le mineur est consciemment et activement en interaction. Elles doivent donner aux mineurs des choix distincts par rapport aux fonctionnalités qu'ils souhaitent activer.

9. **Communication des données.** Les entreprises ne doivent pas communiquer les renseignements personnels des mineurs, à moins de pouvoir démontrer une raison impérieuse de le faire, en tenant compte de l'intérêt supérieur de l'enfant.

10. **Géolocalisation**. Les entreprises doivent désactiver par défaut les options de géolocalisation (à moins de pouvoir démontrer une raison impérieuse de ne pas le faire, en tenant compte de l'intérêt supérieur de l'enfant) et aviser les mineurs de manière évidente lorsque le suivi de leur localisation est activité. Les options permettant d'afficher la géolocalisation du mineur à d'autres personnes devraient être automatiquement désactivées à la fin de chaque session d'utilisation.

11. **Outils de contrôle parental.** Si les entreprises proposent des outils de contrôle parental, elles doivent informer le mineur à ce sujet d'une façon qui est adaptée à son âge. Si leur service en ligne permet à un parent ou à un adulte responsable de suivre l'activité en ligne d'un enfant ou sa géolocalisation, les entreprises doivent aviser les mineurs de manière évidente lorsqu'ils sont surveillés.

12. **Profilage.** Les entreprises doivent désactiver par défaut les options reposant sur le profilage (à moins de pouvoir démontrer une raison impérieuse de ne pas le faire, en tenant compte de l'intérêt supérieur de l'enfant). Elles ne devraient effectuer de profilage que lorsque des mesures appropriées sont en place pour protéger le mineur de tout effet nuisible (en particulier, le fait d'être exposé à du contenu nuisible à leur santé ou à leur bien-être).

13. **Techniques trompeuses.** Les entreprises ne doivent pas utiliser de techniques trompeuses pour mener ou encourager le mineur à fournir des renseignements personnels non nécessaires ou à désactiver des paramètres de protection de la vie privée.

14. **Jouets et objets connectés.** Les entreprises qui fournissent des jouets ou des objets connectés doivent s'assurer d'y implanter des outils efficaces pour assurer la conformité à tous les autres principes du code.

15. **Outils en ligne.** Les entreprises doivent fournir des outils accessibles, mis en évidence, afin d'aider les mineurs à exercer leurs droits liés aux renseignements personnels et à signaler leurs préoccupations.

Le code énonce aussi des recommandations particulières pour les mineurs en fonction de cinq catégories d'âge :

Âge	Description
0-5 ans	Phase de pré-alphabétisation et d'alphabétisation précoce
6-9	Années fondamentales d'enseignement primaire
10-12	Années de transition
13-15	Jeune adolescence
16-17	Approche de l'âge adulte

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