Université de Montréal

VIE PRIVÉE DES MINEURS EN LIGNE : PROTECTION DES DONNÉES PERSONNELLES

Étude comparée entre le droit canadien, américain et celui de l'Union européenne

Par

DIANA PAOLA ALVAREZ BAUTISTA

Faculté de Droit

Mémoire présenté en vue de l'obtention du grade de maître (LLM) en droit des technologies de l'information

Juin 2021

Université de Montréal

Unité académique : département des Études Supérieurs, Faculté de droit

---

Ce mémoire intitulé

VIE PRIVÉE DES MINEURS EN LIGNE : PROTECTION DES DONNÉES PERSONNELLES

Étude comparée entre le droit canadien, américain et celui de l´Union européenne

Présenté par

Diana Paola Alvarez Bautista

A été évaluée par un jury composé des personnes suivantes :

Nicolas Vermeys
Président

Vincent Gautrais
Directeur de recherche

Pierre Trudel
Membre du jury

qui lui a décerné la mention « très bon »

Résumé

Cette recherche s'intéresse à un sujet d'actualité portant sur la vie privée des mineurs en ligne, plus particulièrement sur la protection des données personnelles. Depuis l'avènement des nouvelles technologies de l'information et des communications (NTIC) et la venue du web 2.0, la protection des données personnelles demeure question d'actualité en plus d'être fort complexe.

Cette question demeure encore plus criante lorsqu'il s'agit de mineurs. La présente recherche s'intéresse d'abord à l'utilisation d'Internet par les mineurs, à la notion de vulnérabilité du mineur et de l'insuffisance des règles actuelles. Elle s'intéresse également à la distinction conceptuelle entre « mineur » et « enfant » avant de s'arrêter plus longuement aux principales formes d'infractions qui portent atteinte à la vie privée et à l'intégrité des mineurs.

Plus loin dans ce mémoire, on s'intéresse aux dispositions législatives et réglementaires au Canada, aux États-Unis et au sein de l'Union européenne. Dans la dernière partie on montre les différences significatives entre le Canada, les États-Unis et l'Union européenne. Dans la conclusion de ce mémoire, nous revenons sur les faits saillants de cette recherche comparative en insistant sur le fait qu'il est complexe de protéger les données personnelles des mineurs et qu'il existe des différences importantes dans les législations et les règlements en vigueur sur le plan national et international.

Mots-clés : mineurs, enfants, protection des données personnelles, consentement du mineur, consentement parental, cyberintimidation, leurre par Internet, sextage.

Abstract

This research study addresses a current concern regarding the privacy of minors online, more specifically the protection of personal data. Since the emergence of new information and communication technologies (NICT) and the introduction of Web 2.0, the protection of personal data remains a relevant and very complex issue.

This issue is even more critical when it comes to minors. This research study first looks at Internet use by minors, the notion of a minor person's vulnerability and the limitations of the current rules. It also examines the conceptual distinction between "minor" and "child" before focusing on the main aspect of violation of a minor's privacy and integrity.

Later in this master's thesis, the legislative and regulatory provisions in Canada, the United States and the European Union are examined. The final section highlights the significant differences between Canada, the United States and the European Union. In the conclusion for this dissertation, we will look back at the highlights of this comparative study, emphasizing that the task of protecting the personal data of minors is complex and that there are significant disparities in the laws and regulations in force at the national and international levels.

Keywords: minors, children, personal data protection, minor's consent, parental consent, cyberbullying, Internet luring, sexting.

Table des matières

Liste des sigles

ACM	Association canadienne du marketing
AEPD	Agencia española de protección de datos
ARCO	Droits d'accès, de rectification, de cession et d'obtention des données
CCPE	Centre canadien de protection de l'enfance
CCQ	Code civil du Québec
CDE	Comité des droits de l'enfant
CEPD	Comité européen de la protection des données
CIDE	La Convention relative aux droits de l'enfant (1989)
CJUE	Cour de justice de l'Union européenne
COPPA	Children's Online Privacy Protection Act
CPVP	Commissariat à la protection de la vie privée du Canada
DDE	Déclaration des droits de l'enfant (1959)
FTC	Federal Trade Commission
ICO UK	Information Commissioner's Office del Reino Unido
INTECO	Instituto Nacional de tecnologías de la comunicación
LADOPPRP	Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels
L´OPC	L'Office de la protection du consommateur
LPCQ	Loi sur la protection du consommateur
LPRPDE	Loi fédérale canadienne sur la protection des renseignements personnels et les documents électroniques
LPRPSP	Loi sur la protection des renseignements personnels dans le secteur privé
MSP	Ministère de la Sécurité publique du Québec
OC	Option consommateurs
OCDE	Organisation de coopération et de développement économiques
OIT	Organisation internationale du Travail
ONU	Organisation des Nations unies
PL64	Projet de loi 64 du Québec

RGPD	Règlement (UE) 2016/679 relatif à la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel et la libre circulation.
RIPD	Red Iberoamericana de protección de datos
R.J.Q	Recueil de jurisprudence du Québec
SPC	Sécurité publique Canada
SQ	Sûreté du Québec
SSI	Service de la société de l'information
TIC	Technologies de l'information et de la communication
UE	Union européenne
UIT	Union internationale des télécommunications
UNICEF	Fonds des Nations Unies pour l'enfance
UNESCO	Organisation des Nations Unies pour l'éducation, la science et la culture

À mes filles Camila et Paula

Remerciements

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui je voudrais témoigner toute ma gratitude.

Je voudrais tout d'abord adresser toute ma gratitude à mon directeur de mémoire, M. Vincent Gautrais, pour avoir accepté d'encadrer cette recherche. Je le remercie bien sincèrement pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à alimenter ma réflexion.

Je tiens à témoigner aussi toute ma reconnaissance à l'équipe pédagogique en droit des technologies de l'information de l'Université de Montréal pour avoir assuré un enseignement de qualité. Je remercie le personnel administratif des études supérieures, en particulier Ingrid Rodriguez, pour ses services de qualité et son soutien constant.

Un grand merci à mon mari German Marino qui a toujours été là pour moi; sans lui tout cela n'aurait pas été possible. Je remercie mes filles Camila et Paula, mes très chers parents, Rosaura et Segrid ainsi que mes sœurs Johanna et Silvana pour leurs encouragements, confiance et soutien indéfectible.

Enfin, je voudrais exprimer ma reconnaissance envers les amis et collègues qui m'ont apporté leur soutien moral et intellectuel tout au long de ma démarche. En particulier, mes amis Keren Alvarado, Caroline Parente, Maria Godoy et Clémence Frances qui ont toujours été là pour moi. Leur soutien inconditionnel et leurs encouragements ont été d'une grande aide.

À tous ces intervenants, je présente mes remerciements, mon respect et ma gratitude.

Introduction

Les nouvelles technologies de l'information et de la communication (ci-après « TIC »)[1] de même que l'Internet et les réseaux sociaux se sont considérablement développés depuis le début du XXIe siècle. Cette évolution a entraîné des changements majeurs dans la façon dont les gens interagissent, communiquent et s'expriment entre eux[2]. Il est donc nécessaire d'élargir la portée des droits des personnes en reconnaissant l'existence de droits liés au cyberespace.

Il est indéniable également que les progrès technologiques ont permis aux mineurs (terme à définir ultérieurement) d'avoir accès dès leur plus jeune âge à des appareils électroniques, comme les ordinateurs, les *smartphones* ou encore les tablettes, lesquels leur permettent de naviguer sur Internet et d'interagir grâce à ces nouvelles technologies, à travers différents réseaux sociaux (mise en relation directe entre utilisateurs) et médias sociaux dont le but est de publier des contenus.

Certes, les mineurs partagent leur vie privée afin d'obtenir une reconnaissance sociale. Ils transmettent jour après jour sur le web une grande quantité de données contenant des informations personnelles propres ou concernant des tiers : vidéos et photos révélant leur identité, textes et audio décrivant leur personnalité et leurs habitudes ainsi que des coordonnées GPS précisant leur emplacement. Cependant, la plupart d'entre eux n'ont pas conscience que toutes les données personnelles qu'ils fournissent volontairement ou involontairement, aussi insignifiantes soient-elles, laissent des traces qui en font des sujets facilement identifiables, et ce, en permettant de créer leur profil virtuel[3] et de reconstruire à la fois leur identité numérique et celle en dehors du réseau.

---

[1] Office québécois de la langue française (OQLF), *Le Grand dictionnaire terminologique (GDT)*, Québec, 2008 *sub verbo* « Technologies de l'information et de la communication ». *:* Les technologies de l'information et de la communication sont définies comme « l'ensemble des technologies issues de la convergence de l'informatique et des techniques évoluées du multimédia et des télécommunications, qui ont permis l'émergence de moyens de communication plus efficaces, en améliorant le traitement, la mise en mémoire, la diffusion et l'échange de l'information ». En ligne seulement : Office québécois de la langue française <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8349341>.

[2] Dido Harding, « Staying Safe Online » dans Jon Brown, dir, *Online Risk Child Impact Prot Prev*, 1e éd, John Wiley & Sons, Ltd, 2017 177 à la p 177.

[3] Voir Ana María Gil Antón, *¿Privacidad del menor en internet?: « me gusta », !!!todas las imágenes de mis amigos a mi alcance con un simple click!!!.*, 1e éd, Monografía - Revista Nuevas Tecnologías 13, Cizur Menor (Navarra), España, Aranzadi Thomson Reuters, 2015.

En d'autres termes, bien que les TIC offrent un ensemble de possibilités pour le développement des mineurs et permettent l'exercice de multiples droits, comme la liberté d'expression[4] et l'éducation; les risques auxquels les mineurs sont exposés l'emportent bien souvent sur les opportunités.

En effet, les mineurs sont constamment surveillés par les grandes entreprises qui stockent leurs données dans le *Big Data*, notamment par le biais de jouets intelligents (par exemple, poupées et peluches interactives, des consoles de jeux, petits robots, des tablettes ou des drones)[5], des géo-localisateurs, des réseaux sociaux ou encore des études de marché. De cette façon, les entreprises créent des profils de mineurs pour les exposer au marketing ciblé ou à la publicité personnalisée.

Parmi les autres comportements qui portent atteinte aux droits des mineurs en traitant leurs données, on peut citer la cyberintimidation (cyberbullying)[6], le leurre par Internet (grooming)[7] et les textos ayant une portée sexuelle (sextage ou sexting en anglais)[8]. De telles pratiques mettent en péril la vie privée[9], l'honneur, l'intégrité[10], l'intimité et la réputation[11] des mineurs.

---

[4] *Convention internationale relative aux droits de l'enfant*, Rés AG 44/25, 20 novembre 1989, R.T. Can. 1992, n° 3 Annexe, (entré en vigueur le 2 septembre 1990, accession par le Canada le 12 janvier 1992) , art 13.

[5] Voir notamment Option consommateurs, *Enfants sous écoute : la protection de la vie privée dans l'environnement des jouets intelligents*, Montréal, Québec, Commissariat à la protection de la vie privée du Canada, 2018 à la p 9, en ligne : <https://option-consommateurs.org/wp-content/uploads/2018/11/oc-jouets-i-rapport-final.pdf> (consulté le 2 décembre 2019)

[6] Voir en particulier Centre canadien de protection de l'enfance [CCPE], *Fiche de prévention sur la cyberintimidation* , Centre canadien de protection de l'enfance inc, 2017. Le CCPE définit la cyberintimidation comme « étant une forme d'intimidation extrême entre jeunes dans l'espace numérique. Il s'agit d'un comportement abusif, ciblé, délibéré et répétitif destiné à causer du tort à une autre jeune personne ». En ligne : <https://www.cyberaide.ca/pdfs/C3P_SafetySheet_Cyberbullying_fr.pdf>. Voir aussi « Cyberaide.ca », en ligne: Cyberaide.ca <https://cyberaide.ca/app/fr/>.

[7] Voir généralement Centrale canadienne de signalement des cas d'exploitation sexuelle d'enfants sur Internet (Cyberaide), « Le conditionnement », en ligne: *Cyberaide.ca* <https://cyberaide.ca/app/fr/child_sexual_abuse-grooming>. La CCPE indique que « Le conditionnement est une tactique utilisée par un abuseur pour gagner la confiance d'un enfant et des adultes de son entourage dans le but d'entrer en relation avec l'enfant et d'exercer une emprise sur lui».

[8] Voir Groupe de travail interinstitutionnel sur l'exploitation sexuelle des enfants 2016, « Sexting » dans *Guide Terminol Pour Prot Enfants Contre L'exploitation L'abus Sex*, Luxembourg, ECPAT International et ECPAT Luxembourg, 2017 122 à la p 48. Le *«Sexting» ou «sexto»* sont des termes pour désigner l'envoi de messages sexuellement explicites et autoproduits via téléphone portable ou messagerie instantanée.

[9] *CIDE*, *supra* note 4, art 16. : « Nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance [...] ».

[10] *Ibid*. « Nul enfant ne fera l'objet [...] d'atteintes illégales à son honneur et à sa réputation ».

[11] *La situation des enfants dans le monde 2017 : Les enfants dans un monde numérique*, Fonds des Nations Unies pour l'enfance (UNICEF France), 2017 à la p 128.

Par conséquent, étant donné que les mineurs n'ont ni la capacité ni la maturité pour décider de manière consciente des risques qui peuvent se présenter tant dans le présent que dans leur vie future, la transmission intentionnelle ou non de données à caractère personnel, les place en fait dans un groupe vulnérable qui exige une protection spéciale de la part des gouvernements par la mise en œuvre de normes efficaces. Il faut donc adopter différents types de mesures pour protéger les droits et les intérêts des mineurs.

À la lumière de ce qui précède, nous orientons notre réflexion vers la vie privée des mineurs en ligne par rapport à la protection de leurs données personnelles. À ce sujet, nous proposons de réaliser une étude comparée entre le droit canadien, américain et celui de l'Union européenne, en présentant l'état de lieux concernant la protection des données personnelles des mineurs (Partie I) et l'approche des modèles réglementaires et des normes de traitement des données à caractère personnel dans les législations à l'étude (Partie II).

Pour ce faire, dans la Partie I de notre étude, nous commencerons par une approche factuelle de la problématique autour de la protection des données des mineurs (Titre 1, chapitre 1), en analysant l'utilisation d'Internet par eux, la notion de vulnérabilité et les règles particulières insuffisantes. Nous tenterons également de résoudre certains dilemmes conceptuels. Le premier concerne la différence entre le concept de mineur et celui d'enfant. Le second, nous élargirons la notion d'âge de la majorité numérique (Titre 1, chapitre 2).

Ensuite, nous présenterons la classification des risques que les mineurs peuvent rencontrer en ligne, de même quelques facteurs qui augmentent la possibilité pour les mineurs de s'exposer à des comportements portant atteinte à leur vie privée et de devenir des victimes, des auteurs d'abus ou encore de comportements répréhensibles. Notamment, les aspects liés au degré de développement psychologique du mineur, comme la maturité et l'inconscience; la croyance qu'ils sont experts en l'utilisation de ces outils; la configuration inadéquate des paramètres de confidentialité[12]; la croyance que l'anonymat existe[13] et l'impunité dans le cyberespace (Titre 2, chapitre 1). Par la suite, nous mettrons l'accent sur certains risques auxquels les mineurs peuvent

[12] Commission d'accès à l'information du Québec (CAI), Rapport quinquennal 2011 : Technologies et vie privée : à l'heure des choix de société, Québec, CAI, 2011, en ligne : <https://www.cai.gouv.qc.ca/rapport-quinquennal-2011/>.
[13] Ministère de la Sécurité publique du Québec (MSP), « La cyberintimidation et le cyberharcèlement », (décembre 2009), en ligne: <https://www.securitepublique.gouv.qc.ca/police/publications-et-statistiques/statistiques/cyberintimidation/en-ligne.html>.

être exposés par la divulgation exorbitante de données personnelles en ligne et la gestion inadéquate de leur vie privée, en particulier la cyberintimidation, le leurre par Internet et le *sextage* (Titre 2, chapitre 2).

Au Titre II de ce document, nous nous pencherons sur les modèles réglementaires et les normes de traitement des données à caractère personnel propres au droit canadien, américain et à celui de l'Union européenne. En particulier, nous porterons une attention aux enjeux et défis de chaque réglementation face aux risques de la vie privée des enfants sur Internet et la nécessité d'adapter le système juridique pour surmonter la fragmentation technique du droit avec l'environnement numérique.

Parmi les enjeux et les défis communs, nous pouvons citer ceux qui concernent le consentement du mineur; l'absence, la déficience ou l'inexactitude de la portée de la notion de mineur; la carence d'harmonisation par rapport à l'âge de la majorité numérique; et l'absence ou l'insuffisance des mécanismes de vérification tant de l'âge du mineur que de l'identité du représentant légal ainsi que les problèmes de mise en œuvre, le cas échéant.

À cette fin, au chapitre 1 du Titre 1, nous analyserons les sources juridiques au niveau fédéral, notamment la *Loi sur la protection des renseignements personnels et des documents électroniques (LPRPDE)* et le *Code de déontologie et normes de pratique de l'Association canadienne du marketing*. En outre, le chapitre 2 exposera brièvement les développements en matière de protection des données des mineurs que nous livre le législateur québécois, dont la *Loi sur la protection des renseignements personnels dans le secteur privé* (LPRSP) et la *Loi sur la protection du consommateur du Québec*.

Enfin, dans le Titre 2, nous examinerons deux sources de niveau international. D'une part, nous analyserons la *Children's Online Privacy Protection Act* (COPPA) des États-Unis, et certaines dispositions du *Règlement général (UE) 2016/679 sur la protection des données* (RGPD) de l'Union européenne, notamment son article 8.

Partie I – État de lieux concernant la protection des données personnelles des mineurs[14]

Titre 1 – Approche factuelle des données personnelles des mineurs

Chapitre 1 – La problématique autour de la protection des données personnelles des mineurs

1.1. L'utilisation d'Internet par les mineurs

À l'échelle mondiale, les TIC et Internet ont révolutionné la façon de communiquer des gens. De nos jours, les mineurs utilisent Internet avec une certaine facilité puisqu'ils sont nés dans un monde numérique et se sont rapidement adaptés à l'évolution accélérée des nouvelles technologies[15]. Si l'usage de l'Internet renferme certes des avantages, il comporte aussi de nouveaux risques pour les utilisateurs, en particulier les mineurs.

À l'heure actuelle, les études quantitatives et qualitatives portant sur la pénétration et l'utilisation d'Internet et des TIC chez les mineurs sont rares, particulièrement si l'on se réfère à des études ayant pour objet les mineurs de moins de 15 ans[16]. Il arrive que les enquêtes et les entretiens avec les mineurs[17] soient plus coûteux et plus complexes que ceux avec la population adulte, en particulier si l'on tient compte du facteur lié au consentement et/ou à l'autorisation de leur représentant légal.

Cependant, dans un rapport présenté par le *Fonds des Nations Unies pour l'enfance* (ci-après « l´UNICEF ») en 2017, les enfants et les adolescents de moins de 18 ans représentent

[14] Dans l'ensemble de ce mémoire, l'utilisation du genre masculin a été adoptée afin de faciliter sa lecture.
[15] Marc Prensky, « Digital Natives, Digital Immigrants Part 1 » (2001) 9:5 Horiz 1-6.
[16] Tenant compte du fait que les enquêtes sont généralement dirigées vers des personnes de plus de 15 ans. L'UIT propose d'utiliser la classification suivante par tranche d'âge : « moins de 5 ans; 5 à 9 ans; 10 à 14 ans; 15 à 24 ans; 25 à 34 ans; 35 à 44 ans; 45 à 54 ans; 55 à 64 ans; 65 à 74 ans et 75 ans et plus 53 ». Voir notamment Union internationale des télécommunications (UIT), *Manuel pour mesurer l'accès des ménages et des particuliers aux TIC et l'utilisation de ces technologies* , Service de la production des publications (PUBL) de l'UIT, 2020 n 188 et 288. En ligne : <*http://handle.itu.int/11.1002/pub/815edb48-en*>.
[17]Amanda Lenhart, « The challenges of conducting surveys of youth », (21 juin 2013), en ligne: *Pew Res Cent* <https://www.pewresearch.org/fact-tank/2013/06/21/the-challenges-of-conducting-surveys-on-youths/>.

environ un utilisateur d'Internet sur trois dans le monde. De son côté, les données de *l'Union internationale des télécommunications* (ci-après UIT[18]) révèlent que près de 70 % des jeunes dans le monde sont connectés en ligne, ce qui représente un quart du nombre total des personnes utilisant Internet[19]. En conclusion, dans le monde, 71 % des mineurs sont en ligne, contre 48 % de la population totale[20]. En ce qui concerne la pénétration d'Internet par les mineurs Canadiens, la société de statistiques « *Statista* » révèle qu'en 2019, 55,1 % des enfants âgés de 0 à 11 ans utilisent Internet, contre 97,9 % des mineurs âgés de 13 à 17 ans[21]. En outre, *Global Kids On-line Canada*[22] affirme que plus de 90 % des jeunes Canadiens qui utilisent Internet sont âgés entre 14 à 18 ans.

Il ne fait aucun doute que le rapport croissant des enfants au monde numérique, de même que le phénomène de la mondialisation, sont inexorables. Les mineurs représentent déjà un pourcentage significatif de la population mondiale connectée et leur participation ne fera qu'augmenter dans le futur, compte tenu du fait que les pays adoptent de plus en plus des politiques économiques et sociales pour réduire la fracture numérique entre leurs populations[23].

L'Internet est donc devenu un élément essentiel de la vie des enfants et des adolescents. Cependant, des études montrent qu'un pourcentage élevé de mineurs ne connaissent pas leurs droits par rapport aux responsables du traitement de données personnelles, ne comprennent pas les politiques de confidentialité et limitent la terminologie de ces données uniquement au nom, à l'âge, au téléphone, au courriel et au lieu d'études.

Le manque de sensibilisation de l'enfant à la protection des données personnelles diffère de l'état de « *digital natives* » cité en 2001 par Marc Prensky dans son article intitulé « *Digital Natives,*

---

[18] Voir « À propos de l'Union internationale des télécommunications (UIT) », en ligne: *UIT* <https://www.itu.int:443/fr/about/Pages/default.aspx>. L'UIT est l'institution spécialisée des Nations Unies pour les technologies de l'information et de la communication (TIC).

[19] UIT, *Measuring digital development: Facts and figures 2020* , ITU Publications, 2020. En ligne: < https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx>. Voir ausi UIT, « Let's work together to build a safer Internet for children: Doreen Bogdan-Martin », (5 février 2019), en ligne: *ITU News* <https://news.itu.int/lets-work-together-to-build-a-safer-internet-for-children/>.

[20] note 11 à la p 1.

[21] Statista Research Department, « Canada: internet user penetration by age 2019 », (31 août 2015), en ligne: *Statista.com* <https://www.statista.com/statistics/373955/canada-online-penetration-age/>.

[22] Global Kids Online Canada, « The Canadian Kids Online project will investigate young Canadian's experiences in online environments. », en ligne: *Glob Kids Online* <http://globalkidsonline.net/gko-launching-in-canada-with-a-focus-on-privacy/>.

[23] note 11 à la p 7. UNICEF indique que *dans le monde, environ 29 % des jeunes – soit 346 millions de personnes – n'ont pas accès à Internet.*

Digital Immigrants »[24]. Le terme Natif numérique se réfère à la génération née après 1995, et qui a grandi avec Internet. Selon l'expert en éducation et chercheur américain, le natif numérique a une capacité naturelle, qui lui permet d'être plus compétent dans l'environnement numérique, puisque les outils technologiques occupent une place centrale dans sa vie et il dépend d'eux pour toutes sortes de situations quotidiennes, comme étudier, communiquer, acheter, s'informer ou s'amuser.

> « … the first generations to grow up with this new technology. They have spent their entire lives surrounded by and using computers, videogames, digital music players, video cams, cell phones, and all the other toys and tools of the digital age »[25].

Néanmoins, tel que l'ont souligné Ellen Helsper et Rebecca Eynon[26], Danah Boyd[27] et Sonia Livingston[28], s'il est vrai que le terme « natif numérique » suggère que les enfants savent utiliser les nouvelles technologies de façon spontanée, parce qu'ils sont en contact avec eux dès leur naissance, cela ne signifie pas pour autant qu'ils sont compétents pour utiliser correctement ces outils et protéger leurs données de manière adéquate. Il est important de préciser qu'être « natif numérique » ne signifie pas être « compétent numérique » [29].

Fait que Prensky a reconnu des années plus tard dans un article intitulé « *H. Sapiens Digital: From Digital Immigrants and Digital Natives to Digital Wisdom* » (2009)[30], où il a introduit et

---

[24] Voir notamment Prensky, *supra* note 15.

[25] *Ibid*.

[26] Voir Ellen Johanna Helsper & Rebecca Eynon, « Digital natives: where is the evidence? » (2010) 36:3 Br Educ Res J 503-520., en ligne : <https://www.jstor.org/stable/pdf/27823621.pdf?refreqid=excelsior%3Aaa88b13441da85e703f3a4531b8b14ad> (Consulté le 26 november 2019). Hesper et Eynon ont conclu que: « Although young people do use the Internet more, our analysis does not support the view that there are unbridgeable differences between those who can be classified as digital natives or digital immigrants based on when they were born ».

[27] Voir aussi Danah Boyd, *It's Complicated: The Social Lives of Networked Teens*, Yale University Press, 2014 à la p 191. Danah Boyd, a indiqué: « Many of today´s teens are indeed deeply engaged with social media and are active participants in networked publics, but this does not mean that they inherently have the knowledge or skills to make the most of their online experiences. The rhetoric of "digital natives," far from being useful, is often a distraction to understanding the challenges that youth face in a networked world ».

[28] Voir Sonia Livingstone, « Enabling media literancy for "Digital Natives" – A contradiction in terms? » (2009) Digit Nativ Myth (London School of Econo) , en ligne: <http://www2.lse.ac.uk/media@lse/POLIS/home.aspx> à la p 5. Selon Livingstone, « watching children click links quickly or juggle multiple windows does not, necessarily, confirm that they are engaging with online resources wisely or, even, as they themselves may have hoped – we must not be beguiled by their confidence ».

[29] *'Digital Natives': A Myth?*, by Ranjana Das et al, London, UK, London School of Economics and Political Science, 2009 aux pp 8-10 , publisher: POLIS, London School of Economics and Political Science.

[30] Marc Prensky, « H. Sapiens Digital: From Digital Immigrants and Digital Natives to Digital Wisdom » (2009) 5:3 Innov J Online Educ 1-11.

développé le concept de « *Sagesse numérique* » [31], surmontant ainsi le concept de natif numérique. Le terme de sagesse numérique, désigne la personne qui, en plus de savoir comment utiliser les technologies, a également la capacité de les évaluer et de les utiliser de manière juste et appropriée. Prensky mentionne d'ailleurs à ce sujet ce qui suit:

> « Digital wisdom can be, and must be, learned and taught. As we offer more courses in digital literacy, we should also offer students guidance in developing digital wisdom.[32]»

Alors, il est clair que peu de nos mineurs ont la compétence numérique[33] qui leur permettent d'évaluer les risques potentiels et les implications auxquels ils sont exposés lorsqu'ils naviguent sur Internet. Abandonner les mineurs à leur sort dans le cyberespace, c'est les exposer aux risques inhérents à l'utilisation de ces outils, notamment l'usurpation d'identité, la cyberintimidation, le sextage, le grooming, le vol d'images et l'exposition à des pratiques publicitaires agressives.

Internet et les TIC ne constituent pas un risque en soi. Mais, étant donné la nature transfrontalière de Internet et des TIC, le manque de maturité et de conscience des mineurs, la grande quantité de données sensibles qu'ils fournissent sur Internet, le sentiment d'anonymat[34] et la pérennité de l'information[35], il est nécessaire de garantir un environnement électronique plus sûr pour nos enfants. Pourtant, pour que ces risques n'aboutissent pas à un dommage, il est nécessaire aussi de protéger ses données personnelles afin de prévenir toute atteinte à d'autres droits fondamentaux du mineur, dont l'honneur, la liberté, la vie privée, la réputation, la dignité et ce qui porte atteinte à son intégrité[36].

Par conséquent, des mesures efficaces et coordonnées de la part des administrations publiques et privées sont nécessaires, mais surtout l'accompagnement des parents ou leurs représentants, lesquels par l'éducation peuvent faire acquérir aux mineurs des connaissances sur la façon de protéger leurs données personnelles, le fonctionnement des politiques de confidentialité,

---

[31] *Ibid* à la p 6.
[32] *Ibid*.
[33] Alexander J A M van Deursen & Jan A G M van Dijk, *Digital Skills: Unlocking the Information Society*, Digital Education and Learning, New York, Palgrave Macmillan Ltd., 2014 à la p 69.
[34] Ministère de la Sécurité publique du Québec (MSP), *supra* note 13.
[35] *Ibid*.
[36] Nicolás Antúnez González, *Fortalecimiento de herramientas para la protección de datos personales frente al debilitamiento del principio del consentimiento* , Salamanca, España, Ratio Legis, 2016.

afin de parvenir entre autres à une interaction adéquate avec les autres membres du réseau[37]. Compte tenu des considérations exprimées, le système juridique a été amené à renouveler la réglementation en vigueur jusqu'à présent, en tentant de remédier aux diverses situations qui se produisent et qui n'étaient pas reflétées légalement.

En effet, aux États-Unis, la *Children's Online Privacy Protection Act* (ci-après « COPPA »[38]) réglemente le traitement des données personnelles des enfants de moins de 13 ans. L'Union européenne, conformément au *Règlement (UE) 2016/679 relatif à la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel et la libre circulation* (ci-après RGPD[39]) a plutôt établi que le traitement des données personnelles d'un mineur est considéré comme licite lorsqu'il est âgé d'au moins 16 ans. Toutefois, elle confère aux États membres le pouvoir de fixer par voie législative un âge inférieur, qui peut être défini entre 13 et 16 ans[40]. En revanche, la *loi fédérale canadienne sur la protection des renseignements personnels et les documents électroniques* (ci-après LPRPDE[41]) ne précise pas l'âge et ne fait pas de distinction entre les mineurs et les adultes.

1.2. La notion de vulnérabilité du mineur

La notion de vulnérabilité de l'enfant est directement liée au développement psychologique. Outre son propre développement physique, le mineur assimile et apprend de son milieu, ce qui est nécessaire à sa maturation[42]. Pour le meilleur et pour le pire, tout mineur, par le seul fait d'être mineur, est extrêmement perméable aux influences qui se produisent dans son environnement au fil des différentes étapes de son développement.

---

[37] Voir notamment *Developing a framework for researching children's online risks and opportunities in Europe*, by Sonia Livingstone, Giovanna Mascheroni & Elisabeth Staksrud, Zotero, Londres, EU Kids Online, 2015 à la p 3.
[38] *Children's Online Privacy Protection Act*, 15 USC §§ 6501–6506, (1998).
[39] *CE, Règlement (CE) 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)*, 2016 JO L1191.
[40] *Ibid*, art 8.
[41] *Loi sur la protection des renseignements personnels et les documents électroniques,* LC 2000, c 5.
[42] Voir notamment Commissariat à la protection de la vie privée du Canada, *Rapport annuel au Parlement 2016-2017 concernant la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur la protection des renseignements personnels: Des craintes réelles, des solutions pour y remédier : Plan pour rétablir la confiance dans la protection de la vie privée*, Gatineau (Québec), CPVP, 2017.

Dans le cas du traitement des données personnelles chez les mineurs, il convient de tenir compte du fait que les compétences numériques continuent à se développer pendant l'enfance et l'adolescence[43]. En conséquence, les mineurs révèlent facilement leurs données dans l'espace cybernétique en l'absence d'un développement et d'une maturité complets. Les mineurs, lorsqu'ils sont en phase d'apprentissage, ne sont pas pleinement conscients des risques et des conséquences qui peuvent résulter de la transmission de renseignements personnels. Cette condition, l'immaturité ou l'inexpérience, rend le mineur vulnérable aux risques, le plaçant dans un état d'impuissance, ce qui exige une protection spéciale de ses droits, en les transformant en un groupe d'attention prioritaire.

Deux aspects pertinents de la notion de vulnérabilité se dégagent de ce qui précède, soit 1) les risques auxquels le mineur est exposé : le risque d'être exposé à une situation menaçante, le risque de ne pas être en mesure d'y faire face et le risque de subir de graves conséquences; et 2) l'impuissance, c'est-à-dire le manque de structure ou de ressources pour faire face avec succès à la situation de risque. C'est ce dernier aspect, l'impuissance, qui fait que les mineurs sont considérés comme un groupe vulnérable et qu'ils ont besoin d'une protection spéciale.

Cela a suscité au cours des dernières années un vaste débat sur les mesures à adopter pour améliorer la protection des données des mineurs, sur le rôle que doivent jouer les représentants légaux (concernant au consentement ou l'accès aux données, entre autres) et les entités de protection des données aux niveaux national et international.

Des législations telles que celles de l'Union européenne et du Canada ont été inspirées par des instruments internationaux, comme la *Déclaration des droits de l'enfant*, adoptée le 20 novembre 1959 par *l'Assemblée générale de l'Organisation des Nations Unies* (ci-après ONU) et la Convention relative aux droits de l'enfant, afin de promouvoir progressivement la promulgation de normes, concepts, lignes directrices et/ou programmes éducatifs visant à protéger les données des mineurs sur Internet.

Les différentes initiatives sont élaborées sur la base des principes et concepts directeurs de ces instruments. Parmi ces principes et concepts, on trouve la déclaration explicite selon laquelle

[43] Prensky, « H. Sapiens Digital », *supra* note 30.

les mineurs constituent un groupe vulnérable et exigent donc une protection spéciale. Dans ce contexte, la *Déclaration des droits de l'enfant* (1959), renferme le considérant suivant dans son préambule :

> « Considérant que l'enfant, en raison de son manque de maturité physique et intellectuelle, a besoin d'une protection spéciale et de soin particulier, notamment d'une protection juridique appropriée, avant comme après la naissance ».

De même, la *Convention relative aux droits de l'enfant* (ci-après CIDE), adoptée 30 ans plus tard, en 1989, prévoit à l'article 3.2 que :

> « Les États parties s'engagent à assurer à l'enfant la protection et les soins nécessaires à son bien-être, compte tenu des droits et des devoirs de ses parents, de ses tuteurs ou des autres personnes légalement responsables de lui, et ils prennent à cette fin toutes les mesures législatives et administratives appropriées »[44].

De son côté, la *Cour suprême du Canada* a évoqué que « [l]a reconnaissance de la vulnérabilité inhérente des enfants demeure profondément enracinée en droit canadien et elle se manifeste par la protection des droits au respect de la vie privée des jeunes »[45]. Pour sa part, l'Union européenne a, pour la première fois, par le biais du RGPD, élaboré une réglementation spécifique sur le traitement des données à caractère personnel des mineurs en fonction de sa vulnérabilité, tel qu'il est énoncé dans le considérant 38, à savoir :

> « 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… » [46].

En ce sens, un développement optimal du mineur n'est présent que dans des environnements gérés dans la perspective de « *l'intérêt supérieur du mineur*[47] ». La CIDE[48] n'offre

---

[44] La CIDE est l'instrument des droits de l'homme qui a reçu le plus de ratifications dans l'histoire de l'humanité, puisque tous les pays du monde, sauf la Somalie et les États-Unis, (ce dernier, pour ne pas accepter l'interdiction de la peine de mort pour le mineur), l'ont ratifiée.

[45] *AB c Bragg Communications Inc*, [2012] 2 RCS 567.

[46] *RGPD*, *supra* note 39. Considerant 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… ».

[47] *Observation générale no 14 (2013) sur le droit de l'enfant à ce que son intérêt supérieur soit une considération primordiale (art. 3, par. 1)*, Doc off CDE NU, 62e Sess, Doc NU CRC/C/GC/14 (2013). Le Comité des droits de l'enfant [CDE], estime que « le concept d'intérêt supérieur de l'enfant vise à assurer tant la réalisation complète et effective de tous les droits reconnus dans la Convention que le développement global de l'enfant ».

[48] *CIDE*, *supra* note 4.

pas de définition précise de l'intérêt supérieur, mais stipule que dans toutes les mesures qui concernent les enfants, qu'elles soient le fait des institutions publiques ou privées de protection sociale, des tribunaux, des autorités administratives ou des organes législatifs, l'intérêt supérieur de l'enfant doit être une considération primordiale (article 3 (1))[49].

En outre, nous pouvons constater que ce principe a incité les législateurs fédéraux et provinciaux à protéger les droits de l'enfant dans différents domaines. Le *Code civil du Québec*, art. 33[50] et la *Loi sur la protection de la jeunesse*, art. 3[51], prévoient que les décisions concernant l'enfant doivent être prises dans son intérêt et dans le respect de ses droits[52]. De même, aux articles 248[53] et 249[54], la *loi sur la protection du consommateur du Québec*[55], compte tenu du principe de l'intérêt supérieur, interdit la publicité à but commercial destinée aux enfants âgés de moins de 13 ans. Selon un Jugement de la Cour suprême du Canada,

> « … l'objectif de réglementer la publicité commerciale destinée à des enfants est … de protéger un groupe qui est très vulnérable à la manipulation commerciale… Les capacités des enfants ne sont pas aussi développées que celles des adultes pour évaluer la force persuasive de la publicité. » [56]

Cet extrait nous permet de conclure que le mineur a besoin de plus de protection que les adultes, mais aussi qu'il existe certains facteurs qui augmentent les risques auxquels eux sont exposés lorsqu'ils sont connectés à Internet et qui leur sont inhérents, dont l'immaturité et leur inconscience.

Par conséquent, comprendre que le mineur fait partie d'un groupe vulnérable et qu'il a donc besoin d'une protection juridique spéciale, est le point de départ pour les gouvernements et les organismes ou entités responsables chargés de la protection des données dans différents pays, pour développer des normes et des politiques qui comblent le vide juridique qui existe en matière de protection des données des mineurs.

---

[49] *Ibid*, art 3(1).
[50] Art 33 CcQ
[51] *Loi sur la protection de la jeunesse*, RLRQ c. P-34.1, art 3.
[52] *L'intérêt supérieur de l'enfant : signification et mise en application au Canada*, Coalition canadienne pour les droits des enfants, 2009 aux pp 8-26.
[53] *Loi sur la protection du consommateur*, RLRQ c P-40.1, art 248.
[54] *Ibid*, art 249.
[55] *Loi sur la protection du consommateur*, *supra* note 53.
[56] *Irwin Toy Ltd c Québec (Procureur général)*, [1989] 1 RCS 927 .

À ce sujet, nous terminerons par une citation de la professeure Lina Orneales, qui résume clairement la nécessité de protéger le mineur par le biais de la réglementation[57].

> « Face à la vulnérabilité des mineurs et aux nouvelles formes de coexistence sociale par le biais des réseaux sociaux numériques, le droit ne peut pas rester à la traîne. Internet est un espace plein d'opportunités, c'est la porte du monde de la connaissance urbi et orbi, et l'un des nouveaux rôles de l'État consiste à faire comprendre qu'il ne s'agit pas d'un espace sans loi » [notre traduction][58].

1.3. Règles particulières insuffisantes

Bien que les mineurs représentent un tiers des utilisateurs d'Internet, les politiques en vigueur dans le monde ne tiennent pas spécifiquement compte de leurs droits et de leurs besoins particuliers. Aux niveaux national et international, nous constatons qu'il existe des règles et des lignes directrices qui ont énoncé les principes généraux de tout traitement des données, mais uniquement de manière générale, sans référence expresse au cas des mineurs.

Nous pouvons le constater dans des instruments et directives internationaux, dont la résolution 45/95 de l'Assemblée générale des Nations Unies du 14 décembre 1990, sur les principes directeurs relatifs à la réglementation des fichiers informatisés de données à caractère personnel [59], l'Observation générale nº 16 du Comité des droits de l'homme[60] où il est expressément fait référence au traitement de données à caractère personnel et les résolutions 68/167 et 69/166 sur le droit à la vie privée à l'ère numérique[61].

Nous trouvons un autre exemple dans la LPRPDE canadienne qui ne prévoit aucune disposition spécifique concernant les mineurs. Toutefois, le législateur et les entités de protection

---

[57] Lina Ornelas, « El derecho de las niñas, niños y adolescentes a la protección de sus datos personales: evolución de derechos y su exigencia frente a las redes sociales » dans *Protección Datos Pers En Las Redes Soc Digit En Part Niños Adolesc*, Buenos Aires, Argentina : Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) y del Instituto de Investigación para la Justicia (IIJusticia), 2011.

[58] *Ibid* à la p 73.

[59] *Principes directeurs pour la réglementation des fichiers personnels informatisés*, Doc off AG NU, 45e sess, 68e séance, Doc NU A/RES/45/95 (1990).

[60] Voir notamment *Observation générale no 16: Article 17 (Droit au respect de la vie privée)*, Doc off HCDH NU, 32e sess (1988), Doc NU HRI\GEN\1\Rev.1 (1994).

[61] Voir notamment *Le droit à la vie privée à l'ère du numérique*, Doc off AG NU, 75e Sess, Doc NU A/RES/75/176 (2020); *Le droit à la vie privée à l'ère du numérique*, Doc off AG NU, 69e Sess, 73e Séance, Doc NU A/RES/69/166 (2014); *Le droit à la vie privée à l'ère du numérique*, Doc off AG NU, 68e sess, 70a séance, Doc NU A/RES/68/167 (2013).

à la vie privée ont reconnu que l'enfant avait besoin d'une protection spéciale compte tenu de sa vulnérabilité.

À l'opposé, rares sont les systèmes juridiques du monde qui ont accompli un travail considérable pour contrôler et limiter le traitement inadéquat des données des mineurs sur Internet. On peut citer notamment les États-Unis qui, par l'entremise du COPPA, réglementent le traitement des données à caractère personnel pour les enfants et aussi l'Union européenne qui consacre au traitement des données relatives aux mineurs l'article 8 du RGPD.

Comme nous le verrons au Titre 2 de la Partie II de ce mémoire, COPPA exige que les exploitants des sites Web, des applications mobiles, des tablettes et d'autres technologies similaires conçues pour les mineurs de moins de 13 ans ou des sites dirigés à un public en général ayant une connaissance effective qu'ils traitent des données personnelles des mineurs, obtiennent le consentement « vérifiable » des parents avant de recueillir ou de partager des renseignements auprès des mineurs de moins de 13 ans.

Pour sa part, le RGPD dispose que le traitement des données personnelles d'un mineur est considéré licite lorsqu'il est âgé d'au moins 16 ans, mais donne aux États membres le pouvoir de fixer par la loi un âge qui ne peut être inférieur à 13 ans. En Espagne, à titre d'exemple, l'âge minimum a été fixé à 14 ans.

Mais la question qui se pose est-elle de savoir si tous ces efforts sont suffisants pour protéger les mineurs qui circulent sur le réseau? Ne sera-t-il pas nécessaire d'établir des paramètres internationaux pour la protection des données des mineurs, y compris une limite d'âge généralisée à partir de laquelle les mineurs peuvent donner leur consentement, des critères et procédures pour légitimer le consentement donné par le mineur au traitement de ses données personnelles?

Dans le même ordre d'idées, la Red Iberoamericana[62] pour la protection des données a évoquée qu'en matière de protection des données personnelles il manque des critères universels contraignants qui protègent la vie privée des mineurs, les plus vulnérables, en indiquant ce qui suit :

[62]La Red Iberoamericana de protección de datos (ci-après « RIPD ») *se définit comme un forum qui développent des initiatives et des projets relatifs à la protection des données à caractère personnel en Amérique latine*. En ligne : <http://www.redipd.org/index-ides-idphp.php>.

> « Les normes internationales à caractère contraignant brillent par leur absence et les quelques instruments juridiques qui existent brillent par leur manque de précision et leur caractère de "minimum" avec les conséquences que cette insécurité juridique provoque notamment, lorsque les données appartiennent aux mineurs »[63].

Par conséquent, les problèmes d'insécurité juridique tiennent à l'absence de règles régissant la protection des droits des mineurs en général et de leurs données en particulier. Dans cet esprit, l'UNICEF, dans un rapport[64], est catégorique en soulignant que pour protéger les mineurs en ligne, il est nécessaire de combler toutes les lacunes qui peuvent survenir en ce qui concerne l'utilisation et la protection de mineurs lors de l'utilisation des TIC et de Internet, dans les termes suivants :

> « Tout d'abord, nous devons identifier et combler les lacunes dans l'accès à des ressources en ligne de qualité, la connaissance de ce que les enfants font sur Internet et la compréhension par les enfants de la manière de se protéger en ligne, mais aussi dans l'élaboration des politiques et des cadres réglementaires, qui ne se sont pas adaptés au rythme des changements » [65].

Il est donc nécessaire de protéger les mineurs contre les dangers que peut présenter le traitement abusif de leurs données. Des comportements, comme le vol de données, la cyberintimidation, le leurre par Internet, le *sextage*, la publicité trompeuse et la publicité ciblée se manifestent à cause de la facilité avec laquelle on peut accéder aux données. De surcroît, il faut aussi faire face aux rares mécanismes de protection, au manque d'outils pour combattre ces pratiques et l'absence de sensibilisation au moment de l'exécution des activités lors de la navigation sur Internet.

En conclusion, la sécurité juridique sera renforcée par la mise en place d'un cadre juridique plus costaud et plus cohérent en matière de protection des données pour les mineurs utilisant les TIC et Internet, mais aussi il est urgent de renforcer tous les domaines susceptibles de contribuer à la sécurité des enfants sur Internet dont le domaine familial, social et juridique.

Le domaine familial fait référence à l'accompagnement de l'enfant par les membres de sa famille lorsqu'il navigue sur Internet. Le domaine social réfère aux politiques éducatives de l'enfant, aux familles, aux éducateurs et à la communauté, par des campagnes et/ou politiques

---

[63] *Informe 2016. Tema monográfico: la protección de datos de los menores de edad*, por Guillermo Escobar Roca, dialnet.unirioja.es, Madrid, España, Red Iberoamericana de Protección de Datos, 2017.
[64] note 11.
[65] *Ibid* à la p 9.

publiques sur les risques auxquels les mineurs sont exposés lors du traitement de leurs données dans des environnements virtuels. Quant au domaine juridique, il est lié à la responsabilité des États de modifier et/ou de compléter, selon le cas, les normes relatives à la protection des données des mineurs dans le cyberespace, et ce, afin de garantir et d'assurer une plus grande sécurité juridique, en tenant compte de la protection spéciale et de l'intérêt supérieur du mineur.

Chapitre 2 – Distinction des définitions entre « Mineur » et « Enfant »

2.1. Le terme mineur est-il plus large que celui « d'enfant »?

D'emblée, il nous faut préciser que cette étude ne vise pas à détailler la manière dont le traitement juridique du mineur a évolué au cours de l'histoire, mais il est clair que le XX^{e} siècle trace une ligne qui marque un avant et un après dans son développement.

Au départ, les enfants étaient considérés comme des êtres passifs, « êtres inachevés »[66], soumis entièrement à l'autorité parentale[67]. Ensuite, au XX^{e} siècle, apparaît la notion d'enfants en tant que sujets indépendants de droits et considérés comme des êtres en développement possédant une dignité intégrale[68]. L'octroi d'une protection spéciale se pose parce qu'ils sont conçus comme des êtres dans le besoin en raison de leur immaturité.

Dans ce cadre, un ensemble de règles spécifiques concrètes est développé dans le domaine particulier de l'enfance. C'est ainsi que surgit le courant puérocentrique[69], c'est-à-dire un système dans lequel « l'enfant » devient la figure qui reçoit toutes sortes de privilèges et d'avantages légaux, parfois même en dépit et en opposition de ses propres parents. Les règles et l'interprétation de cette théorie trouve son expression la plus pertinente dans le principe juridique de « l'intérêt

[66] Thierry Moreau, « Cent septante-cinq ans de regards sur l'enfant » (2005) 175-25:6205 J Trib 814-815.
[67] Edith Deleury, Michèle Rivet & Jean-Marc Neault, « De la puissance paternelle à l'autorité parentale : Une institution en voie de trouver sa vraie finalité » (1974) 15:4 Cah Droit 779-870.; voir aussi : Guy Raymond, « L'autorité parentale sous contrôle ? » (2003) 22:2 Enfances Psy 25-37.
[68] Dominique Youf, « Seuils juridiques d'âge : du droit romain aux droits de l'enfant » (2011) n°11 Sociétés Jeun En Diffic Rev Pluridiscip Rech, en ligne: <http://journals.openedition.org/sejed/7231> aux pp 4-6.; Voir Fédération des associations de parents de l'enseignement officiel, *L'évolution de la place de l'enfant dans la société* , FAPEO, 2008 aux pp 8-11. En ligne : <https://www.fapeo.be/wp-content/analyses/archives/Place_enfant_societe.pdf>
[69] *CDE Observation générale no 14*, *supra* note 47.

supérieur de l'enfant » (ou meilleur intérêt de l'enfant)[70]. Cela implique que chaque enfant doit être protégé au-dessus de tout autre sujet, tel que son père ou sa mère, ses tiers ou l'administration publique. Par conséquent, il est dit que l'intérêt du mineur prévaut sur les intérêts d'autres sujets, raison pour laquelle la vision puérocentrique est prioritaire par rapport à toute autre considération[71].

L'émergence des droits de l'enfant a été principalement le fait des organisations internationales et de la doctrine des droits de l'enfant. Ce développement a eu une influence importante sur les législations mondiales, en particulier sur les normes suprêmes. Au plan international, la CIDE constitue le document le plus important. Dans son texte, se trouve tant la définition du mot « enfant » en tant que mineur, que la conception puérocentrique du droit, exprimée dans « l'intérêt supérieur de l´enfant ».

L'article premier prévoit que: « Au sens de la présente Convention, un enfant s'entend de tout être humain âgé de moins de dix-huit ans, sauf si la majorité est atteinte plus tôt en vertu de la législation qui lui est applicable » et l'article 3.1 ajoute que : « Dans toutes les décisions qui concernent les enfants, […] l'intérêt supérieur de l'enfant doit être une considération primordiale ».

Du texte des articles 1 et 3.1 précédemment cités, on peut rapidement conclure que la CIDE utilise le mot « mineur » et « enfant » comme synonymes. On estime qu'il faut déterminer si le concept approprié pour désigner ce groupe de population est celui de « mineur » ou, au contraire, on devrait recourir à d'autres termes, récents et de plus en plus acceptés, comme « filles, garçons, pré-adolescent(es), adolescents(es) », expressions largement utilisées dans les pays d'Amérique centrale et du Sud[72].

---

[70] Sénat du canada, *La cyberintimidation, ça blesse! : respect des droits à l'ère numérique : Rapport du Comité sénatorial permanent des droits de la personne*, 9, (décembre 2012) (présidente: Mobina S B Jaffer, vice-président: Patrick Brazeau) à la p 58; note 52 à la p ´6., en ligne: <https://www.fundacionhenrydunant.org/images/stories/biblioteca/derecho-ninos-ninas/QL-yiwAzxp7.pdf.pdf> (consulté le 1 décembre 2019).

[71] Alfonso-Luis Calvo Caravaca & Javier Carrascosa González, « Protección de menores » dans *Derecho Int Priv*, 18e éd, Granada, España, 2018 1496 à la p 354.

[72] Instituto de investigación para la justicia, *Mémorandum de Montevideo: Mémorandum sur le droit à la protection des renseignements personnels et la vie privée dans les réseaux sociaux sur l'Internet, en particulier ceux des enfants et des adolescents* , IIJusticia, 2009. Le Mémorandum définit un cadre réglementaire contenant des recommandations pour les pays d'Amérique latine, afin d'atteindre un équilibre entre la protection des droits de l'enfant et la protection contre les risques auxquels ils sont exposés en ligne.

De même, l'article 2 de la *Convention nº 182* de l'*Organisation internationale du Travail* de 1999 (ci-après « OIT »[73]) sur les pires formes de travail des enfants, précise que le terme « enfant » s'applique à « l'ensemble des personnes de moins de 18 ans ».

Le premier défi est de distinguer les notions de « mineur » et « enfant »[74]. Ces expressions sont souvent confondues en utilisant des sens généraux ou confus. Cela pose également d'autres problèmes qui vont au-delà de l'aspect purement sémantique. Le terme *mineur* est une expression de sens juridique et se rapporte à la condition de la personne qui, en raison de son âge, n'a pas atteint la pleine capacité civile. En revanche, l'expression *enfant* désigne les personnes qui se trouvent dans l'étape comprise entre la naissance et le début de l'adolescence. Autrement dit, le mineur n'est pas seulement l'enfant, mais les adolescents sont également inclus dans la catégorie des mineurs.

L'emploi du terme « mineur » comme synonyme d'« enfant », « adolescent » et « jeune », peut se faire en dehors du cadre juridique, raison pour laquelle la CIDE précitée utilise ces deux termes indistinctement. Autrement dit que la notion d'« enfant » peut être utilisée non pas comme une donnée biologique ayant un effet juridique, mais comme une référence comparative de la personne adulte en général.

C'est pourquoi l'expression « mineur », dans le domaine juridique, est plus large et comprend l'enfant et l'adolescent, notamment tous ceux qui n'ont pas atteint l'âge de la majorité. Force est de constater que l'âge de la majorité est une question sujette à des variations en fonction du moment historique et de chaque juridiction.

À partir de ce qui précède, il faut déterminer ce qu'est un « mineur » du point de vue juridique[75]. Comme indiqué précédemment, selon la CIDE on entend par enfant tout être humain âgé de moins de dix-huit ans. Cette disposition n'étant pas obligatoire, les États membres peuvent

---

[73] *Convention C182 concernant l'interdiction des pires formes de travail des enfants et l'action immédiate en vue de leur élimination*, Organisation international du travail [OIT], 17 juin 1999, Doc OIT C182/1999, 87ème session (entrée en vigueur : 19 novembre 2000), art 2.

[74] Groupe de travail interinstitutionnel sur l'exploitation sexuelle des enfants 2016, *supra* note 8 à la p 1. L'absence de consensus international concernant le langage qui devrait être utilisé a eu un impact négatif sur les efforts mondiaux pour la collecte des données et l'identification de différentes modalités d'exploitation et d'abus sexuels des enfants.

[75] Voir notamment Académie française, *Dictionnaire de l'Académie française*, 9e éd, France, 2011 *sub verbo* « mineur ». Les principaux dictionnaires renvoient au terme légal désignant comme « mineur » « *Qui n'a pas atteint l'âge de la majorité légale* ». En ligne : <https://www.dictionnaire-academie.fr/article/A9M2240>.

fixer l'âge de la majorité différemment. De même, les États peuvent indiquer l'âge auquel l'enfant devient majeur en matière civile et du travail, et aussi à partir de quel âge il assume la responsabilité pénale. En revanche, la Convention nº 182 de l'OIT n'autorise pas de telles exceptions.

Par exemple, des États membres qui ont ratifié la CIDE, comme la Colombie, le Brésil, les pays membres de l'Union européenne et certaines provinces du Canada (notamment le Québec, l'Ontario, l'Alberta et le Manitoba) ont fixé l'âge de la majorité conformément à la recommandation de la CIDE, en clair, à 18 ans. Toutefois, certains États membres ont prévu dans leur législation des âges différents, à titre d'exemple en Argentine il est acquis à 21 ans, au Paraguay à 20 ans, en Écosse à 19 ans et dans certaines provinces du Canada à 19 ans.

Deux précisions doivent être apportées, la première étant que la nature juridique de l'expression « mineur » est civile; en d'autres mots que la minorité fait référence à un état civil de la personne. Or, bien que la notion d'état civil soit complexe et ne fasse pas l'objet d'un développement dans ce travail, le concept d'état civil qualifie l'âge de la minorité en tant qu'état de la personne.

Deuxièmement, il faut préciser que la différence entre un majeur et un mineur ne réside pas dans la capacité d'être sujet de droit (capacité juridique[76]), mais dans la capacité d'agir[77]. En d'autres termes, le mineur, même s'il est titulaire de droits dès sa conception (dans certaines législations) ou à la naissance, est limité pour l'exercer en raison de sa minorité (état civil) et du degré de maturité (capacité naturelle). Les mineurs, lorsqu'ils atteignent l'âge de la majorité acquièrent la pleine capacité d'agir (sauf exceptions prévues par la loi). Ils deviennent donc les titulaires actifs d'un droit qu'ils peuvent exercer eux-mêmes.

Néanmoins, une grande partie des législations mondiales consacrent des dispositions prévoyantes, pour un certain acte juridique spécifique, un âge qui diffère de la minorité civile, en

[76] Gaël Henaff, « L'enfant, l'âge et le discernement » (2000) 44 Lien Soc Polit 41-50 à la p 42. Voir aussi, Le Curateur public du Québec, « Les droits du mineur - Tutelle des biens du mineur », en ligne: <https://www.curateur.gouv.qc.ca/cura/fr/mineur/tutelle-biens/droits/index.html>. À cette égard le curateur public indique que « [c]'est à 18 ans, âge de la majorité au Québec, que l'enfant devient pleinement apte à exercer tous ses droits civils (exemples : conclure un contrat important, disposer d'importants montants d'argent, faire un emprunt). Avant cet âge, il ne peut agir seul ».

[77] Il faut noter ici que cette distinction n'existe pas dans les systèmes juridiques de commom law, mais il existe de « legal capacity » qui distingue une capacité passive (to acquire rights) et une capacité active (to act).

reconnaissant la capacité des mineurs à accomplir cet acte, par exemple en se mariant, en testant ou pour consentir le traitement de données à caractère personnel sans qu'il faille faire appel à leurs représentants (âge de la majorité numérique).

En bref, lorsque l'âge de la majorité diffère, nous choisirons d'utiliser le terme « mineur » ou « mineurs » indistinctement, sauf dans les cas où une loi ou une directive les désigne comme enfant, adolescent, jeune ou autrement. Ces termes définissent le champ d'application et assurent une plus grande sécurité juridique que l'emploi du terme « enfant ».

Une fois défini, le terme à utiliser dans ce mémoire pour désigner les mineurs comme sujets de droit nécessitant une protection spéciale de leurs données dans le cyberespace, il est impératif que des règles spéciales soient adoptées pour protéger les mineurs sur Internet. Des règles qui protègent la capacité du mineur d'être sujet de droits (facteur objectif de l'âge) ainsi que sa capacité à exercer des droits en fonction du degré de son développement ou de sa maturité (facteur subjectif)[78], et ce, en harmonisant ces deux facteurs.

2.2. Que faut-il entendre par majorité numérique?

En règle générale, une personne acquiert sa majorité civile[79] à l'âge de 18 ans ou à l'âge fixé par chaque loi, comme nous l'avons vu précédemment. Toutefois, le législateur peut fixer un âge différent de celui de la majorité civile, en reconnaissant la capacité d'agir des mineurs pour la réalisation d'un acte juridique spécifique. En accordant ce privilège aux mineurs, le législateur tient compte du principe de la capacité ou de l'autonomie progressive[80], notamment le processus progressif par lequel les mineurs peuvent exercer eux-mêmes des droits en fonction de leur âge et de leur degré de maturité.

Dans ce contexte, la majorité numérique correspond à l'âge auquel le régulateur considère qu'une personne peut consentir librement à un traitement de données à caractère personnel. Une fois que la majorité numérique a été obtenue, le mineur peut, par lui-même, et sans l'autorisation

[78] Milda Macenaite & Eleni Kosta, « Consent for processing children's personal data in the EU: following in US footsteps? » (2017) 26:2 Inf Commun Technol Law 146-197 à la p 154.
[79] Académie française, *supra* note 75 *sub verbo* « majorité ». Le terme indique « …âge, déterminé par la loi, auquel une personne devient en droit capable et responsable. Atteindre la majorité civile… »).
[80] Voir aussi Mª Belén Andreu Martínez, *La protección de datos personales de los menores de edad*, 1ᵉ éd, Navarra, España, Thomson Reuters Aranzadi S.A, 2013 à la p 68.

préalable de ses parents ou du tuteur légal, disposer et donner son consentement pour que les fournisseurs de services aient accès et recueillent ses données à des fins commerciales. Autrement dit, la majorité numérique consiste à fixer l'âge légal minimal en vertu duquel les mineurs doivent obtenir l'autorisation de leurs parents ou tuteurs légaux pour consentir au traitement de leurs données; par exemple pour créer un compte courriel, s'inscrire sur des plateformes ou des applications ou sur un réseau social, que ce soit *Facebook*[81], *Snapchat*[82], *YouTube*[83] ou *Instagram*[84].

Actuellement, par exemple, l'âge légal prévu pour s'inscrire sur la plateforme de *Facebook* et *Instagram* est 13 ans. Toutefois, dans les conditions d'utilisation, il est précisé que l'âge minimum peut être différent, si le pays à partir duquel la personne s'inscrit, exige un âge minimum différent. Il semble alors que ces réseaux sociaux se déresponsabilisent en passant aux utilisateurs l'obligation de vérifier si, conformément à la loi où ils habitent, ils atteignent l'âge de la majorité numérique. Cependant, comme nous le verrons dans les prochains chapitres, la question de la validation de l'âge n'est pas exempte d'interprétations ambiguës en raison d'une réglementation insuffisante.

Il se dégage de ce qui précède la question de savoir à quel âge les mineurs peuvent donner leur consentement au traitement de leurs données sans l'autorisation de leur tuteur?[85]. En effet, il n'existe actuellement aucune approche unifiée permettant de déterminer l'âge auquel un mineur est en mesure de gérer lui-même ses données personnelles et, sur la base de ce critère, fixer un âge spécifique et unifié de majorité numérique.

---

[81]Voir « Facebook » dans *Wikipédia Encycl Libre*. « Facebook [ˈfeɪsbʊk] est un réseau social en ligne qui permet à ses utilisateurs de publier des images, des photos, des vidéos, des fichiers et documents, d'échanger des messages, joindre et créer des groupes et d'utiliser une variété d'applications ».

[82]Voir « Snapchat » dans *Wikipédia Encycl Libre*.« Snapchat (ou Snap dans le langage courant) est une application gratuite de partage de photos et de vidéos de la société Snap Inc »).

[83]Voir « YouTube » dans *Wikipédia Encycl Libre*.(« YouTube (en français : [jutyb] ou [jutjub]a, en anglais : [ˈjutub]b) est un site web d'hébergement de vidéos et un média social sur lequel les utilisateurs peuvent envoyer, regarder, commenter, évaluer et partager des vidéos ».

[84]Voir « Instagram » dans *Wikipédia Encycl Libre*. « Instagram [ˈɪnstəgɹæm] » est une application, un réseau social et un service de partage de photos et de vidéos fondée et lancée en octobre 2010. Depuis 2012, l'application appartient à Facebook ».

[85] Chambre des communes du Canada, *Vers la protection de la vie privée dès la conception : examen de la loi sur la protection des renseignements personnels et les documents électroniques : Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique*, 42e législature, 1re session (Février 2018) (président: Bob Zimmer) aux pp 38-39.

Pour déterminer la capacité d'un mineur à accomplir certains actes ou à exercer ses droits, les régulateurs devront recourir à une discipline différente du droit, comme l'est la psychologie évolutionniste (évopsy). Cette discipline fournira un guide pour savoir dans quelle tranche d'âge le mineur acquiert un développement psychologique adéquat qui lui permet de comprendre et d'exercer de façon responsable ses droits. Certains considèrent que l'on peut fixer l'âge entre 12 ou 16 ans[86].

En ce sens, l'âge apparaît comme une circonstance objective[87], de sorte qu'il est plus sûr de recourir au critère de l'âge plutôt qu'à celui de la maturité suffisante du mineur. Il est clair que le deuxième concept peut être plus juste, mais si l'on considère que l'âge et la maturité varient d'une personne à l'autre, le critère de l'âge apporte une plus grande sécurité juridique[88]. Si une norme de protection est établie en se référant à un degré de maturité ou de jugement plus élevé uniquement sans fixer d'âge, il faudra analyser chaque cas d'une façon particulière.

En ce qui concerne le concept de majorité numérique, il faut partir du fait que les différentes législations internationales qui ont inclus dans leurs normes de protection des données une référence spécifique aux mineurs, ne parviennent pas à harmoniser entre elles l'âge minimum d'un mineur pour la navigation. Plus important encore, ils ne parviennent pas à harmoniser l'âge dans son propre cyberespace, comme c'est le cas actuellement dans l'Union européenne qui, en vertu de l'article 8 du RGPD, laisse aux États membres le soin de l'établir entre 13 ans et 16 ans.

Le tableau suivant montre le statut de l'âge du consentement dans les 27 États membres de l'UE. Comme nous le verrons, la majorité des pays se trouvent aux extrémités de la fourchette

[86] Voir à cet égard *Children's Data and Privacy Online: Growing Up in a Digital Age An Evidence Review*, by Sonia Livingstone, Mariya Stoilova & Rishita Nandagiri, London, London School of Economics and Political Science, 2018 aux pp 8-10; *RGPD*, *supra* note 39, art 8.
[87] Stefano Rodota, « Contemporary society, the privacy of minors and social networks » dans *Soc Netw Child Priv*, Madrid, España, Editorial Reus, 2011 47 à la p 48.
[88] Gil Antón Ana María, *El derecho a la propia imagen del menor en Internet*, Madrid, España, Dykinson S.L., 2013 à la p 229.

autorisée par le règlement, à savoir 13[89] et 16[90] ans. Seuls quelques-uns ont maintenu l'âge à 14[91] ou 15[92] ans.

Tableau I : Âge de consentement dans les pays de l'UE

Âge de consentement dans la EU (Article 8 RGPD)					
13 ans			**14 ans**		
Belgique	Danemark	Estonie	Autriche[1]	Bulgarie[2]	Chypre[3]
Finlande	Lettonie	Malte	Italie[4]	Espagne[5]	Lituanie[6]
Portugal	Suède				
15 ans			**16 ans**		
France	Grèce	Tchèque	Irlande	Pays-Bas	Croatie
			Slovaque	Allemagne*	Hongrie
			Pologne*	Roumanie*	Luxembourg
			Slovénie**		

* La loi sur la protection des données reste silencieuse au sujet de l'âge de la majorité numérique. Il est donc entendu que l'âge de la majorité numérique est de 16 ans conformément au RGPD.
** La loi sur la protection des données est en cours d'adoption. Une fois la loi soit adoptée, l'âge de la majorité sera de 15 ans.

D'ailleurs, d'autres pays non-membres de l'UE ont légiféré conformément au RGPD, dont le Royaume-Uni qui a fixé l'âge de la majorité numérique à 13 ans[93] et la Serbie qui a opté pour les 15 ans[94]. Pour sa part, la loi américaine COPPA interdit la collecte des données personnelles sur des jeunes de moins de 13 ans sans autorisation parentale.

---

[89] Belgique : Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 30 julliete 2018, JO, 5 septembre 2018, p. 68616, n° 2018040581, art. 7; Danemark : LOV nr 502 af 23/05/2018, JO, 24 mai 2018, n° 7910-0004Art. 6(2). (Uniquement en danois); Estonie: Personal Data Protection Act (2018), JO, 4 janvier 2019, p 11, Ch. 3, art. 8; Finlande : Data Protection Act (1050/2018), abrogeant l'ancienne loi sur les données personnelles (523/1999). art. § 5; Lettonie : Personal Data Processing Law (June 2018), JO, 4 juin 2018, n° op 2018/132.1, art 33; Malte: Ch. 586 Data Protection Act (28 mai 2018), art 33(g); Portugal: Lei nº 58/2019, JO, 8 août de 2019, p. 3, n° 151/2019 (série I), art. 16; (Notre traduction); Suède: Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, JO, 24 avril 2018, ch 2 (art. 4). (Uniquement en suédois).

[90] Irlande : Data Protection Act 2018 (Act 7 of 2018), JO, 29 mai 2018, nº SI 174/2018, art. 31(1); Pays-Bas : Uitvoeringswet Algemene Verordening gegevensbescherming ("UAVG "), JO, 22 may 2018, nº stb-2018-144, art. 5. (Uniquement en néerlandais); Slovaque : Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (18/2018 Z. z), 2017, JO, 30 janvier 2018, art 15(1). (uniquement en slovaque).

[91] Autriche: Federal Act concerning the Protection of Personal Data (DSG) (BGBl. I Nr. 120/2017), JO, 31 juillet 2017, nº 14/2019, art. 2 § 4 (4); Bulgarie: Loi sur la protection des données personnelles, JO, 26 février 2019, n° 17, art 25(c); Chypre: Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018 (125(I)/2018), JO, 31 juillet 2018, p. 827, nº 4670, art. 8 (1). (uniquement en grec); Italie: Codice in materia di protezione dei dati personali (Decreto legislativo, n.196 du 30 giugno 2003), JO, 4 septembre 2018, n° 205, art. 2- quinquies. (uniquement en italien); Espagne: Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, OJ, 6 diciembre 2018, sec. I, p. 119788, n° 294, art. 7, (uniquement en espagnol); Lituanie: Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas 1996 m. birželio 11 d. Nr. I-1374, OJ, 3 juil. 1996, n° 63-1479, art. 6. (uniquement en lituanien). Nouvelle version de 2018-07-16: No XIII-1426, 30/06/2018, publié sur TAR 2018-07-11, soit 2018-11733.

[92] France : Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO, 7 janvier 1978, 227, n° 0006, art 45 ; Grèce : Law 4624/2019, JO, 29 august 2019, art 21; Tchèque : Zákon č. 110/2019 Sb, 2. března 2019, § 7.

[93] Data Protection Act 2018 (R-U), article 9 (a).

[94] Serbie : Закон о заштити података о личности, JO, 13 novembre 2018, nº RS 87, art. 16.

Dans le titre 2 (Partie II) de ce mémoire de maîtrise, on pourra constater que les progrès accomplis par certaines législations sont indéniables. Ainsi, la tentative d'établir une majorité numérique nous rapproche d'une meilleure protection des droits des mineurs et surtout, loin de limiter la liberté des enfants et des adolescents comme l'ont indiqué certains détracteurs de la disposition européenne[95], l'objectif est de préserver la sécurité de nos mineurs. À cet égard, nous examinerons de manière claire et spécifique, ce qui concerne la majorité d'âge numérique en Europe, au Canada et aux États-Unis. En outre, nous analyserons les aspects positifs et négatifs de sa mise en œuvre.

En terminant, on laisse une autre question importante dans le débat : dans le dessein d'obtenir une plus grande sécurité juridique, la règle objective de l'âge doit-elle alors s'appliquer, tant pour consentir au traitement des données, que pour l'exercice des droits d'accès, de rectification, de cession et d'obtention des données des mineurs?[96] (ci-après « droits ARCO »[97]).

Titre 2 – Risques, mineurs et données personnelles

Chapitre 1 – Risques auxquels sont confrontés les mineurs

Les progrès des TIC et l'utilisation de l'Internet ont sans aucun doute contribué à améliorer les mécanismes d'éducation et de communication, l'accès à l'information et au savoir[98]. Toutefois, à côté des multiples avantages et opportunités[99] que représente l'utilisation de ces outils, on trouve les risques auxquels les mineurs sont exposés[100].

---

[95] Voir à cet égard Djordje Krivokapic & Jelena Adamovic, « Impact of general data protection regulation on children's rights in digital environment » (2016) 64 Anali Pravnog Fak U Beogr 205-220 aux pp 209-2011.
[96] José Luis Piñar Mañas, « The fundamental right of data protection and privacy of minors in social networks » dans *Soc Netw Child Priv*, Editorial Reus, 2011 61 à la p 97,105. Gil Antón, *supra* note 88 à la p 193.
[97] Andreu Martínez, *supra* note 80 aux pp 148-157.
[98] Milda Macenaite & Eleni Kosta, « Consent for processing children's personal data in the EU: following in US footsteps? » (2017) 26:2 Inf Commun Technol Law 146-197 à la p 146.
[99] Jon Brown, *Online Risk to Children: Impact, Protection and Prevention*, 1e éd, John Wiley & Sons Ltd, 2017 à la p 1.
[100] Canada, Bureau de l'Ombudsman et du défenseur des enfants et de la jeunesse, Il devrait y avoir une loi : Les sauts périlleux de la vie privée des enfants au 21e siècle, Ottawa, Ont, Groupe de travail des commissaires à la vie privée et des défenseurs canadiens des enfants et des jeunes, 2009 aux pp 4-5,7 En ligne :

La sociologue S. Livingstone estime qu'il est très difficile de tracer la limite entre les possibilités et les risques auxquels les mineurs sont exposés en ligne[101], car il existe une corrélation entre les deux concepts, autrement dit, plus d'opportunités, plus de risques[102]. C'est pourquoi, aux fins de notre analyse, nous nous efforcerons de séparer ces deux aspects en nous penchant en particulier sur les risques auxquels les mineurs sont exposés par rapport à leurs données personnelles.

À ce sujet, il est important de rappeler que chaque jour les mineurs partagent volontairement[103] *(« extimité »*[104]) ou involontairement toutes sortes d'informations en ligne. Les mineurs fournissent des informations qui sont traditionnellement considérées comme sensibles, telles que le nom, la date de naissance, l'adresse de résidence, le courrier électronique, le numéro d'identification et des photos qui révèlent l'image personnelle[105]. Mais ils partagent aussi d'autres types d'informations qui, selon le contexte, peuvent être considérées comme des informations à caractère personnel. Par exemple, on peut citer ici des commentaires publiés sur les réseaux sociaux, les blogues ou les tweets (ces commentaires révèlent entre autres des goûts, des préférences, des pensées, des idées)[106]. À leur tour, nous trouvons les données techniques provenant du simple fait de naviguer sur Internet, parmi lesquelles nous pouvons citer « une adresse IP, la géolocalisation d'une personne, les informations contenues dans les cookies, l'identification unique d'un appareil mobile ou l'historique des sites web visités par une personne »[107].

<https://www.cyanb.ca/images/ChildrensOnlinePrivacy-f.pdf>.; Macenaite & Kosta, « Consent for processing children's personal data in the EU », *supra* note 98 à la p 146.; Brown, *supra* note 99 à la p 2.; Agencia española de protección de datos, *Ficha didáctica: Situaciones de riesgo en el entorno Web 2.0: Suplantación de identidad, Ciberbullying, Grooming, Sexting* à la p 3. En ligne : <http://tudecideseninternet.es/aepd/images/articulos/ficha-06.pdf.>.

[101] Sonia Livingstone, « Children's and Young People's Lives Online » dans *Online Risk Child*, 1e éd, John Wiley & Sons, Ltd, 2017 23 à la p 23.

[102] *Ibid* à la p 32.; voir aussi Andy Phippen, « Cyberbullying and Peer-Oriented Online Abuse » dans *Online Risk Child* The NSPCC/Wiley Series, 1e éd, John Wiley & Sons, Ltd, 2017 37 à la p 37.

[103] Commission d'accès à l'information du Québec, *supra* note 12 à la p 29.

[104] Voir notamment: Serge Tisseron, Sylvain Missonnier & Michaël Stora, *L'enfant au risque du virtuel*, Dunod, 2012 à la p 18,137-149. Le terme d'«extimité» est utilisé notamment dans le domaine des réseaux sociaux, pour faire référence à l'information que l'utilisateur décide de publier et de communiquer ouvertement sur son profil de réseau social; Voir aussi Caroline Vallet, *La protection des mineurs face à la cyberpédopornographie : étude comparée entre le droit criminel canadien et français*, yvon blais éd, Minerve, Montréal, Québec, 2011 à la p 199.; *Les jeunes et Internet : de quoi avons-nous peur ?*, by Élodie Kredens & Barbara Fontar, France, Fréquence écoles org, 2010.

[105] Option consommateurs, *supra* note 5 à la p 42.

[106] *Ibid* aux pp 42-43.

[107] *Ibid*.

Des facteurs tels que le manque de maturité[108], l'utilisation inadéquate de l'Internet sans supervision d'un adulte, la croyance qu'ils sont experts dans l'utilisation de ces outils, la configuration inadéquate des paramètres de confidentialité[109], la croyance que l'anonymat existe[110] et l'impunité dans le cyberespace sont des conditions qui augmentent la possibilité pour les mineurs de s'exposer à des comportements portant atteinte à leur vie privée et de devenir des victimes ou des auteurs d'abus ou de comportements répréhensibles.

À cela s'ajoute le fait que les mineurs ne sont souvent pas conscients de ces dangers[111], et sont moins conscients de l'impact que la transmission massive de données peut avoir dans un avenir rapproché, et pas seulement sur leur réputation en ligne, mais aussi tout au long de leur développement familial, social et professionnel.

Le mineur ne sait pas que toutes les informations qu'il fournit façonnent son identité numérique[112], et comme cette information restera, sauf exception, de façon permanente dans le monde en ligne[113], elle se transforme avec le temps, vers un individu pleinement identifiable[114]. Comme l'explique le professeur S. Rodota, le mineur peut parfois analyser ipso facto les risques et les conséquences à court terme d'un acte, mais il lui est difficile de prévoir les conséquences à long terme[115].

---

[108] Macenaite & Kosta, « Consent for processing children's personal data in the EU », *supra* note 98 aux pp 146-147.
[109] Commission d'accès à l'information du Québec, *supra* note 12 à la p 29.
[110] Ministère de la Sécurité publique du Québec (MSP), *supra* note 13.
[111] Agencia española de protección de datos, *supra* note 100 à la p 3.
[112] Voir notamment *At a crossroads: "Personhood" and digital identity in the information society*, by Bob Blakley et al, STI working paper series DSTI/DOC(2007)7, Organisation for Economic Cooperation and Development (OECD) Directorate for Science, Technology and Industry, 2008. On peut déduire de ce document que l'identité numérique possède un certain nombre de caractéristiques : 1. Social. Au fur et à mesure que l'individu se projette, les autres utilisateurs commencent à le reconnaître et à l'identifier, sans même vérifier si l'identité est réelle ou non. 2. subjective. Cela dépend de la perception que les autres ont de l'individu par l'information qu'il crée. 3. Valide. L'information peut générer un "capital informationnel". 4. Indirecte ou référentielle : L'identité numérique ne permet pas de connaître directement la personne, mais une référence à la personne ou à l'objet. 5. L'identité numérique se construit tant par les informations fournies par un individu en particulier que par les informations fournies par des tiers. 6. L'information sur l'identité numérique peut produire des effets positifs et négatifs dans le monde réel. 7. Dynamique: elle change et se modifie constamment. 8. Contextuel : selon le contexte dans lequel il est utilisé, l'effet peut être négatif ou non pertinent.
[113] Commission d'accès à l'information du Québec, *supra* note 12 à la p 30.; note 85 à la p 42.
[114] Commission d'accès à l'information du Québec, *supra* note 12 à la p 29.
[115] Rodota, *supra* note 87 à la p 51.

De leur côté, Livigstone et Haddon ont classé les opportunités et les risques que les mineurs peuvent rencontrer en ligne, en tenant compte de la manière dont les mineurs accèdent à Internet et l'utilisent. Selon ces auteurs, les relations des mineurs avec le réseau se développent à travers trois formes de communication : 1. de contenu : le mineur en tant que récepteur de contenus distribués massivement sur Internet, 2. de contact : le mineur en tant que participant dans une situation interactive généralement dirigée par un adulte et 3. de comportement : le mineur en tant qu'acteur dans une interaction où il peut être l'initiateur ou l'auteur[116].

De même, il est possible de déduire du classement, que selon la façon dont les mineurs communiquent sur le réseau, il y a quatre types de zones dans lesquelles les opportunités sont présentées: d'apprentissage, de compétences et de connaissances numériques; de participation et d'engagement social; de créativité et d'expression; d'identité et de connexion sociale. Par conséquent, il est possible de déterminer que les TIC et Internet apportent par eux-mêmes une quantité exorbitante d'opportunités pour le développement des mineurs dans tous les domaines où ils se déroulent, en permettant l'exercice d'un large éventail de droits, comme le droit à l'éducation, le droit à la liberté d'expression, à la liberté d'information et à la liberté d'association[117].

Or, cette classification met également en évidence les risques auxquels les mineurs sont confrontés dans l'exercice de leurs droits sur Internet, des situations qui peuvent généralement conduire à la violation d'un ou de plusieurs droits des mineurs[118]. Nous constatons la présence de risques dans quatre types de domaines qui pourraient affecter le développement et le bien-être de l'enfant : commerce, agression, sexualité et valeurs. Il est évident que certaines situations peuvent être classées dans plusieurs catégories[119].

[116] Voir notamment Sonia Livingstone & Leslie Haddon, « Introduction: kids online: opportunities and risks for children » dans Sonia Livingstone & Leslie Haddon, dir, *Kids Online Oppor Risks Child*, Bristol, UK, The Policy Press, 2009 1 aux pp 8-10.; Maialen Garmendia et al, « Los menores en internet. Usos y seguridad desde una perspectiva europea » (2012) 15:38 Quad CAC 37-44 à la p 38.; Lina Mariola Díaz cortés, « Menores e Internet: Entre las oportunidades y los riesgos. Un punto de partida para entender las políticas criminales » dans *Algunos Desafíos En Protección Datos Pers* D° Sociedad de la información 26, Comares, 2018 136 aux pp 141-142.
[117] Díaz cortés, *supra* note 116 à la p 143.
[118] *Ibid*.
[119]Livingstone & Haddon, *supra* note 116.,

Tableau II : Classification des risques selon Staksrud et Livingstone

Table 1: A classification of online risks for children			
RISKS	**Content: Child as recipient**	**Contact: child as participant**	**Conduct: child as actor**
Commercial	Advertising, spam, sponsorship	Tracking/ harvesting personal info	Gambling, illegal downloads, hacking
Aggressive	Violent/ gruesome/ hateful content	Being bullied, harassed or stalked	Bullying or harassing another
Sexual	Pornographic/ harmful sexual content	Meeting strangers, being groomed	Creating/ uploading pornographic material
Values	Racist, biased info/ advice (e.g., drugs)	Self-harm, unwelcome, persuasion	Providing advice (e.g., suicide/ pro-anorexia)

[120]

En outre, on peut déduire que non seulement les adultes peuvent tirer profit de l'utilisation de l'information privée du mineur, mais que celui-ci peut avoir à la fois le statut de victime et celui de délinquant. Cela signifie que, dans certaines circonstances, c'est le mineur qui commet le comportement atypique et anti-juridique, entraînant la violation des droits d'autres mineurs. C'est dans le même sens que le professeur David Oswell lorsqu'il indique ce qui suit :

> « There have been three main figures of childhood in Internet policy discourse: the child-as-victim, the child-in-danger and the dangerous child »[121]

Enfin, comme nous l'avons indiqué précédemment, bien que l'on ait voulu indiquer clairement que l'utilisation d'Internet offre des possibilités importantes pour le développement de l'enfant, aux fins du présent document, nous mettons l'accent sur les risques directement liés à la mauvaise gestion des données personnelles des mineurs, dont la violation est capable de porter atteinte à la vie privée, à l'intégrité physique et morale du mineur[122]. Compte tenu des classifications présentées, certains des risques auxquels sont confrontés les mineurs en raison de la violation de leurs données personnelles, par eux-mêmes ou par des tiers[123], sont la cyberintimidation, le leurre par Internet et le *sextage*.

[120] Tableau obtenu à partir de *Ibid* aux pp 9-10.; Elisabeth Staksrud & Sonia Livingstone, « Children and online risk: Powerless victims or resourceful participants? » (2009) 12:3 Inf Commun Soc 364-387 à la p 367.

[121] David Oswell, « The Place of 'Childhood' in Internet Content Regulation: A Case Study of Policy in the UK » (1998) 1:2 Int J Cult Stud 271-291 à la p 278.

[122] Darcy Hango, « La cyberintimidation et le cyberharcèlement chez les utilisateurs d'Internet âgés de 15 à 29 ans au Canada » (2016) 75-006-X Stat Can (Regards sur la societé canadienne) 20 à la p 2.

[123] Agencia española de protección de datos, *supra* note 100 à la p 4.

Chapitre 2 – Les dangers potentiels perçus: certaines formes d'infractions qui portent préjudices à la vie privée et à l'intégrité des mineurs

2.1. Cyberintimidation

La « cyberintimidation », le « cyberharcèlement », le « cyberbullying » (mot en anglais), l'« intimidation électronique », l'« intimidation en ligne » et le « harcèlement en ligne »[124] ou comme les appellent les plus jeunes « haïr », « drame », « potins » ou « trollage »[125], se réfèrent en termes généraux à une forme de harcèlement et d'agression qui se produit entre pairs, afin de menacer le destinataire, en faisant usage d'Internet ou de tout moyen technologique.

Il convient de noter que, bien que certains de ces comportements diffèrent quant à leur mode de perpétration, les documents que nous avons analysés utilisent ces termes de manière interchangeable[126]. Par conséquent, aux fins de ce travail, nous utiliserons indifféremment les expressions indiquées au début de cette section, pour nous référer aux comportements de harcèlement ou d'intimidation par voie électronique entre mineurs.

Cependant, dans le rapport « *ensemble contre l´intimidation* » du Comité d'experts sur la cyberintimidation au Québec (2015), les auteurs affirment que la cyberintimidation est aussi appelée « cyberharcèlement » lorsque les actions sont répétées ou « cyberagression » en cas d'incident unique[127]. Il importe de souligner qu'il n'existe pas de définition universelle de la cyberintimidation[128], et comme l'a exprimé le Comité sénatorial permanent des droits de la personne, il est difficile de cerner ce concept[129].

---

[124] *La sécurité des enfants en ligne : Défis et stratégies mondiaux*, par Le centre de recherche Innocenti (CRI), Innocenti Insights D, Italie, UNICEF, 2012 à la p 2. En ligne : <https://www.unicef-irc.org/publications/pdf/ict_fre.pdf>.
[125] Sécurité publique Canada, « Qu'est-ce que la cyberintimidation? », (21 décembre 2018), en ligne: <https://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/cbrbllng/prnts/cbrbllng-fr.aspx#ftn1>.
[126] Le centre de recherche Innocenti (CRI), *supra* note 124 à la p 2.
[127] Gouvernement du Québec*, Ensemble contre l´intimidation! : Rapport du Comité d'experts sur la cyberintimidation*, Québec, 2015 à la p 6. En ligne : <http://www.cps02.org/media/rapport-com-experts-cyberintimidation.pdf>.
[128] Ministère de la Justice du Canada*, Cyberintimidation et distribution non consensuelle d'images intimes: Rapport aux ministres fédéraux/provinciaux/territoriaux responsables de la Justice et de la Sécurité publique,* Groupe de travail sur la cybercriminalité du Comité de coordination des hauts fonctionnaires, 2013 à la p 4.
[129] note 70 à la p 10.

Le *Centre canadien de protection de l'enfance* du Canada (ci-après « CCPE ») décrit la cyberintimidation « comme étant une forme d'intimidation extrême entre jeunes dans l'espace numérique. Il s'agit d'un comportement abusif, ciblé, délibéré et répétitif destiné à causer du tort à une autre jeune personne »[130]. De son côté, *Sécurité Publique Canada* indique que la cyberintimidation, « se produit lorsqu'un enfant ou un adolescent devient la cible des agissements d'autres personnes, au moyen d'ordinateurs, de téléphones cellulaires ou d'autres appareils et le but est de l'embarrasser, de l'humilier, de le tourmenter, de le menacer ou de le harceler[131]». Dans l'Union européenne, seuls 14 pays membres[132], dont la France[133] , la République fédérale d'Allemagne[134] et l'Espagne[135] ont développé à travers différentes entités une définition officielle de cyberbullying, et chacune diffère de l'autre selon le contexte de chaque pays.

En somme, bien que ces définitions ne soient pas identiques, nous trouvons des éléments communs qui nous permettent d'identifier les principales caractéristiques de la cyberintimidation[136]: a) se développe entre pairs : le harceleur (Cyberbullies) et la victime n'ont pas atteints l'âge de la majorité [137], et il n'y a pas de différence d'âge marquée entre eux; b) comportement récurrent : il s'agit de comportements qui se répètent au fil du temps [138]. Toutefois, dans certains cas, même si le comportement d'intimidation n'est exécuté qu'une seule fois (par exemple, le partage d'une vidéo diffamatoire sur les réseaux sociaux), « l'acte préjudiciable se répète automatiquement chaque fois qu'une personne accède au contenu ou encore décide de le

[130] Centre canadien de protection de l'enfance [CCPE], *supra* note 6.
[131] Voir notamment Sécurité publique Canada, *supra* note 125.
[132] Autriche, Bulgarie, Chypre, République tchèque, Finlande, France, République fédérale d'Allemagne, Hongrie, Irlande, Italie, Luxembourg, Malte, Pays-Bas et Espagne.
[133] La France définit le cyberharcèlement comme « un acte agressif, intentionnel, perpétré par un individu ou un groupe d'individus au moyen de formes de communication électroniques, de façon répétée, à l'encontre d'une victime qui ne peut facilement se défendre seule ».
[134] Pour sa part, la RFA utilise le terme « Cyber-mobbing » et le définit comme « l'insulte, la menace, l'exposition ou le harcèlement des personnes qui utilisent les médias de communication, comme les téléphones intelligents, les courriels, les sites Web, les forums, les chats et les communautés ».
[135] Agencia española de protección de datos, *supra* note 100 à la p 5. «Le cyberharcèlement est une situation de harcèlement, insultes, brimades, y compris le chantage d'un mineur à l'autre via les médias des services web 2.0 tels que blogues, courrier, messagerie instantanée, réseaux sociaux, la messagerie de texte par téléphone ou appareil mobile ou la publication de vidéos et de photographies sur des plateformes électroniques de diffusion de contenus» [notre traduction].
[136] Ministère de la Sécurité publique du Québec (MSP), *supra* note 13 aux pp 4-5.
[137] Ángel Acedo Penco & Alejandro Platero Alcón, « The Privacy of Children and Adolescents in Social Networks: Special Reference to the European and Spanish Regulatory Regime, with some Considerations on the Chilean » (2016) 5:2 Rev Chil Derecho Tecnol 63-94 à la p 83.
[138] Damiano Menin et al, « Was that (cyber)bullying? Investigating the operational definitions of bullying and cyberbullying from adolescents' perspective » (2021) 21:2 Int J Clin Health Psychol 100221 à la p 3.

partager à son tour »[139]; c) dommages intentionnels : en règle générale, l'harceleur prémédite l'acte, mais dans certains cas, le mineur agit sans intention malveillante[140], (comme, lorsqu'il pense que ce qu'il a dit sur Facebook n'est qu'une blague); d) déséquilibre de pouvoir : l'harceleur exerce d'une certaine manière un pouvoir sur la victime; e) incapacité de se défendre : le harcèlement engendre chez le mineur (victime), une affection psychologique qui le rend sans défense et; f) le comportement est exécuté en utilisant des moyens technologiques (téléphones cellulaires, ordinateurs, tables, consoles, etc.) ou des moyens techniques (en utilisant différentes applications comme les réseaux sociaux, blogues, forums, messages texte, courriels, sites web, messagerie instantanée, salles de chat, jeux en ligne, photos, vidéos).

Comme nous pouvons le constater, le cyber-harcèlement est un comportement qui, comparé au harcèlement traditionnel, peut avoir une impact plus important sur la vie du cyberharcelé[141], car le harcèlement en ligne permet à l'agresseur d'accéder à la victime à tout moment (24 /7)[142] et en tout lieu (donne au harceleur un sentiment de pouvoir sur la victime) et lui donne également la possibilité de rester anonyme, en gardant son identité secrète ou en la falsifiant (augmente la croyance que l'acte n'aura aucune répercussion[143])[144]. En outre, étant donné le caractère mondial d'Internet, le cyber-harcèlement peut prendre un caractère massif et devenir viral [145] en raison de la distribution et de la réplication rapides des messages[146].

Selon l'UNESCO, « [l]e cyberharcèlement touche jusqu'à un enfant sur dix »[147]. Au Canada, un jeune sur cinq âgé entre 15 et 20 ans a indiqué avoir été victime de cyberintimidation, conformément au rapport présenté par l'UNICEF et *Une Jeunesse*[148]. En ce qui concerne les chiffres d'une étude réalisée sur 5 700 adolescents aux États-Unis, 33,8% des jeunes ont souffert

[139] note 70 à la p 27.
[140] note 127 à la p 13.
[141] note 70 aux pp 19-26.
[142] note 127 à la p 8; Le centre de recherche Innocenti (CRI), *supra* note 124 à la p 3.
[143] Sammer Hinduja & Justin W Patchin, *Cyberbullying Fact Sheet: Identification, Prevention, and Response* , Cyberbullying Research Center, 2019 à la p 4.
[144] note 70 aux pp 24-26; note 127 à la p 8.
[145] Hinduja & Patchin, *supra* note 143 à la p 3.
[146] note 127 à la p 12.
[147] UNESCO, *Au-delà des chiffres: en finir avec la violence et le harcèlement à l'école*, n. ED/477/0000368997, Paris, UNESCO, 2019 à la p 7.
[148] *Quelle est la situation au Canada? : L'indice canadien du bien-être chez les enfants et les jeunes*, by UNE JEUNESSE, UNICEF Canada, 2019 à la p 49.

de cyberintimidation au cours de leur vie [149]. Un autre document révèle qu'en avril 2019, plus d'un tiers des élèves du secondaire aux États-Unis avait déjà été victimes de harcèlement en ligne[150]. En outre, *Forbes France* montre que « 54 % des ados affirment avoir fait l'objet de moqueries en ligne et 42 % ont déjà été harcelés moralement[151] ».

Un autre thème commun à prendre en compte et qui se dégage des documents analysés, relativement à l'utilisation de données à caractère personnel, est le fait que ce comportement peut se présenter sous différentes formes, notamment [152] :

- Manipulation : le mineur est menacé, victime de chantage et/ou contraint de divulguer sans son consentement des informations personnelles susceptibles de lui nuire (divulgation de secrets ou d'informations embarrassantes), notamment dans le dessein d'un avantage, de causer des dommages ou l'exclusion. L'AEPD a expliqué que « en particulier, il s'agit de données sensibles, comme l'idéologie, la religion, les croyances, l'origine ethnique, la santé, la vie et l'orientation sexuelle[153] »; de même, lorsque des informations sur le mineur sont divulguées, qu'elles soient vraies ou non, afin de lui attribuer la commission d'un délit (calomnie) ou de tout acte portant atteinte à sa dignité ou à son honneur.
- Usurpation d'identité : se présente lorsque le cyber-harceleur crée un profil au nom de la victime ou vole les clés d'accès à ses profils de réseaux sociaux, courriels, jeux en ligne, applications web, et en utilisant le profil numérique de la victime, envoie ou publie du contenu inapproprié ou honteux sur la victime ou sur d'autres personnes pour la blesser, se moquer (par exemple télécharger des photos, des commentaires et/ou des vidéos qui nuisent à la réputation, ou pour se moquer) ou même publier des informations pour que la victime soit localisée par d'autres personnes ou encore fournir des services sexuels au nom de la victime.

---

[149] Hinduja & Patchin, *supra* note 143 à la p 3; *Primer informe global sobre cyberbullying*, por Wezum, observatorio joven, Fundación Pontificia Scholas Occurrentes, 2019 à la p 16.
[150] J Clement, *Cyber bullying - Statistics & Facts* , Statista, 2019.
[151] Forbes France, « Cyberharcèlement : Comment Lutter Efficacement Contre Ce Fléau Digital ? », *Forbes Fr* (23 octobre 2019), en ligne: <https://www.forbes.fr/technologie/cyberharcelement-comment-lutter-efficacement-contre-ce-fleau-digital/>.
[152] *Protocolo de actuación escolar ante el ciberbullying*, by R Del Rey et al, Google Scholar, Bilbao, Equipo multidisciplinario de investigación sobre ciberbullying [EMICI], 2011 à la p 15; UNICEF Argentina, *¿Qué es el ciberbullying?* , UNICEF Argentina à la p 2; Robin M Kowalski, *Cyber bullying: bullying in the digital age*, Malden, MA., Blackwell Pub, Blackwell, 2008 aux pp 46-51; x-Rouge canadienne, « La cyberintimidation », en ligne: *Croix-Rouge Can* <http://www.croixrouge.ca/nos-champs-d-action/prevention-de-la-violence-et-de-l-intimidation/educateurs/prevention-de-l-intimidation-et-du-harcelement/la-cyberintimidation>.
[153] AEPD, *Guía de protección de datos para la prevención de delitos*, AEPD, 2018 aux pp 3-14.

- Harcèlement : quand, par quelque moyen technique que ce soit, le mineur harceleur parvient à accéder aux coordonnées d'un autre mineur, comme son courrier électronique, son numéro de portable, ses profils de réseaux sociaux, afin de le harceler, l'humilier, le menacer; ou dans le cas où la victime serait une femme, exercer une violence de genre**.**
- Cybertraquage : lorsque, sur la base de différentes représentations en ligne, par l'envoi constant de messages abusifs ou intimidants, le mineur craint pour sa sécurité.
- Exclusion : les informations personnelles du mineur sont utilisées pour exclure le mineur ou le placer dans des groupes ou forums. De même, lorsque des images dégradantes, des vidéos ou des messages sont utilisés pour harceler les enfants.

En résumé, la cyberintimidation suppose « l'utilisation et la diffusion d'informations blessantes ou diffamatoires (…) »[154] [notre traduction], présuppose la violation de la vie privée et la protection des données personnelles des mineurs dès le moment où leurs informations sont utilisées sans consentement. Lorsque cela constitue non seulement une violation de la réglementation relative à la protection des données personnelles, le mineur peut commettre une ou plusieurs infractions, sans souvent être conscient des conséquences ou de la gravité de ses actes.

Or, la cyberintimidation n'est mentionnée dans aucune des lois sur la vie privée et sur la protection des données, ce qui implique clairement qu'il faut chercher à encadrer le comportement dans la violation de l'une quelconque des dispositions de ces lois, comme c'est le cas en matière civile et criminelle. Toutefois, le RGPD de l'UE a introduit en faveur des mineurs un « droit à l'oubli » à l'article 17 qui leur permet de demander la suppression de leurs données personnelles. Le droit à l'oublie se présente comme un outil important pour la protection des données des mineurs, en particulier lorsque le harcèlement en ligne est présenté par l'utilisation de données personnelles qui ont été publiées ou collectées par voie électronique sans avoir obtenu le consentement nécessaire. Nous reviendrons sur ce sujet ultérieurement dans notre travail.

En conclusion, il est clair que la cyberintimidation a des conséquences sur la vie privée de la victime mineure que peuvent être dévastatrices, comme dans le cas d'Amanda Michelle Todd, de

[154] España, Ministerio de Industria, Energía y Turismo*, Guía de actuación contra el ciberacoso*, Instituto Nacional de tecnologías de la comunicación [INTECO], 2014 à la p 3. En ligne: < http://www.injuve.es/convivencia-y-salud/guia-de-actuacion-contra-el-ciberacoso>.

Port Coquitlam en Colombie-britannique, qui a été convaincue par un inconnu dans une salle de chat de montrer sa poitrine sur webcam. Un an plus tard, après une période de chantage, l'individu a partagé avec ses amis, une photo d'elle nue. Amanda Todd a souffert de harcèlement et de cyberintimidation pendant trois ans, principalement à cause d'une mauvaise gestion des données personnelles, mais aussi en raison d'une protection juridique insuffisante sur le sujet[155].

Par conséquent, il est nécessaire que les gouvernements mettent en place des mesures, telles que des programmes visant à sensibiliser et à éduquer tous les acteurs concernés, y compris les parents, les jeunes, le personnel scolaire et les fournisseurs de services Internet pour prévenir et éradiquer le problème. Le législateur au niveau mondial a pour défi fondamental de réglementer concrètement la cyberintimidation et de jeter les bases de la protection des droits des victimes et de leur exercice. De même, ils doivent élaborer des politiques et des instruments juridiques prévoyant des procédures claires et des mesures préventives pour permettre aux acteurs de détecter, de surveiller et de signaler efficacement les incidents de cyberintimidation.

Pour atteindre cet objectif, il est vraiment important que le Canada, les États-Unis et l'Union européenne adoptent au niveau national une définition officielle de la cyberintimidation, incluant les éléments essentiels du comportement : répétition, dommage, intention et différence de pouvoir.

2.2. Leurre par Internet

Cette conduite est connue sous divers vocables en anglais, « cybergrooming », « Child grooming » ou « grooming en ligne », au Canada comme « leurre » (luring en anglais) ou « le conditionnement[156] », ou sous le nom de « sollicitation des enfants ou manipulation en ligne »[157] en France. Le grooming tout comme le cyberbullying se présente comme un acte de harcèlement et de chantage. Cependant, lorsque nous parlons de cybergrooming, nous nous trouvons dans une

[155] Denyse Perreault, « La cyberintimidation : "please, no hate" » (2016) 13:4 Perspect Infirm 21-24; « Suicide d'Amanda Todd » dans *Wikipédia*; Emily lazatin, « Appeal case to begin in Netherlands for Amanda Todd's alleged tormentor », *Glob News* (22 octobre 2018), en ligne: <https://globalnews.ca/news/4581300/amanda-todd-dutch-accused-criminal-appeal/>; « L'homme qui a cyberintimidé Amanda Todd condamné à 11 ans de prison au Pays-Bas », (16 mars 2017), en ligne: <https://www.lapresse.ca/actualites/201703/16/01-5079235-lhomme-qui-a-cyberintimide-amanda-todd-condamne-a-11-ans-de-prison-au-pays-bas.php>.

[156] Centrale canadienne de signalement des cas d'exploitation sexuelle d'enfants sur Internet (Cyberaide), *supra* note 7.

[157] Le centre de recherche Innocenti (CRI), *supra* note 124 à la p 30.

situation où les parties des deux extrêmes ne sont plus des mineurs, mais un adulte (agresseur) qui se fait passer pour un mineur afin d'atteindre sa victime (un mineur) et d'en obtenir des avantages de nature sexuelle[158].

Le grooming est l'un des risques auxquels sont exposés les mineurs en ligne en raison de l'utilisation et de la surexposition inadéquates de leurs données personnelles. L'agresseur, par l'utilisation d'Internet et des téléphones mobiles, entre en contact avec des mineurs notamment par messages texte (SMS), message multimédia (MMS), réseaux sociaux, salles de chat, forums, programmes de messagerie instantanée, groupes de discussion, jeux en ligne[159], par lesquels il peut obtenir des informations personnelles du mineur, comme son âge, sexe, adresse de la maison, lieu d'études, amis, goûts, idées, membres de la famille, courriel, habitudes et hobbies ou toute autre donnée qui permet d'entamer une sorte de conversation sur le réseau social ou même dans le monde physique[160]. Une fois ces informations obtenues, les délinquants les exploitent pour commettre des infractions sexuelles avec des mineurs.

La CCPE du Canada a signalé que :

> « Le leurre par Internet est une infraction commise par une personne (souvent adulte, mais pas nécessairement) qui utilise un moyen technologique (texto, messagerie instantanée, courriel, etc.) pour communiquer avec une jeune personne afin de commettre plus facilement une infraction sexuelle contre cette jeune personne. Par exemple, une personne commettrait une infraction de leurre par Internet si, dans une communication avec une jeune personne, elle lui demandait, lui suggérait ou essayait de la convaincre de produire ou de transmettre des photos ou des vidéos intimes où elle se montre nue ou à demi vêtue[161] ».

Dans le domaine international, *la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels* [162], connus sous le nom de « *la Convention de*

---

[158] UIT, *Directives pour la protection de l'enfance en ligne, destinées aux enfants* , UIT, 2009 à la p 51; Centre Canadien de Protection de L'enfance [CCPE], *Fiche de prévention sur le leurre* , Centre canadien de protection de l'enfance inc, 2017; UNICEF Argentina & Ministerio de justicia y derechos humanos, *Grooming: Guía práctica para adultos: Información y consejos para entender y prevenir el acoso a través de Internet* , 2014 à la p 2.
[159]Voir notamment UIT, *supra* note 158 à la p 51; note 154 à la p 22.
[160] Sergio Hernandéz Ramírez, *La protección de datos personales de menores en redes sociales: desafíos y recomendaciones* Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación [INFOTEC], 2018) [unpublished] à la p 2.
[161] Centre Canadien de Protection de L'enfance [CCPE], *supra* note 158.
[162]*Convention du Conseil de l'Europe: La protection des enfants contre l'exploitation et les abus sexuels (Convention de Lanzarote)*, 2007, STCE 201. La Convention de Lanzarote, impose la criminalisation de tous les types d'infractions à caractère sexuel perpétrées contre des enfants.

Lanzarote »[163] est le premier instrument juridique international définissant le grooming, et exige des États parties prenantes qu'en vertu de l'art. 23 appelé « sollicitations d'enfants à des fins sexuelles », criminalisent « la proposition intentionnelle, par le biais des technologies de l'information et de la communication, d'un adulte de rencontrer un enfant « dans le but de commettre à son insu une infraction établie conformément aux articles 18, paragraphe 1.a, ou 20, paragraphe 1.a, lorsque cette proposition a été suivie d'actes matériels conduisant à ladite rencontre » [164].

Au niveau communautaire, nous trouvons la *directive 2011/93-UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil*[165]. Les deux documents conviennent que pour que le comportement soit punissable, il faut que l'adulte ait l'intention de rencontrer le mineur en dehors du réseau, qu'une proposition soit faite pour se rencontrer personnellement et que cette proposition soit suivie d'actes matériels pouvant conduire à la rencontre.

Au Canada, ce comportement est réprimé depuis 2002 par l'article 172.1 du Code criminel[166] sous le titre « *leurre* » ou en anglais comme "*Luring a child*" et sanctionne l'utilisation de tout moyen de communication en vue de commettre d'autres délits d'ordre sexuel contre un mineur de 18, 16 ou 14 ans. Il est important de noter que cet article a fait l'objet d'une décision de la Cour suprême du Canada dans l'affaire *R. c. Morrison, 2019 CSC 15*[167]. L'arrêt précité entraîne

[163] Ce document est entré en vigueur le 1er juillet 2010 et a été ratifié à ce jour par 45 États membres et un État non membre : Tunisie. Il a également été signé, mais non ratifié par l'Arménie et l'Irlande.
[164] *Convention de Lanzarote*, *supra* note 162, art 23.
[165] L'article 6(1) indique : « Sollicitation d'enfants à des fins sexuelles : … les comportements intentionnels suivants soient punissables: le fait pour un adulte de proposer, au moyen des technologies de l'information et de la communication, une rencontre à un enfant qui n'a pas atteint la majorité sexuelle, … lorsque cette proposition a été suivie d'actes matériels conduisant à ladite rencontre, est passible d'une peine maximale d'au moins un an d'emprisonnement ».
[166] *Code criminel*, LRC 1985, c C-46, art 172.1. Cet article établit : « (1) Commet une infraction quiconque communique par un moyen de télécommunication avec : a) une personne âgée de moins de dix-huit ans ou qu'il croit telle, en vue de faciliter la perpétration …; b) une personne âgée de moins de seize ans ou qu'il croit telle, en vue de faciliter la perpétration …; c) une personne âgée de moins de quatorze ans ou qu'il croit telle, en vue de faciliter la perpétration […] ».
[167] *R.c Morrison*, [2019] CSC 15 . L'accusé a été condamné en première instance à quatre mois d'emprisonnement pour le délit de leurre d'enfant, pour avoir eu pendant deux mois des conversations sexuelles en ligne avec « Mia » une fille de 14 ans. Le profil de « Mia » a été créé par la police après avoir trouvé une annonce mise en ligne sur Craigslist par M. Morrison, intitulée en anglais « Papa recherche sa petite fille », dans laquelle il affirmait qu'il était

une certaine insécurité juridique dans la protection des mineurs qui font l'objet de ces comportements. La Cour a sans aucun doute durci le délit de leurre d'enfants, mais en faveur de l'accusé, en transférant la charge de la preuve à la Couronne, en lui demandant de prouver que le coupable savait vraiment l'âge de sa victime, et de ce fait, il est presque impossible qu'une personne soit reconnue coupable de ce comportement et, par conséquent, les progrès législatifs en la matière sont nettement en recul.

Pour sa part, le ministère de la justice des États-Unis, dans un rapport présenté au Congrès[168], développe le concept de « *online enticement of children* » pour se référer au grooming en ligne et le décrit comme suit :

> « Child predators often use the internet to identify, and then coerce, their victims to engage in illegal sex acts. These criminals will lurk in chat rooms or on bulletin board websites that are popular with children and teenagers. They will gain the child's confidence and trust, and will then direct the conversation to sexual topics. Sometimes they send the child sexually explicit images of themselves, or they may request that the child send them pornographic images of themselves. Often, the defendants plan a face-to-face for the purpose of engaging in sex acts »[169].

Selon les définitions proposées, on peut conclure que le grooming se présente lorsqu'un adulte (groomer ou harceleur) de manière délibérée et abusive, en utilisant tout moyen de communication, entre en contact avec un mineur dans le but de le maltraiter ou de l'exploiter sexuellement. Habituellement, l'adulte pour établir une relation d'amitié avec le mineur, parfois en se faisant passer pour un autre mineur, dissimule son identité à travers de l'usage d'un pseudonyme ou de faux profils sur Internet, et en utilisant les informations personnelles qu'il a obtenues de l'enfant, gagne facilement sa confiance et obtient ensuite le contrôle émotionnel de sa victime pour obtenir des avantages sexuels[170]. Cette technique de manipulation psychologique[171] est généralement connue comme technique de « Séduction » ou de flatterie [172].

---

intéressé par les jeunes femmes pour avoir des conversations sexuelles. La Cour suprême du Canada a déclaré inconstitutionnelle la présomption légale énoncée à l'article 172.1(3) du Code pénal pour violation du principe de présomption d'innocence consacré à l'article 11 (d) de la Charte canadienne des droits et libertés.

[168] É-U, US Department of Justice, *The national strategy for child explotation prevention and interdiction: a report to Congress*, 2010.

[169] *Ibid* à la p. 3.

[170] Garmendia et al, *supra* note 116, à la p. 41.

[171] UIT, *supra* note 158, à la p. 51.

[172] Le centre de recherche Innocenti (CRI), *supra* note 124, à la p. 2.

Une fois qu'il a gagné la confiance, l'harceleur en utilisant la persuasion[173] obtient que le mineur lui révèle des renseignements à caractère personnel (des secrets intimes, des photos ou des vidéos compromettantes, avec du contenu sexuel et/ou érotique) de lui-même ou de ses amis[174]. Lorsque l'agresseur obtient ce qu'il demande, il commence à faire chanter le mineur et à le menacer de rendre public le matériel et de l'envoyer à ses parents, amis et connaissances si le mineur n'envoie pas plus de vidéos, photos, ou refuse de s'engager dans des activités sexuelles ou des rencontres personnelles.

Toutefois, il est important de noter que l'abus sans contact peut façonner le comportement de leurre, étant donné que les actes sexuels, l'abus sexuel et l'exploitation sexuelle peuvent être présentés en ligne sans que le délinquant ait l'intention de rencontrer et de connaître personnellement le mineur[175][176]. À titre d'exemple[177], on peut citer la législation du Canada[178], de la France[179], des États-Unis [180] et du Royaume-Uni[181], qui prennent comme aspect principal la communication avec le mineur dans l'intention d'obtenir un avantage sexuel, et ne nécessitent pas que le groomer ait l'intention de connaître sa victime. Naturellement, le « grooming » en ligne non seulement affecte psychologiquement le mineur et viole clairement ses données personnelles, mais en règle générale, il « est le préambule à la violence sexuelle à l'égard des mineurs et donc le résultat d'activités illicites plus graves telles que la pédophilie, la pédopornographie[182] », la traite des êtres humains et l'homicide.

---

[173] *Keeping Kids Safe: How Child Sexual Predators Groom Children*, by Kylie Rymanowicz, États-Unis, Michigan State University Extension (MSU), 2020 à la p. 4.
[174] UIT, *supra* note 158, à la p. 51.
[175] International centre for missing & exploited children (ICMEC), *Online grooming of children for sexual purposes: Model legislation & global review*, 1e éd, États-Unis, The Koons Family Institute on International Law & Policy, 2017 à la p 6.
[176] *Avis sur l'article 23 de la Convention de Lanzarote et sa note explicative*, Adopté 17 Juin 2015.
[177] International centre for missing & exploited children (ICMEC), *supra* note 175 à la p 8,42-60. Ce document conclut que des 196 pays étudiés, 63 ont une législation sur le grooming en ligne, dont 51 définissent ou décrivent le comportement, et seulement 34 pénalisent le grooming sur Internet sans tenir compte de l'intention de rencontrer personnellement le mineur.
[178] *Code criminel*, *supra* note 166, art 172 (1).
[179] arts 227-22-1 C pén. Cette législation s'applique aux infractions commises contre une personne âgée de moins de 15 ans. (France).
[180] *Crimes and criminal procedure*, 18 USC, part I ch 115 § 2422(b) (1940). Cette législation s'applique aux infractions commises contre une personne âgée de moins de 18 ans.
[181] *Sexual Offences Act 2003*, (R-U), 2003 Ch. 42, arts 14 and 15. Cette législation s'applique aux infractions commises contre une personne âgée de moins de 16 ans.
[182] Hernandéz Ramírez, *supra* note 160 à la p 14.

Ce phénomène, qui touche à bien des égards les mineurs, s'est développé rapidement ces dernières années, comme le confirment les données rapportées sur les cybercrimes par certains des services de police du Canada, révélant 850 cas en 2015 directement liés au leurre d'un enfant au moyen d'un ordinateur, contre 1 132 en 2017 et 1 450 en 2019[183]. Au sein du territoire européen, les chiffres publiés par le Département de l'éducation en Angleterre ont identifié plus de 18 700 victimes présumées d'exploitation sexuelle d'enfants entre 2018 et 2019[184]; à cause de cela, certains médias ont déclaré le « grooming » comme une épidémie.

Il est donc clair que le « grooming » en ligne a augmenté au fil des ans et c'est un comportement qui n'est possible que par la quantité exorbitante de données personnelles d'enfants que l'on peut trouver sur le réseau. Toutefois, en ce qui concerne les normes de protection des données relatives aux mineurs, on ne trouve pas encore une norme spécifique qui sanctionne l'utilisation de données sur les mineurs dans le but d'obtenir un quelconque avantage sexuel.

En bref, le leurre en ligne a un impact important sur les mineurs victimes de cet acte, sur le noyau familial et sur la société. Il est donc nécessaire que les pays s'unissent pour élaborer des concepts unifiés en la matière, comme une définition unique, la fixation de l'âge minimal de l'assujetti au délit (indépendamment de l'âge du consentement ou d'autres infractions à caractère sexuel) et pour prévoir des peines minimales et aggravantes[185]. De même, il faut édicter des règles qui protègent les données des mineurs et sanctionnent leur utilisation lorsqu'elles ont pour but de commettre tout type de comportement délictueux à l'encontre d'un mineur.

---

[183] Statistique Canada, *Tableau : 35-10-0001-01: Cybercrimes déclarés par la police, selon l'infraction reliée à la cybercriminalité (certains services de police), Canada* , 2020. En ligne : <https://doi.org/10.25318/3510000101-fra>

[184] Lizzie Dearden, « 'Radical rethink' on grooming gangs needed after 19,000 children sexually exploited in year », *The Independent* (30 décembre 2019), en ligne: <https://www.independent.co.uk/news/uk/crime/grooming-gangs-child-sex-abuse-victims-rotherham-rochdale-latest-a9264656.html>; Mail on sunday report, « Nearly 19,000 children in England are exploited in a year », *Dly Mail Online* (28 décembre 2019), en ligne: <https://www.dailymail.co.uk/news/article-7833493/Nearly-19-000-children-sexually-groomed-England-past-year.html>.

[185] International centre for missing & exploited children (ICMEC), *supra* note 175 à la p 61.

2.3. Le Sextage

Cette conduite est également connue au Canada sous le nom de « autoexploitation juvénile », « Partage non consensuel d'images intimes »[186] ou « sexting » en anglais. Au Québec, le sextage est aussi connu comme « autoportraits érotiques » ou « sexfies »[187]; pour leur part, les Français l'appellent « textopornographie »[188]. Dans certains pays comme l'Espagne, le terme « sex-casting » est utilisé pour désigner l'enregistrement de vidéos à contenu sexuel via la webcam et leur diffusion par tout moyen électronique et Internet[189].

Le sextage entre mineurs s'entend par la création, l'envoi ou la réception de messages à caractère sexuel (également connu sous le nom de sextos) au moyen d'Internet ou d'autres dispositifs électroniques[190] tels que les réseaux sociaux, les téléphones mobiles, les courriels, les applications, webcam. Ce comportement comprend des photos et des vidéos sexuellement explicites [191] (photos ou vidéos montrant nu ou semi-nu, soit l'auteur, soit une troisième personne); messages textes ou des publications écrites en langage sexuel[192]; sessions de chat en direct où une personne capture des images d'actes sexuels par webcam; et/ou captures d'écran de photos ou de vidéos enregistrées par une webcam[193].

Le sextage, comme la cyberintimidation et le grooming sur Internet, a augmenté rapidement. Selon une étude réalisée en 2018 par l'Université de Calgary auprès de plus de 110,000 adolescents, « un adolescent sur sept rapporte qu'il envoie des sextos et qu'un sur quatre reçoit des

---

[186] Ministère de la Sécurité publique du Québec [MSP], « Sextos- Échanger des photos intimes n'est pas un jeu d'enfants! », en ligne : <https://www.securitepublique.gouv.qc.ca/police/prevention-criminalite/semaine-de-la-prevention-de-la-criminalite/sextos.html> (consulté le 10 janvier 2020).

[187] Lise Poupart, La cyberviolence dans les relations amoureuses des jeunes: Guide pour les parents, Association québécoise Plaidoyer-Victimes, 2019 à la p 17, en ligne : <https://aqpv.ca/la-cyberviolence-dans-les-relations-amoureuses-des-jeunes/> (consulté le 11 janvier 2020).

[188] Préposé fédéral à la protection des données [PFPDT] et plateforme nationale de promotion des compétences [Jeunes et Médias], Protection des données: Dossier d'information à la p 21.

[189] INTECO et PantallasAmigas, Guía sobre adolescencia y sexting: qué es y cómo prevenirlo, février 2011 à la p 6.

[190] Ministère de la Justice du Canada, « Sextage : qu'est-ce que la loi permet? », (1 août 2018), en ligne: *Cliquez-Justice* <https://www.cliquezjustice.ca/vos-droits/sextage-qu-est-ce-que-la-loi-permet>.

[191] Cathy Tétreault, *En tant que... victime, auteur ou témoin. Guide d´accompagnement pour le personnel scolaire qui ouvre auprès des victimes, auteurs ou témoins de sextos, de sextorsion et de cyberagression sexuelle*, la collection de la chaire éd, Québec, 2019 à la p 7.

[192] Jeunesse, J´écoute, « Qu'est-ce que le sextage ? », en ligne: *jeunessejecoute.ca* <https://jeunessejecoute.ca/information/quest-ce-que-le-sextage/>.

[193] *Ibid*.

sextos »; en plus, 12 % des adolescents ont envoyé un sexto sans avoir le consentement nécessaire[194]. La CCPE a affirmé que plus de 750 signalements impliquant des jeunes touchés par la diffusion non consentie d'images intimes ou de sextage, ont été présentés au Canada après 2015, dont l'âge moyen a été de 16 ans. Au Québec, par exemple, un mineur sur cinq, pratique le sextage[195].

Aux États-Unis, les chiffres étaient déjà élevés en 2009. À cet égard, *INTECO* révèle que 65 % des filles et 35 % des garçons âgés de 13 à 16 ans ont déclaré avoir envoyé des sextos par courriel [196]. Dans une étude publiée en 2018 auprès de 6 021 élèves du secondaire en Pennsylvanie intitulée « *Teenagers, sexting and the Lawel* », le professeur Strasburger a remarqué que 29 % des mineurs étaient impliqués dans des sexting consensuels[197].

Il est essentiel de préciser que Sexter *per se* n'est pas un comportement illicite[198], au contraire il fait partie du développement sexuel et de la liberté d'expression des mineurs[199]. Or, une fois le sexto envoyé, le mineur perd le contrôle de cette donnée à caractère personnel, puisque si le message est téléchargé pour une raison quelconque dans le cyberespace, « leur propagation risque de devenir virale et sans limites »[200] et aussi, il deviendra difficile de supprimer l'information [201]. Dans certains cas, même si la personne qui reçoit le message n'a pas l'intention de le partager, il peut se produire des situations qui peuvent mettre ces renseignements personnels entre les mains de tiers. Par exemple, celui qui le reçoit peut perdre l'appareil sur lequel la photo, vidéo ou le message se trouve, la clé peut être volée ou un ami peut accéder à son appareil et sans consentement, s'approprier du message.

---

[194] Elizabeth Englander & Meghan McCoy, « Sexting—Prevalence, Age, Sex, and Outcomes » (2018) 172:4 JAMA Pediatr 317-318; Jeff Temple & Sheri Madigan, « One in seven teens are "sexting," says new research », en ligne: *The Conversation* <http://theconversation.com/one-in-seven-teens-are-sexting-says-new-research-92170>.

[195] Lise Poupart, *La cyberviolence dans les relations amoureuses des jeunes: Guide pour les parents*, Association québécoise Plaidoyer-Victimes, 2019 à la p 16.

[196] INTECO & Pantallas Amigas, *Guía sobre adolescencia y sexting: qué es y cómo prevenirlo* , 2011 à la p 4.

[197] Victor C Strasburger et al, « Teenagers, Sexting, and the Law » (2019) 143:5 Pediatrics, en ligne: <https://pediatrics.aappublications.org/content/143/5/e20183183> à la p 2.

[198] Préposé fédéral à la protection des données [PFPDT] & plateforme nationale de promotion des compétences [Jeunes et Médias], *Protection des données: Dossier d'information* à la p 21.

[199] Poupart, *supra* note 195 à la p 16.

[200] *Ibid* à la p 18.

[201] Préposé fédéral à la protection des données [PFPDT] & plateforme nationale de promotion des compétences [Jeunes et Médias], *supra* note 198 à la p 22.

Lorsque, en toute circonstance, nous constatons la diffusion non consentie d'images, de textes, de vidéos qui ont été reçues par le biais d'un sexto, à des fins privées et personnelles, le mineur peut être accusé d'actes de nature criminelle. Le sexting, outre qu'il porte gravement atteinte à la vie privée, à l'honneur, à l'image de l'enfant et au droit à la protection des données personnelles, peut aussi être accompagné de pratiques de cyberintimidation, cybergrooming, sextortion et pédopornographie[202], dont découlent d'autres responsabilités légales et qui bien sûr, provoquent chez le mineur, des dommages plus profonds au niveau psychologique qui peuvent le conduire au suicide.

Au Canada, le sextage est considéré comme un acte criminel[203], même s'il est commis entre deux mineurs[204] conformément à l'article 163.1 du Code criminel[205]. En ce sens, si un mineur a enregistré lui-même l'image (exemple « selfie ») ou la vidéo, et a donné son consentement pour la prise de la photo ou pour l'enregistrement de la vidéo à caractère sexuel[206], le mineur peut être accusé de production de pédopornographie. De son côté, le mineur qui montre ou partage les images et vidéos qu'il a reçues, peut être accusé de distribution de pornographie juvénile ou être en possession de pornographie juvénile[207] (si le mineur conserve ces données pour lui).

Dans ce cadre, il existe une exception présentée dans l'affaire *R. c. Sharpe*[208]*,* par la Cour suprême du Canada [CSC] en 2001, concernant « l'utilisation personnelle » dans le délit de pornographie juvénile par rapport au sextage entre deux mineurs. La CSC a décidé que les jeunes ont le droit de communiquer sexuellement par le biais du sextage [209] à condition que : les mineurs

---

[202] Silvia Barrera Ibañez, *XV. Investigación criminal de los delitos cometidos contra menores como usuarios de internet* , España, Thomson Reuters Aranzadi, 2013 à la p 417.

[203] Le sexting entre adultes de plus de 18 ans est légal lorsque chaque personne accepte volontairement de participer et qu'aucune image intime n'est partagée sans le consentement de la personne sur l'image ou sur la vidéo.

[204] Ministère de la Sécurité publique du Québec [MSP], « Sextos- Échanger des photos intimes n'est pas un jeu d'enfants! », en ligne: <https://www.securitepublique.gouv.qc.ca/police/prevention-criminalite/semaine-de-la-prevention-de-la-criminalite/sextos.html>.

[205] *Code criminel*, *supra* note 166, art 163.1.

[206] Tétreault, *supra* note 191 à la p 14,21; Jeunesse, J´écoute, « Sextage et consentement : Faits importants », en ligne: *jeunessejecoute.ca* <https://jeunessejecoute.ca/information/sextage-et-consentement-faits-importants/>. « Au Canada, l'âge de consentement aux activités sexuelles est de 16 ans. Également, il existe deux exceptions de proximité d'âge : les jeunes âgés de 12 et 13 ans peuvent avoir des relations sexuelles avec des personnes qui sont moins de 2 ans plus vielles qu'eux; et les jeunes âgés de 14 et 15 ans avec des personnes qui sont moins de 5 ans plus vielle qu'eux ».

[207]Commission scolaire des Draveurs, *Le sextage* , 2015; Ministère de la Sécurité publique du Québec [MSP], *supra* note 204; *Sexting: Considerations for Canadian Youth*, by The Sex Information and Education Council of Canada [SIECCAN], Sexualityandu.ca, 2011 à la p 2.

[208] *R c Sharpe*, [2001] 1 RCS 45 au para 116.

[209] note 128 à la p 20.

aient plus ou moins le même âge, l'image ou la vidéo ait été envoyée volontairement, ceux-ci ont donné leur consentement sans abus de pouvoir ou d'exploitation et leur utilisation est restée privée parmi ceux qui sont montrés sur l'image ou la vidéo (elle n'a pas été publiée ou partagée). Le mineur ne fera pas non plus l'objet d'une enquête s'il crée et conserve pour son usage privé un texte, une vidéo ou une image sexuelle ou intime de lui-même [210].

Aux États-Unis, il n'existe pas de loi fédérale régissant le sexting, de sorte que la législation et la manière de poursuivre les mineurs varient d'un État (State) à l'autre. À ce jour, seuls 25 États ont expressément réglementé le sextage chez les mineurs, en particulier chez les adolescents[211]. Ces lois sur le sexting interdisent généralement l'envoi d'images explicites, et aussi considérant que le mineur ne peut pas contrôler ou empêcher une autre personne de lui envoyer un sexto, pourtant, le délit dans cet événement se présentera si le sexto est « maintenu » en sa possession (dans certains États, le mineur peut prouver qu'il tente de supprimer le message)[212].

On trouve une exception dans la législation du Texas, qui prévoit que le sexting n'est pas pris en compte si les personnes impliquées sont deux mineurs qui n'ont pas plus de deux ans de différence et ont une relation amoureuse, ceci est connu comme la disposition « Roméo et Juliette »[213]. Une autre exception se présente dans la législation de l'État du Nebraska relative à la pornographie juvénile qui prévoit une « défense positive » selon laquelle le consentement explicite des deux mineurs concernés n'est pas sanctionné par le comportement de sexting.

En Europe, la *Convention de Lanzarote* du Conseil de l'Europe précitée prévoit que les États doivent prendre les mesures législatives appropriées pour ériger en infraction pénale le fait de produire intentionnellement de la pédopornographie (art. 20.1), mais rien n'est dit directement de la conduite de sexting. On peut toutefois citer comme exemple la législation espagnole, qui,

---

[210] Jeunesse, J'écoute, « Sextage : la vie privée et la loi », en ligne: *jeunessejecoute.ca* <https://jeunessejecoute.ca/information/sextage-la-vie-privee-et-la-loi/>.
[211] Sameer Hinduja & Justin W Patchin, « Sexting Laws Across America », en ligne: *Cyberbullying Res Cent* <https://cyberbullying.org/sexting-laws>; « U.S. states with state sexting laws 2019 », en ligne: *Statista* <https://www.statista.com/statistics/509314/us-states-with-state-sexting-laws-policy/>.
[212] Haley Zapal, « State-by-State Differences in Sexting Laws », (9 avril 2019), en ligne: *Bark* <https://www.bark.us/blog/state-by-state-differences-in-sexting-laws/>.
[213] Strasburger et al, *supra* note 197 à la p 5.

s’éloignant de la notion de pornographie juvénile, a inséré dans le code pénal l’article 197.7 par la loi organique 1/2015 du 30 mars.

Il est donc clair que les conséquences de la transmission de ce type d’informations personnelles affectent le détenteur des données, entraînent des conséquences sociales et psychologiques pour la victime et si nous ajoutons à cela que conformément à l’absence de lois spécifiques régissant le comportement lorsque les personnes impliquées sont mineures, ce mineur qui avait un désir d’explorer sa sexualité, pourrait finir par être accusé de production de pédopornographie.

En conclusion, il est jugé souhaitable de fixer une limite d’âge ainsi que les critères et la procédure de détermination du comportement, avec pour fin de légitimer le consentement donné exclusivement par le mineur pour le traitement de ce type de données à caractère personnel.

Partie II – Dispositions nationales et internationales

Titre 1 – Cadre légal canadien

Chapitre 1 – Sources juridiques au niveau fédéral

Section 1 – Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)

La vie privée en ligne et la protection de l'information au Canada sont régies par la *Loi sur la protection des renseignements personnels et les documents électroniques* (ci-après « LPRPDE », également connue sous le nom de PIPEDA, pour son sigle en anglais)[214], ou par des lois provinciales similaires (Colombie-Britannique [215], Alberta[216] et Québec[217]).

Toutefois, le texte de la loi ne renferme aucune référence spécifique à la protection des données relatives aux mineurs, comme dans l'article 8 du RGPD de l'UE. Cependant, en principe, deux dispositions contenues dans la LPRPDE nous permettraient de comprendre quelle est la situation actuelle en matière de protection des données des mineurs au Canada.

D'une manière générale, la loi réglemente la collecte, l'utilisation et la divulgation d'informations personnelles par les organisations du secteur privé exerçant des activités commerciales à but lucratif et d'autres entreprises réglementées par le gouvernement fédéral, y compris les banques, les compagnies aériennes et les sociétés de télécommunications constituées sous juridiction fédérale.

Aux termes de la LPRPDE, « information personnelle » désigne « toute information sur une personne identifiable »[218] factuelle ou subjective, enregistrée ou non[219]. Sur la notion

[214] *Loi sur la protection des renseignements personnels et les documents électroniques*, *supra* note 41.
[215] *Personal Information Protection Act*, SBC 2003, c. 63. (ci-après « Loi de la Colombie-Britannique »).
[216] *Personal Information Protection Act*, SA 2003, c. P-6.5. (ci-après « Loi de l'Alberta »).
[217] *Loi sur la protection des renseignements personnels dans le secteur privé*, LRQ, c. P-39.1. (ci-après « LPRSP »).
[218] *Loi sur la protection des renseignements personnels et les documents électroniques*, *supra* note 41. Définitions.
[219] *Morgan c Alta Flights (Charters) Inc*, 2006 Cour d'appel fédérale; Commissariat à la protection de la vie privée du Canada, « Survol de la LPRPDE », (9 janvier 2018), en ligne: <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/lprpde_survol/>, Last Modified: 2019-06-07.

d'information, la Cour fédérale a noté que « les renseignements seront des renseignements concernant un individu identifiable lorsqu'il y a de fortes possibilités que l'individu puisse être identifié par l'utilisation de ces renseignements, seuls ou en combinaison avec des renseignements d'autres sources »[220].

On peut citer comme informations personnelles l'âge, le nom, un numéro d'identification, le revenu, l'origine ethnique ou le groupe sanguin; une opinion, une évaluation, un commentaire, le statut social ou une mesure disciplinaire; le dossier d'un employé, un dossier de crédit ou de prêt, un dossier médical[221]; certaines données techniques notamment l'adresse IP, la géolocalisation, les cookies, l'identifiant unique d'un appareil mobile ou l'historique des sites web visités par un individu.[222]

Par ailleurs, la deuxième disposition qui nous intéresse pour le sujet d'étude est celle qui figure à l'article 4.3.4 de l'annexe 1 de la LPRPDE prévoyant que « [l]a forme du consentement que l'organisation cherche à obtenir peut varier selon les circonstances et la nature des renseignements. Pour déterminer la forme que prendra le consentement, les organisations doivent tenir compte de la sensibilité des renseignements ».

De la définition des informations à caractère personnel et du texte de l'article 4.3.4 transcrit précédemment, nous pouvons dire que la LPRPDE a comme objectif principal de protéger la vie privée de toutes les personnes sans distinction d'âge[223], et que l'information dans certains cas peut devenir plus sensible que d'autres. Pour le sujet qui nous occupe, il est possible de conclure que les informations personnelles des mineurs sont de nature sensible et nécessitent donc une protection particulière de la part du législateur.

Dans cette perspective, le *Commissariat à la protection de la vie privée du Canada* (ci-après « CPVP ») et *Option consommateurs* (ci-après « OC »), entre autres, se sont exprimés:

> « … le Commissaire a toujours considéré les renseignements personnels relatifs aux jeunes et aux enfants comme étant de nature particulièrement sensible, surtout ceux des

[220] *Gordon c Canada (Santé)*, 2008 Cour fédérale.
[221] Commissariat à la protection de la vie privée du Canada, *supra* note 219.
[222] Option consommateurs, *supra* note 5 à la p 43.
[223] Bureau de l'Ombudsman et du défenseur des enfants et de la jeunesse, *supra* note 100 à la p 17.

> plus jeunes enfants, et que toute collecte, utilisation ou communication de tels renseignements doit se faire dans cet esprit ou alors, ne pas se faire du tout ».[224] (CPVP)
>
> « En somme, même si la Loi fédérale ne le précise pas explicitement, on devrait généralement reconnaître le caractère sensible des renseignements personnels des enfants, de telle sorte qu'ils bénéficieront d'un degré de protection plus élevé ».[225] (OC)

Contrairement à ce qu'on pourrait croire, on peut en principe conclure que le droit à la vie privée et la protection des données des mineurs sont bien protégés par la LPRPDE, mais se poseront ensuite des problèmes liés au consentement (pierre angulaire de la loi), à la représentation et aux politiques de confidentialité.

1.1. Le consentement

Afin de permettre aux entreprises de collecter, d'utiliser ou de divulguer les données d'une personne, le principe 4.3 de la LPRPDE exige « connaissance » et « consentement ». Le principe 4.3.2 exige qu'un « consentement valable » soit obtenu préalablement. Cela signifie que le consentement sera opportun si l'autorisation du mineur est obtenue avant la collecte, l'utilisation ou la divulgation de toute information personnelle. Dans certains cas, le consentement peut être demandé après la collecte, par exemple pour une utilisation différente de celle initialement autorisée. En tout état de cause, elle doit être obtenue préalablement à l'utilisation ou à la communication.

Pour ce qui est de la notion de « consentement valable », il faut que les personnes comprennent raisonnablement avant de donner leur consentement « la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication de leurs renseignements personnels »[226].

Comme on peut le constater, la LPRPDE ne fait pas expressément référence au consentement fondé sur l'âge et ne donne pas de directives pour déterminer à quel moment le

---

[224] Commissariat à la protection de la vie privée du Canada, *Vous recueillez des renseignements auprès des enfants? Voici dix conseils sur les services destinés aux enfants et aux jeunes* , 2015 , Last Modified: 2015-12-14.
[225] Option consommateurs, *supra* note 5 à la p 43.
[226] *Loi sur la protection des renseignements personnels et les documents électroniques*, *supra* note 41, art 6.1 et principe 4.3.2; Commissariat à la protection de la vie privée du Canada, *Troisième principe relatif à l'équité dans le traitement de l'information de la LPRPDE – Consentement* , 2018 , Last Modified: 2020-08-13; Commissariat à la protection de la vie privée du Canada, *Consentement et protection de la vie privée - Document de discussion sur les améliorations possibles au consentement sous le régime de la Loi sur la protection des renseignements personnels et les documents électroniques* , 2016 aux pp 3-4 , Last Modified: 2016-05-11.

mineur a la capacité de comprendre la nature, le but et les conséquences de la collecte de ses informations. En effet, la loi reconnaît dans la note de l'article 4.3 de l'annexe 1 que, dans certains cas, il peut être « impossible ou inapproprié de demander le consentement d'un mineur », mais elle ne précise pas les cas et les modalités d'obtention du consentement.

Malgré l'absence de réglementation concernant les données relatives aux mineurs dans la LPRPDE, nous constatons que la CPVP tente de combler les lacunes de la loi en émettant des lignes directrices pour obtenir le consentement des mineurs[227]. Il est important de rappeler que les directives de la CPVP ne sont pas obligatoires en droit canadien, mais qu'elles ont servi de guide pour la protection des données des mineurs et ont encouragé les bonnes pratiques commerciales.

La CPVP a toujours reconnu qu' « il peut s'avérer fort difficile (voire impossible) d'obtenir le consentement valable de jeunes, et en particulier de très jeunes enfants »[228]; c'est pourquoi elle recommande dans ses lignes directrices[229] d'éviter ou de limiter complètement la collecte de données personnelles des mineurs. Nonobstant, elle définit des lignes directrices et des conseils à suivre par les opérateurs dans les cas où il est strictement nécessaire de recueillir des données sur le mineur.

1.1.1. Âge minimum du consentement

La LPRPDE n'établit pas d'âge de la majorité numérique, malgré les recommandations[230] de différentes entités pour modifier la loi et inclure une limite d'âge comme le font la RGPD[231] ou encore la COPPA. Par exemple, Owen Charters de *Repaires jeunesse du Canada* a recommandé

[227] Commissariat à la protection de la vie privée du Canada, *Lignes directrices pour l'obtention d'un consentement valable*, 2018, Last Modified: 2018-05-24.
[228] Commissariat à la protection de la vie privée du Canada, *Projet de position du Commissariat sur la réputation en ligne*, 2018, Last Modified: 2018-01-26.
[229] Commissariat à la protection de la vie privée du Canada, *supra* note 227.
[230] note 85 à la p 78; Bureau de l'Ombudsman et du défenseur des enfants et de la jeunesse, *supra* note 100 à la p 18.
[231] ETHI, *Témoignages*, 1re session, 42e législature, 16 mai 2017, 1555 (Dennis Hogarth, vice-président, Conseil des consommateurs du Canada). « Pour ce qui est des enfants et de la protection de la vie privée, le Conseil convient qu'il devrait être interdit de recueillir des renseignements auprès d'enfants de moins de 16 ans sans autorisation d'un tuteur légal. Cependant, il est difficile de vérifier l'âge d'une personne et les enfants peuvent duper les systèmes… Il faudrait, néanmoins, envisager la possibilité d'inclure dans les modifications prévues à la LPRPDE les mesures de protection énoncées dans le Règlement général sur la protection des données ou RGPD »).

au gouvernement de suivre l'exemple de l'UE qui exige le consentement d'un parent ou d'un tuteur pour accéder à des services en ligne[232].

Parmi les problèmes qui se posent pour justifier le fait de ne pas fixer un âge précis dans la loi figurent la violation possible des droits à la liberté d'expression et d'autres libertés fondamentales consacrés à l'article 2b) de la Loi constitutionnelle de 1982[233]. À cet égard, le professeur Karim Benyekhlef indique que:

> « A law violates the freedom of expression as soon as its effect is to prevent the «pursuit of truth, participation in the community, or individual self-fulfillment and human flourishing»2. Following this principle, prohibition of minors or certain people on SNS would, prima facie, constitute a violation of Section 2b) and the freedom of expression ».[234]

En ce qui concerne la CPVP, à travers ses lignes directrices et conseils, a signalé que pour que le consentement obtenu d'un mineur soit valable, et sauf circonstances exceptionnelles, il faut que le mineur soit âgé de moins de 13 ans, l'autorisation du parent ou tuteur doit être obtenue. En revanche, pour que le consentement d'un mineur ayant atteint l'âge du consentement numérique soit considéré comme valable[235], le processus d'obtention du consentement doit être adapté au niveau de maturité du mineur[236].

Un inconvénient supplémentaire concernant le consentement des mineurs est que la loi ne renferme pas non plus de directives ou de mécanismes permettant de vérifier l'âge réel du mineur. Bien qu'il s'agisse d'une question qui doit être développée à travers des solutions techniques complexes[237], le seul « effort raisonnable »[238] qui exige la LPRPDE est d'obtenir l'autorisation des utilisateurs, et par conséquent, les opérateurs chercheront à obtenir le consentement du mineur sans

---

[232] ETHI, *Témoignages*, 1re session, 42e législature, 25 septembre 2017, 1535 (Owen Charters, président directeur général, Repaires jeunesse du Canada).
[233] *Charte Canadienne des Droits et Libertés*, art 2(b), partie I de la Loi constitutionnelle de 1982, constituant l'annexe B de la Loi de 1982 sur le Canada (R-U), 1982, c 11. « 2.b) liberté de pensée, de croyance, d'opinion et d'expression, y compris la liberté de la presse et des autres moyens de communication ». voir aussi Karim Benyekhlef, « Minors, Social Network Sites And Le Droit Á L'oubli » dans *Soc Netw Child Priv*, Editorial Reus, 2011 229 à la p 238.
[234] Benyekhlef, *supra* note 233 à la p 239.
[235] Commissariat à la protection de la vie privée du Canada, *Ratissage de 2017 du Global Privacy Enforcement Network*, 2017, Last Modified: 2017-10-24.
[236] note 42 à la p 25; Commissariat à la protection de la vie privée du Canada, *supra* note 227; Commissariat à la protection de la vie privée du Canada, *supra* note 228 ch C. Le cas particulier des jeunes.
[237] Benyekhlef, *supra* note 233 à la p 236.
[238] *Loi sur la protection des renseignements personnels et les documents électroniques*, *supra* note 41 Art 4.3.2. Anexe 1.

déployer des techniques de validation ou d'analyse plus poussées, car cela génère des coûts élevés pour ces organisations.

La COPPA aux États-Unis, comme nous le verrons dans un chapitre ultérieur, place la charge de validation sur les sites web et les fournisseurs de services, et propose quelques solutions pour effectuer la validation. De même, COPPA exige que l'opérateur vérifie l'identité des parents et propose des méthodes de validation, certaines plus simples que d'autres, en fonction de l'usage qu'il fera de l'information du mineur. Il convient de noter que tant dans la législation canadienne que dans la COPPA américaine, l'efficacité des mécanismes de validation de l'âge du mineur a pour limite la bonne foi du mineur, car les mineurs peuvent facilement mentir à propos de leur âge.

À partir des lignes directrices fournies par la CPVP, on tentera d'identifier à quel moment et comment l'opérateur obtient le consentement valable d'un mineur.

1.1.2. Consentement parental/tuteur

La CPVP a indiqué que « il y a un âge minimum sous lequel les jeunes enfants ne sont probablement pas en mesure de comprendre pleinement les conséquences de leurs choix concernant la protection de la vie privée »[239]. En conséquence, l'entité indique que, dans le cas des mineurs de moins de 13 ans, et sauf exception, c'est le parent ou le tuteur qui doit donner le consentement pour que l'exploitant puisse recueillir, utiliser et communiquer les données personnelles du mineur[240]. En outre, on remarque ici toute la portée donnée à l'article 4.3.6 de l'annexe 1 de la LPRPDE, qui dispose que le consentement peut être donné par un représentant autorisé (tel qu'un tuteur légal ou une personne ayant une procuration)[241].

Or, l'avocat J. Lawford précise que ce qui est indiqué à l'article 4.3.6 en conjonction avec ce qui est prévu dans la note relative à l'article 4.3 concerne l'incapacité du mineur et la capacité des parents de donner leur consentement au nom du mineur dans certaines circonstances, ce qu'il

[239] Commissariat à la protection de la vie privée du Canada, *supra* note 227. Consentement et enfants
[240] Commissariat à la protection de la vie privée du Canada, « Guide sur la protection de la vie privée à l'intention des entreprises », (24 décembre 2015), en ligne: <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/guide_org/> à la p 15, Last Modified: 2020-10-09.
[241] Commissariat à la protection de la vie privée du Canada, *Rapport de conclusions en vertu de la LPRPDE. Nexopia, site de réseautage social pour jeunes, a enfreint la loi canadienne sur la protection des renseignements personnels*, nº 2012-001, 29 février 2012.

considère comme une grande ambiguïté de la loi, parce qu'il est confus en ce qui concerne le contrôle des données, s'il s'agit du mineur ou du parent. Lawford note que, dans d'autres législations, il ne fait aucun doute que, quel que soit l'âge, la personne concernée est la seule personne ayant le droit de contrôler les données[242], et conclut que dans la LPRPDE,

> « children's personal information may possibly be collected under exactly the same rules as that of adults, with the added wrinkle that consent may be that of the parent or guardian, not the child him or herself, largely at the choice of the marketer ».[243]

Une autre difficulté liée au consentement des parents est la preuve du consentement. La loi ne prévoit aucun mécanisme permettant à l'exploitant de vérifier que le consentement est donné par le parent ou le tuteur. Il convient de noter que, dans de nombreux cas, le parent se trouve en dehors de l'équation du consentement, soit parce que le mineur sait comment se soustraire à l'obligation d'autorisation parentale, soit parce que le parent accorde des congés excessifs au mineur, et/ou l'opérateur n'indique pas clairement sur le site qui doit donner le consentement. Dans l'un quelconque de ces cas, comme le mentionne l'OP, il est douteux « que ce consentement remplisse en toutes circonstances les exigences de la loi »[244].

Le principe 4.3.7 de l'annexe 1 de la LPRPDE prévoit un certain nombre de mécanismes pour obtenir le consentement, comme un formulaire de demande, une case à cocher ou une case orale lorsqu'elle est recueillie par téléphone. En règle générale, le consentement est obtenu en cliquant sur la case à cocher du formulaire d'inscription du site ou du service, mais il a été constaté que, normalement, les parents et les mineurs cliquent sur la case d'acceptation sans lire au préalable le contenu compte tenu de la complexité de ces documents[245].

Certains auteurs notent d'ailleurs à ce sujet ce qui suit: « que the choices that authors of privacy policies make can mislead readers, making informed consent effectively impossible »[246]. En outre, ces conditions prennent un temps considérable à lire[247] et ne sont pas rédigées dans un

---

[242] *All in the Data Family: Children's Privacy Online*, by Counsel John Lawford, 1-895060-86-9, Ottawa, ON, Public Interest Advocacy Centre à la p 51.
[243] *Ibid*.
[244] *Ibid* à la p 52; Option consommateurs, *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*, Montréal, Québec, Commissariat à la protection de la vie privée du Canada, 2018 à la p 35.
[245] Option consommateurs, *supra* note 5 à la p 46.
[246] Valerie Steeves, Jacquelyn Burkell & Anca Micheti, *Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand*, 2007 à la p 62.
[247] Option consommateurs, *supra* note 244 à la p 35.

langage approprié pour que les mineurs et même leurs parents[248] comprennent les implications de leur droit à la vie privée[249].

La CPVP sur la base du principe de transparence, a recommandé comme meilleure pratique « l'approche en couches », par laquelle les organisations énumèrent de brèves déclarations de confidentialité qui renvoient à des descriptions plus détaillées de la façon dont l'organisation traite les informations personnelles, ainsi que l'envoi de formulaires expliquant les pratiques de confidentialité.

Une autre difficulté que certains auteurs ajoutent est que les parents obtiennent le contrôle du droit à la vie privée des mineurs, mais la loi ne prévoit pas de mécanismes permettant aux mineurs de limiter les abus des parents lorsqu'ils ne fournissent pas l'aide nécessaire pour la suppression des données que le mineur a publiées (suppression d'une vidéo ou d'une photo), ou plus grave encore lorsque les parents sont la source de la violation du droit à la vie privée (les parents publient des photos et des informations sur les réseaux sociaux du mineur qui peuvent être inappropriées). Ce dernier point ne sera pas abordé dans le présent travail, mais nous soulignons qu'il a fait l'objet d'une étude détaillée par OC[250].

1.1.3. Consentement des jeunes

Aux difficultés détaillées précédemment, il faut ajouter celles qui se posent en ce qui concerne l'obtention du consentement des jeunes. En principe, ce sont des jeunes qui ont atteint l'âge de la majorité numérique. Toutefois, on considère que font également partie de ce groupe les mineurs qui n'ont pas encore atteint l'âge de la majorité civil (moins de 18 ans ou l'âge de la majorité selon la province).

---

[248] Benyekhlef, *supra* note 233 aux pp 234-235.

[249] Chambre des communes du Canada*, Protection de la vie privée et médias sociaux à l'ère des mégadonnées : Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique*, 41e lég, 1re sess, no 5-ETHI (41-1), (avril 2013) (président : Pierre-Luc Dusseault) à la p 27; ETHI, *Témoignages,* , 1re session, 41e législature, 19 juin 2012, 1100 (Sara Grimes, Université de Toronto). « Cela soulève la question du consentement informé, car « ces documents sont longs et extrêmement complexes […] [et] décrivent une grande variété d'activités de collecte de données et comprennent de nombreux termes qui sont inappropriés et qui ne peuvent pas même être utilisés pour demander le consentement des enfants ».

[250] Pour plus de détails, consultez : Option consommateurs, *supra* note 244.

La CPVP note que le consentement valable d'un jeune est réputé avoir été obtenu[251], quand l'exploitant peut démontrer qu'il a pris les mesures nécessaires pour s'assurer que le processus d'obtention du consentement a été adapté au degré de maturité de l'enfant[252] .

Cela signifie que les jeunes doivent raisonnablement comprendre quelles sont les données personnelles collectées par l'opérateur et comment elles seront utilisées ou communiquées[253]. Rappelons que l'une des deux conditions fondamentales pour que le consentement soit valable est que le consentement soit donné en connaissance de cause. En l'absence de cet élément, le consentement devient sans objet. Ceci est bien expliqué lorsque le professeur K. Benyekhlef fait remarquer que « the consent is rather pointless if it is not enlightened »[254].

Cependant, dans les différents rapports de la commissaire, on constate que les sites destinés aux enfants ne disposent pas de mécanismes différents pour « autonomiser les élèves plus âgés en recherchant le consentement éclairé approprié à leur âge »[255]. Il est donc difficile d'obtenir un consentement valable et de prouver les mécanismes utilisés. La question est simple : comment l'opérateur peut-il entrer pour vérifier la maturité de chaque mineur?

1.2. Modalités d'obtention du consentement valable

La CPVP en tenant compte des résultats du ratissage du Global Privacy Enforcement Network pour la protection de la vie privée, a mis en évidence certains mécanismes pour obtenir le consentement selon la tranche d'âge : 1) affirme que la meilleure pratique serait d'envoyer un courriel aux parents avec des instructions sur la façon d'inscrire leur enfant de moins de 13 ans dans le service, et 2) recommande d'inclure des explications sur les mécanismes de consentement pour les mineurs de plus de 13 ans. Cependant, ce sont les seuls mécanismes référencés[256].

En conséquence, selon les recommandations de la commissaire, l'exploitant doit être en mesure de démontrer qu'il a mis en place un processus d'obtention du consentement et qu'il

[251] Commissariat à la protection de la vie privée du Canada, *supra* note 227. « Consentement et enfants ».
[252] Commissariat à la protection de la vie privée du Canada, *Les technologies de surveillance appliquées aux enfants : Rapport de recherche préparé par le Groupe de recherche du Commissariat à la protection de la vie privée du Canada (Kasia Krzymien)*, octobre 2012 à la p 9
[253] Commissariat à la protection de la vie privée du Canada, *supra* note 241 nº 70. Section 2.
[254] Benyekhlef, *supra* note 233 à la p 234.
[255] Commissariat à la protection de la vie privée du Canada, *supra* note 235.
[256] *Ibid*.

respecte les obligations de la loi[257]. Ce processus doit être fondé sur un « régime de responsabilité efficace » sur la base du septième principe directeur pour l'obtention d'un consentement valable développé par la CPVP[258], qui se traduira finalement par une compréhension suffisante de l'utilisateur sur le type d'informations personnelles que le contrôleur est en train de recueillir et le but ou l'objet de la collecte.

Enfin, pour obtenir le consentement valable des mineurs et garantissant l'utilisation appropriée de leurs données personnelles, on peut trouver dans les documents de la CPVP, que les sites web et les fournisseurs de services en ligne doivent : i) se limiter à la collecte des données qui sont strictement nécessaires et identifier le niveau d'information requis[259]; ii) prendre soin de recueillir des informations par inadvertance, par exemple, lors de la création d'utilisateurs [260]; iii) veiller à ce que les mineurs comprennent les politiques de protection de la vie privée en utilisant non seulement un langage adapté aux capacités cognitives des mineurs, mais en recherchant des techniques interactives et innovantes pour les informer sur les implications de leurs décisions en matière de confidentialité[261]; iv) préciser si est le mineur ou le parent/tuteur, la personne qui doit accepter les termes et conditions[262]; v) vérifier et documenter la manière dont le consentement valable du mineur est obtenu; vi) inclure les paramètres nécessaires pour limiter les utilisateurs à fournir plus d'informations que ce qui est requis, ou qu'un autre membre demande au mineur des informations personnelles, le cas échéant[263], de surveiller le respect des obligations imposées aux mineurs (comme ne pas s'identifier par son nom complet)[264], et mettre en place des mesures techniques (ou autres) empêchant l'utilisation non autorisée des informations concernant les enfants [265] et; vii) garantir la suppression et informer des conséquences du retrait. Les mineurs ou leurs parents peuvent demander la suppression de leurs informations personnelles, sous réserve de

[257] Commissariat à la protection de la vie privée du Canada, *supra* note 224.
[258] Commissariat à la protection de la vie privée du Canada, *supra* note 227.
[259] Commissariat à la protection de la vie privée du Canada, *supra* note 224. « 1. Limitez, ou évitez complètement, la collecte de renseignements personnels ».
[260] *Ibid*. « 2. Prenez garde de ne pas procéder à des collectes « par inadvertance »
[261] *Ibid*. « 6. Tenez compte de l'expérience d'utilisateur ».
[262] *Ibid*. « 7. Identifiez clairement la personne devant consentir aux modalités ».
[263] *Ibid*. « 8. Assurez-vous d'avoir les bons paramètres par défaut en fonction de l'âge de vos utilisateurs ».
[264] *Ibid*. « 9. Soyez au fait de ce qui se passe sur votre site ».
[265] *Ibid*. « 10. Vaut mieux prévenir que contrôler ».

restrictions légales ou contractuelles et d'un préavis raisonnable. À cette fin, les opérateurs doivent prévoir une procédure simple de suppression.

§ Réglementation spécifique

La protection des données à caractère personnel des mineurs dans le cadre d'une réglementation spécifique fait l'objet de discussions depuis plusieurs années déjà. Les commissaires à la vie privée et les défenseurs canadiens des enfants et des jeunes, dans le document de réflexion sur la protection des renseignements personnels des enfants en ligne (2009)[266], sont conscients que la LPRPDE pourrait être modifiée pour inclure des règles claires sur le consentement à la collecte, à l'utilisation et à la divulgation des informations personnelles des enfants[267]. Ils manifestent leur accord total avec le mécanisme proposé par le « *Public Interest Advocacy Centre* »[268], par lequel ils proposent d'établir différents degrés de consentement, selon l'âge du mineur.

> « Nous pourrions, par exemple, modifier la LPRPDE ou des lois provinciales essentiellement semblables pour renforcer les exigences relatives au consentement en fonction de conditions d'âge précises et exiger différents niveaux de consentement d'après les catégories d'âge. Voici un mécanisme proposé pour des exigences variables relatives au consentement que le Centre pour la défense de l'intérêt public a mis de l'avant dans un rapport en 2008, sur la vie privée des enfants en ligne :
>
> 1. Moins de 13 ans : une interdiction générale sur la collecte, l'utilisation et la communication de tous les renseignements personnels d'enfants de moins de 13 ans.
> 2. De 13 à 15 ans : les sites Web seraient autorisés à recueillir et à utiliser des renseignements personnels uniquement pour leurs fins et avec le consentement explicite de l'adolescent et du parent, et il leur serait interdit de communiquer ces renseignements personnels à des tiers.
> 3. De 16 ans à la majorité (18 ou 19 ans) : les sites Web seraient autorisés à recueillir des renseignements personnels avec le consentement de l'adolescent, mais ne pourraient communiquer les renseignements recueillis sur l'adolescent qu'avec le consentement positif de l'adolescent et le consentement explicite de son parent ou de sa mère.
> 4. Après avoir atteint l'âge légal : les sites Web et les sociétés ne seraient plus autorisés à conserver les renseignements recueillis lorsque l'enfant n'avait pas l'âge de la majorité et ils seraient obligés de supprimer les renseignements immédiatement, sans consentement explicite de la personne qui vient d'atteindre l'âge de la majorité ».[269]

[266] Bureau de l'Ombudsman et du défenseur des enfants et de la jeunesse, *supra* note 100.
[267] *Ibid* à la p 28.
[268] Voir Lawford, *supra* note 242 aux pp 69-70.
[269] Voir notamment Bureau de l'Ombudsman et du défenseur des enfants et de la jeunesse, *supra* note 100 à la p 18.

David Elder, de la CMA, a également rappelé dans son témoignage au Comité permanent de l'accès à l'information, à la vie privée et à l'éthique de la Chambre des communes[270] que le consentement dans la LPRPDE est déjà « assez flexible et qu'elle reconnaît qu'il faut appliquer une norme différente quand on s'adresse à des enfants »[271]. OC recommande aussi au gouvernement fédéral et/ou provincial « de modifier les lois sur la protection des renseignements personnels afin de limiter la collecte, l'utilisation et la communication que les entreprises peuvent faire des renseignements personnels d'enfants à des fins commerciales et autres »[272].

De même, dans le rapport de la commission parlementaire qui a examiné la réforme de la LPRPDE en 2018, le comité a noté que « des mesures devraient également être mises en place afin de limiter la capacité des organisations de collecter, d'utiliser et de communiquer des renseignements personnels concernant des personnes mineures » [273] et a donc recommandé « la mise en place de règles concernant la collecte, l'utilisation et la communication de renseignements personnels concernant les mineurs » [274]. Mais à cette recommandation, le gouvernement à travers le Ministre de l'Innovation, des Sciences et du Développement économique a répondu que « [l]a question d'appliquer des mesures explicites de protection des mineurs en vertu de la loi fédérale présente des défis particuliers, car la définition d'un mineur, de compétence provinciale, en fait intrinsèquement partie »[275].

Or, on considère que la protection des mineurs est une question qui doit être résolue au niveau fédéral, y compris une série de paramètres, d'outils et de principes directeurs que les provinces et territoires ainsi que les commissions respectives de protection de la vie privée, puissent être appliquées de manière uniforme au niveau national. En outre, l'établissement d'une norme fondée sur l'âge, et non sur le développement affectif ou cognitif du mineur, renforcerait la sécurité juridique tant pour les mineurs que pour les opérateurs. Ainsi, contrairement à ce qui a été dit par

---

[270] ETHI, *Témoignages*, 1re session, 41e législature, 16 octobre 2012, 1700 (David Elder, ACM).
[271] note 249 à la p 27.
[272] Option consommateurs, *supra* note 244 à la p 48.
[273] note 85 à la p 40. Voir la recommandation 9 sur les règles de consentement spécifiques pour les mineurs.
[274] *Ibid*. Voir la recommandation 9 sur les règles de consentement spécifiques pour les mineurs.
[275] Chambre des communes du Canada, *Réponse du gouvernement au rapport du Comité permanent de 1' accès à 1' information, de la protection des renseignements personnels et de 1' éthique intitulé Vers la protection de la vie privée : Examen de la Loi sur la protection des renseignements personnels et les documents électroniques*, ETHI 8512-421-344, 2016 à la p 5. En ligne : <https://www.noscommunes.ca/content/Committee/421/ETHI/GovResponse/RP9995236/421_ETHI_Rpt12_GR/421_ETHI_Rpt12_GR-f.pdf>.

le gouvernement fédéral, la Cour suprême du Canada dans une affaire de cyberharcèlement a indiqué que la protection des droits au respect de la vie privée des jeunes « est fondée sur l'âge et non sur la sensibilité de l'enfant en particulier… Le droit attribue la vulnérabilité accrue en fonction de l'âge et non du tempérament »[276].

En terminant, il convient de noter que la situation actuelle n'est pas encourageante. La LPRPDE est en cours de révision et, contrairement au projet de loi 64 du Québec[277], elle ne traite pas expressément du consentement à la collecte, à l'utilisation et à la divulgation d'informations personnelles sur les mineurs. La fixation d'un âge minimum, soit de 13 ans comme proposé par la CPVP, soit de 14 ans comme au Québec, apporte une certitude juridique.

Section 2 – Code de déontologie et normes de pratique : Association canadienne du marketing

Tout d'abord, il convient de rappeler qu'au Canada, l'industrie de la publicité et du marketing comprend un large éventail de lois, statuts et règlements fédéraux et provinciaux, décisions, principes, orientations et codes de pratique de l'industrie émis par différentes entités et organismes d'autorégulation. Dans certains cas, ces lois et mécanismes sont d'application générale. Dans d'autres cas, ils ne s'appliquent qu'à un type de service ou de produit[278].

Dans le cas qui nous concerne, l'autorégulation de la publicité et du marketing est un système par lequel l'agence et l'industrie établissent des règles volontaires et des normes de pratique qui vont au-delà de leurs obligations légales, afin de protéger les droits des utilisateurs. *L'Association canadienne du marketing* (ci-après « ACM ») est un organisme clé d'autorégulation qui couvre toutes les disciplines, les moyens et les technologies de marketing et de publicité dans la plupart des secteurs commerciaux au niveau national[279].

---

[276] *A.B. c. Bragg Communications Inc.*, *supra* note 45.
[277] *PL 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, 1re sess, 42e lég, Québec, 2020*. 1re sess, 42e lég, Québec, 2020. (ci-après « Projet de Loi 64 »). En ligne : <http://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html>.
[278] Bill Hearn, « Canada: Canadian Advertising & Marketing Law: An Overview of the Rules, The Regulators And Their Powers », *Fogler Rubinoff LLP* (14 février 2017), en ligne: <https://www.mondaq.com/canada/advertising-marketing-branding/568494/canadian-advertising-marketing-law-an-overview-of-the-rules-the-regulators-and-their-powers>.
[279] *Ibid*.

L'ACM est allé de l'avant en élaborant des propres règles, par l'entremise du *Code de déontologie et des normes de pratique*[280] (ci-après « le Code ACM ») et des lignes directrices sur le marketing auprès des enfants et des adolescents[281]. Étant donné que l'on est face à un processus d'autorégulation, ces règles ne sont uniquement obligatoires à ses membres, reconnaissant que les mineurs appartiennent à un groupe vulnérable[282]. Aussi, le Code ACM par exemple consacre deux sections exclusivement réservées au marketing destiné aux mineurs et à la protection de leurs données personnelles. C'est ainsi que, nous trouvons ici les trois aspects qui ont conduit à choisir ce code de bonnes pratiques, comme un outil important dans le développement des droits de protection des données des mineurs, texte au sujet duquel nous procéderons à une brève analyse.

D´abord, on peut lire dans les lignes directives que ces deux sections relatives au marketing qui sont destinés aux enfants et adolescents, se fondent principalement sur le fait que le mineur n'est pas un adulte et, par conséquent « marketers must respect involvement of the child's parent or guardian in any communication or transaction »[283]. À ce propos et compte tenu du facteur objectif de l'âge, aux fins du Code, le terme « enfant » désigne une personne âgée de moins de 13 ans[284] tandis que le terme « adolescent »[285] dénomme une personne ayant atteint ses 13 ans, mais n'ayant pas encore atteint l'âge de la majorité dans sa province ou son territoire de résidence[286], sauf exception définie par le Code de déontologie.

Comme on peut le constater, le code ACM fait une différence importante par rapport à toutes les législations étudiées dans ce mémoire, car il reconnaît l'importance de protéger indépendamment les droits des mineurs, en les séparant des dispositions relatives aux adultes, en reconnaissant que selon la tranche d'âge dans laquelle le mineur se trouve, il peut être accordé plus ou moins de liberté dans l'exercice de ses droits.

---

[280] Association canadienne du marketing (ACM), *Code de déontologie et normes de pratique*, Toronto, Ontario, TheCMA.ca, 2019.
[281] Canadian Marketing Association, *Guidelines for Marketing to Children and Teenagers*, 2007, Last Modified: 2018-05-24.
[282] *Ibid* à la p 1.
[283] *Ibid*.
[284] Association canadienne du marketing (ACM), *supra* note 280, art K1 Âge.
[285] *Ibid*, art L1 Âge et mise en pratique. « Ces directives ne s'appliquent pas aux adolescents vivant indépendamment de leurs parents ou de leurs tuteurs et qui, selon la loi ou les règlements fédéraux, provinciaux et territoriaux, sont présumés adultes ».
[286] *Ibid*.

Par conséquent, en ce qui concerne la collecte, l'utilisation et la diffusion des informations personnelles concernant le mineur, le Code dispose que, pour toutes les transactions que le fonctionnaire souhaite effectuer sur des informations concernant des enfants de moins de 16 ans, le consentement explicite et sans équivoque d'un parent ou tuteur de l'enfant doit être obtenu, en reconnaissant que « the marketing to children is more sensitive or more intrusive than the gathering of a child's personal information »[287].

En référant aux adolescents de 13 à 16 ans, si l'autorisation ne s'adresse qu'à la collecte et à l'utilisation (non-divulgation) des coordonnées (informations de contact), l'inclusion dans des projets de recherche et/ou l'interroger à des fins de recherche, il faudra obtenir le consentement préalable du parent ou tuteur. Enfin, dans tous les cas, le consentement des adolescents de plus de 16 ans qui n'ont pas atteint l'âge de la majorité doit être obtenu pour la collecte, l'utilisation et la divulgation de leurs informations personnelles.

Or, a l´instar de la plupart des lois et des règlements, le problème de la validation de l'âge se trouve dans ce règlement. Bien que les lignes directrices prévoient que « le vendeur est tenu de déterminer l'âge du mineur, en particulier de l'adolescent, pour que les dispositions deviennent effectives »[288], aucun mécanisme de validation n'est prévu dans la norme ou les lignes directrices.

En outre, compte tenu du fait que la mise en œuvre de ce mécanisme génère un investissement important, que la publicité génère des avantages économiques élevés pour les entreprises[289] et que les sanctions en cas de non-respect éventuel ne sont pas significatives, les agences de publicité et de marketing investissent dans des technologies de pointe qui leur permettent de mettre en place des services et des produits innovants à travers lesquels ils collectent des informations personnelles auprès de l'enfant, et ce, sans même s'en rendre compte.

Celle-ci concernent notamment la « publicité immersive » qui est utilisée pour commercialiser leurs produits ou services, au moyen de jeux en ligne interactifs, applications, participation aux activités et tirages au sort en ligne ou via les réseaux sociaux, afin de fidéliser les mineurs à leur marque. Et aussi, la publicité comportementale en ligne (PCL) constitue « une forme

[287] Canadian Marketing Association, *supra* note 281 à la p 3.
[288] *Ibid* à la p 5.
[289] Krzymien, *supra* note 252 à la p 4.

de publicité dans laquelle on dresse le profil d'un internaute à partir de ses activités de navigation d'afficher des annonces et correspondant sur les sites qu'il fréquente »[290]

C'est sur ce point que l'effectivité des dispositions du Code ACM commence à disparaître. En premier lieu parce que « le Code de déontologie se veut général et ne traite pas spécifiquement des défis des stratégies de marketing comportemental en ligne et de la façon dont les enfants utilisent Internet »[291]. En autre, au-delà des lignes directrices, l´ACM en se référant à ces nouvelles techniques, conseille à ses membres de ne pas les utiliser sur des mineurs, mais ce n'est pas une obligation de ne pas le faire[292].

En second lieu, car qu'avec ce type de publicité on viole clairement des règles régissant le marketing des mineurs : en particulier, celle qui prévoit qu'il est interdit d'exploiter la crédulité des enfants, leur manque d'expérience et leur sens de la loyauté[293]. Et celle qui dispose que la publicité destinée aux mineurs soit présentée dans un langage simple et adapté à l'âge, afin que l'enfant puisse facilement la comprendre[294], et ce, en tenant compte du fait que la complexité de la publicité doit être liée à la maturité du mineur auquel elle s'adresse.

Il est évident qu'avec l'utilisation de ces technologies, il n'est pas possible d'obtenir le consentement préalable, libre et éclairé (consentement *opt-in*) du mineur, du parent ou tuteur dans les termes du code, ni dans les termes de la LPRPD, parce que le mineur n'est pas informé de la collecte de ses données ni de la fin de celle-ci, parce qu'ils utilisent des moyens intéressants qui attirent les mineurs en exploitant leur crédulité, par exemple un jeu de leurs personnages préférés ou des vidéos sur les réseaux sociaux comme *YouTube* au *TikTok*, et aussi puisqu'un enfant ne comprend pas les enjeux associés au suivi de ses données[295].

---

[290] *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?* par Option consommateurs, Montréal, Québec, Bureau de la consommation d'Industrie Canada, 2015 à la p iv.
[291] Lawford, *supra* note 242 à la p 45.
[292] Canadian Marketing Association, *supra* note 281 à la p 5.
[293] Association canadienne du marketing (ACM), *supra* note 280, arts K5 et L5 Crédulité.
[294] *Ibid*, arts K6 et L6 Langage adapté à l'âge.
[295] *La trousse numérique*, par Alliance médias jeunesse, Société de développement de l'industrie des médias de l'Ontario et le Fonds des médias du Canada, 2015 à la p 30.

À cet égard, la CPVP a publié sa position sur la publicité comportementale en ligne qui établit des restrictions concernant la surveillance des enfants. Dans le document, le commissariat a indiqué que pour obtenir un consentement valable :

> « Il est difficile de prétendre que de jeunes enfants puissent donner un consentement valable à pareilles pratiques, et le profilage de jeunes en vue de leur offrir de la publicité comportementale ciblée en ligne semble inapproprié dans ces circonstances »[296].

En outre, la situation est plus risquée pour les adolescents âgés de 13 à 16 ans, car le consentement parental n'est exigé qu'en cas de divulgation et dans d'autres cas spécifiques. Il convient de noter que l'information des adolescents a une grande valeur économique, en particulier parce que les adolescents de ces âges commencent à avoir un pouvoir d'achat de plus en plus grand et sont donc eux-mêmes, utilisateurs potentiels d'un service ou d'un produit. Quelque chose de plus intéressant pour une entreprise que des utilisateurs potentiels?

Bref, comme nous pouvons le constater, le Code de l'ACM peut servir de modèle pour une éventuelle modification de la LPRPDE, dans la mesure où non seulement il protège les mineurs de manière spécifique, mais aussi il définit la notion d'enfant et d'adolescent, en tenant compte à la fois du facteur objectif de l'âge et du facteur subjectif de la maturité, et en adaptant les règles en conséquence[297]. De même, il exige le consentement exprès pour la collecte, l'utilisation et la divulgation d'informations personnelles, en plus de définir les événements dans lesquels le consentement parental est requis.

Malheureusement, le champ d'application du code se limite exclusivement au marketing du consommateur, aucun mécanisme n'est mis en place pour vérifier l'âge des mineurs[298], et il n'aborde pas les nouvelles stratégies de marketing comme le marketing comportemental en ligne. De même, si un membre ne se conforme pas aux directives, l'ACM engagera une procédure de médiation interne puis externe pour régler à l'amiable le cas de non-respect. En cas de désaccord, le membre peut être expulsé de l'association. En conclusion, le membre ne reçoit pas de sanctions significatives.

---

[296] Commissariat à la protection de la vie privée du Canada, *Position de principe sur la publicité comportementale en ligne*, 2015, Last Modified: 2015-12-16.
[297] Lawford, *supra* note 242 à la p 45.
[298] Canadian Marketing Association, *supra* note 281 à la p 5.

Chapitre 2 – Sources juridiques au Québec

Section 1 – Loi sur la protection des renseignements personnels dans le secteur privé (LPRPSP)

Au Québec, la *Loi sur la protection des renseignements personnels dans le secteur privé* (ci-après « LPRPSP ») est reconnue comme étant essentiellement similaire à la LPRPDE. En général, la loi provinciale est applicable aux organisations du secteur privé tant que les opérations commerciales sont réalisées exclusivement à l'intérieur de la province. Dans le cas où l'opération présente une composante interprovinciale, ou soit une entreprise sous juridiction fédérale établie au Québec[299], l'organisation est tenue de se conformer aux dispositions de la LPRPDE.

À l'heure actuelle, la LPRPSP tout comme la loi fédérale, ne renferme aucune disposition spécifique protégeant les données des mineurs. L'article 2 définit la notion de renseignement personnel comme des informations qui se rapportent à « une personne physique et permettent de l'identifier », sans qu'il n'y ait de distinction entre mineurs et adultes.

De même, compte tenu du fait qu'au Québec le droit au respect de la réputation et de la vie privée d'une personne est garanti par la Charte des droits et libertés de la personne (ci-après Charte québécoise)[300] et le Code civil du Québec, l'article premier de la LPRPSP nous renvoie au chapitre « Du respect de la réputation et de la vie privée » (articles 35 à 40) du Code civil. Cependant, ces dispositions ne s'appliquent pas non plus exclusivement aux mineurs, ne portent pas sur aspects liés au consentement, l'âge de la majorité numérique ni sur la représentation légale du mineur.

En conséquence, en ce qui concerne la protection des données des mineurs, nous devons nous référer aux dispositions générales du code civil relatives à la capacité et à l´institution de l'autorité parentale. Dans ce cas, on peut conclure qu'une organisation peut recueillir, communiquer ou utiliser les informations de toute personne âgée de moins de 18 ans, lorsque le parent ou le tuteur a donné un consentement.

---

[299] *Air Canada* c. *Constant*, 2003 CanLII 1018 (QC CS), <https://canlii.ca/t/5z0q>.
[300] *Charte des droits et libertés de la personne*, RLRQ c C-12, art 5.

Or, la présente protection législative demeure insuffisante. Néanmoins, le Québec s'est placé à l'avant-garde avec le *Projet de loi no 64*, *« Loi modernisant des dispositions législatives en matière de protection des renseignements personnels »*[301], introduit en juin 2020, qui prévoit de moderniser la législation en vigueur sur la protection des données à caractère personnel.

Se rapprochant des dispositions de la RGPD, le projet de loi 64 (ci-après « PL64 ») ajoute de nouveaux articles à la LPRPSP et à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après « LADOPPRP »), qui traitent spécifiquement de la question du consentement concernant les mineurs.

En règle générale, le PL64 exige « l'obtention du consentement du titulaire de l'autorité parentale pour une collecte, une utilisation ou une communication de renseignement personnel concernant un mineur de moins de 14 ans »[302].

Par exemple, les articles 16 et 96 du PL64 ajoutent l'article 4.1 à la LPRPSP et l'article 30 à la LADOPPRP, respectivement en établissant que :

> « Les renseignements personnels concernant un mineur de moins de 14 ans ne peuvent être recueillis auprès de celui-ci sans le consentement du titulaire de l'autorité parentale, sauf lorsque cette collecte est manifestement au bénéfice de ce mineur. »[303]

De même, on peut lire aux articles 9 et 102 du PL64, que :

> « [l]e consentement du mineur de moins de 14 ans est donné par le titulaire de l'autorité parentale. Le consentement du mineur de 14 ans et plus est donné par le mineur ou par le titulaire de l'autorité parentale » [304].

De la lecture des articles cités, nous pouvons voir comment en termes généraux ils traitent de la même situation, c'est-à-dire la nécessité d'obtenir le consentement du parent ou tuteur des mineurs de moins de 14 ans. Cependant, les articles 16 et 96 du PL64 prévoient une exception[305] dont le mineur peut fournir des renseignements sans le consentement du titulaire de l'autorité

---

[301] *PL64*, *supra* note 277.
[302] *Ibid*.
[303] *Ibid*, art 4.1.
[304] *Ibid*, art 14.
[305] Commission des droits de la personne et des droits de la jeunesse, *Mémoire sur le projet de loi 64 sur la protection des renseignements personnels | CDPDJ* Commission des institutions de l'assemblée nationale, 2020) [unpublished] à la p 83.

parentale, dans les événements que la collecte soit « manifeste au bénéfice du mineur de moins de 14 ans ».

Or, la question qui ne résout pas les dispositions du PL64, se présente ainsi: qu'est-ce qui constitue une collecte « manifestement au bénéfice » du mineur de moins de 14 ans?[306] Quels sont les critères pour déterminer si la collecte est dans l'intérêt du mineur? Qui détermine si la collecte est « manifestement au bénéfice » du mineur? S'il est manifestement dans l'intérêt du mineur, le responsable de l'autorité parentale doit-il donner son consentement? Quelles sont les conséquences si la collecte n'a pas eu lieu manifestement « au bénéfice du mineur »? Il est possible que le législateur ait voulu incorporer subtilement le principe de « *l'intérêt supérieur de l'enfant* »[307], en ajoutant cette exception. Malheureusement, le législateur aurait dû inclure expressément ce principe[308].

Contrairement à ce qui précède, et conformément aux observations de la Commission des droits de la personne et des droits de la jeunesse, la dérogation étudiée concernant le consentement parental, dans le cas où la collecte soit « manifeste au bénéfice du mineur de moins de 14 ans », peut être utile lorsque la personne qui viole les droits du mineur est le détenteur de l'autorité parentale qui a consenti au traitement des données personnelles du mineur[309].

Dans une affaire portant sur l'autorité parentale, la Cour supérieure du Québec a examiné l'étendue de cette autorité et le droit à la vie privée des enfants, et a fait valoir qu'en l'absence de motifs raisonnables, l'autorité parentale doit céder la place au droit à la vie privée de l'enfant[310].

En outre, le PL64 ne prévoit pas de mécanismes permettant d'obtenir le consentement du mineur ou du titulaire de l'autorité parentale, ni n'impose au responsable des données l'obligation de vérifier si celui qui donne le consentement est celui qui détient l'autorité parentale, l'âge du mineur, ou encore la mise en œuvre d'outils pour effectuer ces validations[311].

---

[306] Barreau du Québec, *Mémoire sur le projet de loi 64 sur la protection des renseignements personnels | BQ* Commission des institutions de l'assemblée nationale, 2020) [unpublished] à la p 10.
[307] *CIDE*, *supra* note 4, art 3(1); C.c.Q, *supra* note 50, art 34
[308] Commission des droits de la personne et des droits de la jeunesse, *supra* note 305 à la p 84.
[309] *Ibid* à la p 83.
[310] *2019 QCCS 5769*.
[311] Commission des droits de la personne et des droits de la jeunesse, *supra* note 305 à la p 85.

Un aspect important à garder à l'esprit est que le PL64 prévoit que le consentement doit être « manifeste, libre, **éclairé** et être donné à des fins spécifiques. Il est demandé à chacune de ces fins, **en termes simples et clairs**, distinctement de toute autre information communiquée à la personne concerné »[312].

Du texte précédemment cité, il est surprenant que, si le législateur prévoit que le responsable des données doit expliquer et informer en termes simples et clairs la finalité pour laquelle les données personnelles seront utilisées, il est dommage qu'il n'ait pas expressément inclus que toutes les informations destinées à un mineur, telles que les politiques de confidentialité, soient présentées de manière concise, exhaustive, transparente, et dans un langage clair, simple et adapté à l'âge du mineur[313].

Cette disposition est vraiment importante si l'on veut obtenir un consentement éclairé, ce qui est déjà en principe difficile à obtenir par rapport aux adultes. Le professeur Vincent Gautrais, dans son intervention à l'audition publique sur le projet de loi n° 64, a souligné que « ces dispositions sur le consentement impliquent que l'usager s'intéresse, qu'il lise, qu'il comprenne et même que souvent l'utilisation de données soit explicable », et a indiqué aussi que selon une étude, « ça prend 20 heures par semaine pour un usager moyen d'Internet de lire toutes les politiques de vie privée »[314].

En plus, le PL64 n'interdit pas l'utilisation des informations des moins de 14 ans à des fins commerciales et ne fait pas de différence entre les sites/services destinés exclusivement aux mineurs et les sites/services d'audience mixte ou générale.

Finalement, en ce qui concerne le « droit à l'oubli », le PL64 ajoute un nouvel article 28.1dans la LPRPSP, qui prévoit que :

> « La personne concernée par un renseignement personnel peut exiger d'une personne qui exploite une entreprise qu'elle cesse la diffusion de ce renseignement ou que soit désindexé tout hyperlien rattaché à son nom permettant d'accéder à ce renseignement par un moyen technologique, lorsque la diffusion de ce renseignement contrevient à la loi ou à une ordonnance judiciaire… ».

[312] C'est nous qui marquons en caractère gras.
[313] Commission des droits de la personne et des droits de la jeunesse, *supra* note 305 à la p 85.
[314] Vincent Gautrais, *Consultations particulières et auditions publiques sur le projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, Québec, 2020.

En addition, cet article prévoit que « la décision de cesser de diffuser, de désindexer ou de réindexer un renseignement doit tenir compte « du fait que la personne concernée est mineure ».[315] Cependant, pour garantir la protection de la vie privée et des données personnelles des mineurs, il est fortement recommandé d'élargir ce critère d'évaluation, de manière à ce que les adultes et les mineurs puissent faire usage du droit à l'oubli, tant que les informations à caractère personnel ont été traitées alors qu'il était encore mineur. Nous sommes donc en accord avec la modification proposée par certaines entités, selon laquelle « l'expression « du fait que la personne concernée est mineure » figurant au nouvel article 28.1 de la LPRPSP soit remplacée par « du fait que la personne concernée était mineure au moment de la diffusion »[316].

En guise de dernière réflexion sur le droit à l'oubli, bien que le législateur tente d'inclure un certain nombre de directives et de critères que doivent suivre les organisations pour accéder ou non à une pétition pour supprimer certaines données du mineur, la décision finale comporte toujours un élément discrétionnaire.

En bref, il est clair que le PL64 représente une mise à jour importante et que le Québec fait des efforts louables pour protéger les mineurs, mais il reste plusieurs aspects à régler à court terme concernant la protection des données de mineurs.

Section 2 – Loi sur la protection du consommateur du Québec

Au Québec, la *Loi sur la protection du consommateur* (ci-après « LPCQ ») interdit la publicité à but commercial destinée aux enfants âgés de moins de 13 ans aux articles 248[317] et 249[318]. De même, le règlement d'application de la *Loi sur La Protection du Consommateur* dans

[315] Commission des droits de la personne et des droits de la jeunesse, *supra* note 305 à la p 96.
[316] Option consommateurs, *Mémoire sur le projet de loi 64 sur la protection des renseignements personnels* Commission des institutions de l'Assemblée nationale, 2020) [unpublished] aux pp 12-13; Commission des droits de la personne et des droits de la jeunesse, *supra* note 305 à la p 96.
[317] *Loi sur la protection du consommateur*, *supra* note 53, art 248. « Sous réserve de ce qui est prévu par règlement, nul ne peut faire de la publicité à but commercial destinée à des personnes de moins de treize ans. »
[318] *Ibid*, art 249.*Ibid*, « 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.

ses articles 87 à 91 inclut la section II[319], ayant pour objet de réglementer la publicité destinée aux enfants, mais surtout d'établir un régime d'exception par rapport à la prohibition de publicité dirigée aux enfants.

Il convient de signaler que, dans l'ensemble de ce texte de loi ne se trouve aucune disposition référant à la protection et au traitement de données de mineurs quand ils se trouvent en ligne, contrairement aux dispositions du Code de déontologie expédié par L'ACM. En dépit de cette remarque, *l'Office de la protection du consommateur* (ci-après « L´OPC »), dans son Guide d'application des articles 248 et 249 de la *Loi sur la protection du consommateur* : « Publicité destinée aux enfants de moins de 13 ans »[320], indique clairement que la loi est évolutive[321] et précise que « tous les supports et tous les médias sont visés, quand ils sont employés pour diffuser un message publicitaire à but commercial ». Par rapport aux sites web, il indique que « Une section d'un site Web est, notamment, un média » [322].

Par conséquent, toute publicité en ligne destinée aux enfants de moins de 13 ans et qui répond aux critères d'application énoncés à l'article 249 de la LPCQ[323], est considérée comme illégale, sauf quelques exceptions (ne s'applique pas aux étalages, aux emballages, aux présentoirs et aux vitrines).

Cependant, quand on parle de publicité sur Internet, il est facile de penser à la publicité que nous recevons de manière directe : messages accrocheurs (bannières) ou images d'un produit ou service, vidéos émergeant (pop-ups) ou ceux qui vous forcent à regarder avant ou entre deux jeux

Le fait qu'un tel message publicitaire soit contenu dans un imprimé destiné à des personnes de treize ans et plus ou destiné à la fois à des personnes de moins de treize ans et à des personnes de treize ans et plus ou qu'il soit diffusé lors d'une période d'écoute destinée à des personnes de treize ans et plus ou destinée à la fois à des personnes de moins de treize ans et à des personnes de treize ans et plus ne fait pas présumer qu'il n'est pas destiné à des personnes de moins de treize ans ».

[319] RLRQ *c P-401, r 3*, art 87 à 91.

[320] Office de la protection du consommateur du Québec, *Publicité destinée aux enfants - Guide d'application des articles 248 et 249 Loi sur la protection du consommateur*, 2012.

[321] *Ibid*. « les nouveaux supports et médias qui voient le jour, selon les changements apportés aux pratiques publicitaires et aux supports technologiques, sont aussi touchés ».

[322] *Ibid* à la p 3.

[323] *Ibid* aux pp 4-5. « La loi prévoit également trois critères, qui se traduisent par les questions suivantes: • À qui le bien ou le service annoncé est-il destiné? Est-il attrayant pour les enfants? • Le message publicitaire est-il conçu pour attirer l'attention des enfants? • Les enfants sont-ils visés par le message ou exposés à celui-ci? Sont-ils présents au moment et à l'endroit de sa parution ou de sa diffusion? »

vidéo[324]. Mais c'est un fait que les agences de publicité ont profité des technologies sophistiquées pour améliorer les mécanismes de publicité et aussi commercialiser leurs produits ou services sans que l'utilisateur, qu'il soit adulte ou mineur ne puisse s'en rende compte.

C'est ainsi que nous trouvons que les grandes marques de produits pour enfants font usage de la « *publicité immersive* » pour commercialiser leurs produits ou services, au moyen de jeux en ligne interactifs, applications, participation aux activités et tirages au sort en ligne ou via les réseaux sociaux, et ce, afin de fidéliser les mineurs à leur marque[325].

L'une des méthodes de *publicité immersive* les plus connues sont les « advergames », qui font référence aux « jeux en ligne interactifs centrés sur des marques, des produits ou des personnages liés à une marque »[326]. En ce qui concerne les réseaux sociaux, avec eux sont apparus les célèbres *Youtubers*, *influenceurs*, *blogueurs*, *Tiktokeurs* qui, dans la plupart des cas, sont rémunérés par la marque et/ou par le réseau social pour qu'ils recommandent et donnent leur avis sur leurs produits (jouets, jeux vidéo, musique, nourriture, etc.) ou services[327], sans que le mineur comprenne ou ne se rende compte que c'est de la publicité.

Il est donc clair que les mineurs sont facilement influencés par toutes ces annonces et recommandations, qui, bien qu'elles ne soient pas étiquetées comme publicité, peuvent avoir le même but de la publicité directe, à savoir, un but commercial.

Toutefois, le plus grand risque que présente la publicité immersive pour la vie privée et les données personnelles des mineurs est la capacité technologique qui permet de collecter et de

---

[324] IS4K, « Menores de edad y la publicidad en Internet », (17 décembre 2018), en ligne: *Internet Segura Kids* <https://www.is4k.es/blog/menores-de-edad-y-la-publicidad-en-internet>; Habilo médias, *Marketing en ligne destiné aux jeunes : stratégies et techniques*, Habilo médias, 2012.
[325] Habilo médias, *supra* note 324.
[326] *La publicité destinée aux enfants : Identifier la meilleure protection possible*, par Option consommateurs, Montréal, Québec, Bureau de la consommation d'Industrie Canada, 2008 à la p 46.
[327] « Comment les spécialistes du marketing ciblent les enfants », (25 mai 2012), en ligne: *HabiloMédias* <https://habilomedias.ca/litt%C3%A9ratie-num%C3%A9rique-et-%C3%A9ducation-aux-m%C3%A9dias/enjeux-des-m%C3%A9dias/publicit%C3%A9-et-consommation/comment-les-sp%C3%A9cialistes-du-marketing-ciblent-les-enfants>; Jean Siag, « Montrez-moi cette pub que je ne saurais voir ! », *La Presse+* (23 mai 2016), en ligne: <https://plus.lapresse.ca/screens/859375cb-a6d8-425c-bd30-a8361299c173__7C___0.html>.

stocker automatiquement des informations, l'interconnecter et l'utiliser à l'insu pour créer le profil du mineur et lui présenter une publicité personnalisée[328].

L'Organisation de coopération et de développement économique (ci-après « OCDE ») a déjà indiqué ce qui suit :

> « Pressés de commencer un jeu ou de participer à un concours, les enfants acceptent souvent de répondre en ligne à toutes les questions que l'on peut poser sur eux-mêmes ou leur famille sans attendre d'avoir l'autorisation de leurs parents. Les sites peuvent aussi enregistrer et observer les données retraçant la succession des clics de souris durant l'interaction de l'enfant avec le site; cela leur permet de deviner son personnage publicitaire ou son type de céréales favori en notant la fréquence et la durée de ses activités liées à un certain produit. Toutes ces informations peuvent être compilées pour former des profils personnels détaillés et servir à la conception de publicités personnalisées visant un enfant particulier »[329]

La LPCQ interdit toute publicité à des fins commerciales aux moins de 13 ans, mais en réalité la publicité immersive et la publicité comportementale (PCL) impliquent un anonymat implicite non seulement vis-à-vis des mineurs mais aussi vis-à-vis de l'application de la loi. Il est vraiment difficile pour les mineurs de se rendre compte qu'ils font l'objet d'une surveillance continue de la part de ces organisations publicitaires[330].

En outre, il importe de noter que la LPRPSP ne fait pas de distinction entre adultes et mineurs et que, par conséquent, l'obtention du consentement du mineur ou du représentant de l'autorité parentale est en jeu. La violation des deux régimes (LPRPSP et LPCQ) est absolue, d'une part, le mineur reçoit sous une forme déguisée une quantité de publicité commerciale et, d'autre part, des données personnelles du mineur sont recueillies sans que le consentement correspondant ait été obtenu. Mais comment obtenir le consentement éclairé, s'il n'a pas été bien informé?[331]

---

[328] Option consommateurs, *supra* note 290 à la p iv. « la Publicité comportementale en ligne (PCL), une forme de publicité dans laquelle on dresse le profil d'un internaute à partir de ses activités de navigation d'afficher des annonces et correspondant sur les sites qu'il fréquente ».

[329] OCDE, Comité de la politique, *La publicité et le marketing en ligne visant les enfants.* Document de travail n°. 46, n° de doc DSTI/CP (99)1 45 (1999) à la p 6. En ligne : : http://dx.doi.org/10.1787/236503518832

[330] Commissariat à la protection de la vie privée du Canada, *supra* note 296. « La situation est particulièrement épineuse dans le cas des enfants, qui sont de plus en plus jeunes à naviguer le Web et qui ne savent pas qu'ils font l'objet d'un suivi et encore moins de publicités ciblées. L'obtention d'un consentement valable conformément à la loi n'est pas chose facile ».

[331] Vincent Gautrais et Adriane Porcin, « Les 7 pêchés de la LPC : actions et omissions applicables au commerce électronique » (2009) 43:3 Thémis (R.J.T) 559 à la p 588.

La CPVP s'est également prononcée, dans les *Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne* par rapport au consentement exigé par la LPRPDE et les mineurs, en indiquant que :

« La LPRPDE exige un consentement éclairé pour la collecte, l'utilisation et la communication de renseignements personnels. Il serait difficile d'obtenir le consentement éclairé d'un enfant à des fins de pratiques de publicité comportementale en ligne. Par conséquent, et comme pratique exemplaire, les organisations devraient éviter de suivre les enfants ou les sites Web destinés aux enfants »[332].

Eu égard à ce qui précède, on considère que la *Loi sur la protection du consommateur* du Québec devrait être modifiée de manière à interdire[333] aux agences de publicité et de marketing d'inclure sur les sites Web ou les services de la société de l'information destinés aux enfants de moins de 13 ans ou ayant connaissance de l'utilisation de leurs sites ou services par des mineurs, l'inclusion de toute technologie permettant de suivre[334] et de fournir les PCL ou toute nouvelle méthode de publicité en ligne[335]. En outre, il est fortement recommandé, en ce qui concerne la PCL, de modifier la LPCQ afin d'y inclure des conditions spécifiques concernant la PCL présentée aux jeunes de 13 à 18 ans.

En bref, la LPCQ montre l'importance de protéger les droits des mineurs, en tenant en compte que la violation à ses droits peut arriver d'une manière plus facile que chez les adultes, car ils n'ont pas la maturité ni la capacité adéquate de discernement pour prendre des décisions sans que celles-ci ne soient induites par la publicité, ce qui s'applique dans le même sens à des renseignements personnels. Toutefois, compte tenu des progrès technologiques et des nouvelles formes de publicité, il est nécessaire de l'introduire dans un processus de mise à jour afin de garantir les droits des mineurs[336] et d´interdire « explicitement que la publicité en ligne destinée aux enfants de moins de treize ans est interdite »[337].

---

[332] Commissariat à la protection de la vie privée du Canada, *Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne* , 2015 , Last Modified: 2015-12-17.
[333] Bureau de l'Ombudsman et du défenseur des enfants et de la jeunesse, *supra* note 100 à la p 16.
[334] Commissariat à la protection de la vie privée du Canada, *supra* note 296.
[335] Vincent Gautrais et Adriane Porcin, « Les 7 pêchés de la LPC », *supra* note 331 à la p 590.
[336] Option consommateurs, *supra* note 326 à la p 48.
[337] Gautrais, *supra* note 314 à la p 65.

Titre 2 – Cadre légal étranger

Compte tenu des différences marquées entre l'Europe et les États-Unis en ce qui concerne le traitement du droit à la vie privée et la protection des données des mineurs en ligne, la présente section donne un bref aperçu des deux juridictions. Ces deux modèles, comme celui du Canada, ont progressivement progressé dans leurs normes en incorporant des principes et concepts fondamentaux, afin de reconnaître la vulnérabilité des enfants lorsqu'ils utilisent Internet, notamment parce qu'ils ne connaissent pas et ne comprennent pas les risques d'utilisation abusive de leurs informations personnelles.

À cet égard, dans le cadre de cette étude comparative, nous présenterons spécifiquement la COPPA des États-Unis (Children's Online Privacy Protection Act 1998) dans le premier chapitre et le RGPD (Règlement général (UE) 2016/679 sur la protection des données de l'Union européenne) au chapitre 2.

Compte tenu du fait que ces deux règles régissent le traitement des données à caractère personnel des mineurs en ligne, nous procéderons à un rapprochement normatif des modèles et des normes de chaque législation et réglementation, nous mettrons en évidence les points communs et les différences d'approche, nous présenterons les lacunes des normes les plus importantes, nous analyserons les problèmes conceptuels, les défis et les risques auxquels les enfants sont exposés, et enfin, nous adapterons les systèmes juridiques pour surmonter la fragmentation entre le droit et les progrès technologiques, et protéger la vie privée de même que les données personnelles des mineurs connectés.

Les modèles de protection des données personnelles des États-Unis et de l'Union européenne ont inspiré le traitement juridique de la confidentialité des informations au niveau mondial. On peut citer à titre d'exemple le PL64 au Québec, dont les énoncés s'inspirent du règlement de l'Union européenne sur la protection des données. Mais surtout, ils ont été une référence précieuse dans la construction du droit à la protection des données personnelles des mineurs sur Internet.

Chapitre 1 – États-Unis : Children's Online Privacy Protection Act (COPPA)

Dès la fin du XIXe siècle, et en particulier depuis le début du XXe siècle, le législateur américain se préoccupe de la vie privée des mineurs sur Internet, ce qui s'est traduit par la promulgation, le 12 octobre 1998, « *The Children's Online Privacy Protection Act, 1998* » (ci-après « COPPA »)[338], entré en vigueur le 21 avril 2000 et par la suite, en procédant à la révision et à la modification de la loi dans le but de répondre aux évolutions de la société numérique.

Cette loi fait suite à un rapport réalisé en 1996 par *l'Association Center for Media Education*, intitulé « *Web of Deception: Threats to Children from Online Marketing* »[339] qui avait pour objet d'analyser les pratiques de collecte et d'utilisation des données des mineurs sur Internet. À la suite du rapport, la *Federal Trade Commision* (FTC)[340] a enquêté sur le site « *Kidscom.com* » pour violation de la Section 5 du *Federal Trade Commission Act* (FTC Act) sur « *Unfair or Deceptive Acts or Practices* »[341]. À l'issue de ses recherches, en mars 1998, la FTC a présenté au Congrès des États-Unis un rapport intitulé « *Privacy Online: A Report to Congress* »[342], dans lequel elle a conclu qu'il était nécessaire d'engager une action en justice pour protéger les données des mineurs.

La loi COPPA, contenue dans le chapitre 91, titre 15 du *United States Code* (U.S.C) est en vigueur depuis plus de 20 ans, protégeant les informations personnelles des mineurs lorsqu'ils naviguent sur Internet à travers un modèle adaptable à d'autres régimes nationaux (*Privacy Rights*

---

[338] *Children's Online Privacy Protection Act*, *supra* note 38.
[339] Center for Media Education, « Web of Deception: Threats to Children from Online Marketing », (1996), en ligne: *Democraticmedia* <https://www.democraticmedia.org/article/web-deception-landmark-1996-report-triggered-coppa>.
[340] « COPPA désigne la FTC comme autorité compétente pour administrer et exécuter la loi à travers le développement et l'application de la réglementation, et de l'approvisionnement des règles « refuge » (or « *Safe Harbor* » en anglais) pour promouvoir l'autoréglementation du secteur et pour approuver les lignes directrices des programmes ». La FTC, conformément à son dessein, a publié comme législation secondaire la « Children's Online Privacy Protection Rule », qui figure à l'article 312 du titre 16 du « Code of Federal Regulations (16 CFR § 312) » des États-Unis. La règle de protection est entrée en vigueur le 21 avril 2000 et a fait l'objet d'une modification substantielle en 2013.
[341] « FTC Staff Sets Forth Principles For Online Information Collection From Children », (16 juillet 1997), en ligne: *Fed Trade Comm* <https://www.ftc.gov/news-events/press-releases/1997/07/ftc-staff-sets-forth-principles-online-information-collection>.
[342] Federal Trade Commission, « PRIVACY ONLINE: A REPORT TO CONGRESS », (1998), en ligne: <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>.

for California Minors in the Digital World- "Eraser Law")[343] et internationaux (Art 8 GRDP), car il s'agit d'un des premiers outils juridiques centrés sur la protection de la vie privée et des informations personnelles des enfants lorsqu'ils naviguent sur l'Internet.

1.1. Champ d'application

La COPPA a pour principal objectif de protéger la vie privée des enfants de moins de 13 ans dans l'environnement en ligne et de donner aux parents le contrôle de la collecte, de l'utilisation et de la divulgation des données personnelles recueillies auprès de leurs enfants de moins de 13 ans[344] lorsqu'ils utilisent l'Internet.

Plus précisément, la loi interdit les actes et pratiques injustes et trompeuses concernant la collecte et l'utilisation d'informations personnelles sur les mineurs de 13 ans sur Internet, en empêchant les opérateurs de sites web commerciaux de collecter, de conserver et/ou de vendre des informations personnelles fournies par des enfants lorsqu'ils interagissent avec le site web.

Il convient de noter que la COPPA ne s'applique qu'aux informations personnelles collectées en ligne des enfants de moins de 13 ans (et compris les informations personnelles les concernant eux-mêmes, leurs parents, leurs amis ou d'autres personnes), contrairement au RGPD et à la LPRPDE qui s'appliquent également aux informations relatives à une personne et qui sont collectées par des moyens indirects. Cela signifie que la COPPA ne s'applique pas aux informations que le parent ou toute autre personne donne d'un enfant de moins de 13 ans.

Or, le fait que la loi ne s'applique pas aux informations que quelqu'un d'autre fourni du mineur, crée une insécurité juridique dans sa vie privée et dans le contrôle des données, car l'exploitant du site web pourra collecter, utiliser et divulguer l'information d'un mineur sans qu'il soit obligé de se conformer aux dispositions de la COPPA, notamment celles relatives au consentement. Il est donc impératif d'élargir la portée de la loi afin de protéger les données des mineurs et inclure à la fois la collecte directe et indirecte.

[343] *Privacy Rights for California Minors in the Digital World*, California S.B. 568, 22580-82 (2015).
[344] *Ibid*, art §6501 (1) Definitions.

En ce qui concerne la notion de données personnelles, la COPPA les définit comme « individually identifiable information about an individual collected online » [345]. Cette définition standard comprend les principaux éléments de ce que l'on appelle les informations de base d'une personne [346]. La FTC, à travers les dernières modifications apportées en 2013[347] à la « *Children's Online Privacy Protection Rule* »[348] (ci-après « la Règle COPPA »), définit les informations personnelles au sens large, et ajoute à sa définition le terme « *d'identifiant persistant* »[349].

A l´heure actuelle, un projet de loi présenté le 8 janvier 2020 par les représentants Tim Walberg du Michigan et Bobby Rush de l'Illinois, intitulé : « *Preventing Real Online Threats Endangering Children Today* » (« PROTECT Kids Act ») est en cours de révision[350] par le Congrès des États-Unis. Cette loi vise, entre autres, à ajouter dans la définition de l'information personnelle certains services qui ont émergé dans les dernières années par les développements technologiques, donc les services de géolocalisation, les identifiant persistant ainsi que les données biométriques.

En outre, ils cherchent à interdire complètement la PCL pour les enfants de moins de 13 ans, et dans le cas des jeunes (13-17), que le consentement soit demandé. En plus, ils cherchent à

---

[345] *Children's Online Privacy Protection Act*, *supra* note 38, art §1302 (8). *Children's Online Privacy Protection Rule*, 16 CFR §312 1999, art §312.2. Données personnelles : Comprendre le nom et prénom (la date de naissance et le sexe sont exclus); l'adresse du domicile ou autre adresse physique comprenant le nom de la rue et le nom d'une ville ou d'un village où vit le mineur (le code postal ne fait pas partie de la définition); les informations de contact en ligne comme un écran, nom d'utilisateur ou l'adresse courriel (la personnalisation du contenu, le chat filtré, l'affichage public, la communication opérateur-utilisateur ou l'utilisation de noms d'écran pour permettre aux enfants de se connecter à tous les appareils, sont exclus); le numéro de téléphone; le numéro de sécurité sociale; et des informations que l'enfant révèle sur lui-même ou sur sa famille et qui sont associées aux données ci-dessus. Les fichiers photo, vidéo ou audio, qui permettent d'identifier le mineur à travers la reconnaissance vocale ou par l'image du mineur et l´informations de géolocalisation obtenues au moyen de systèmes de positionnement global (GPS),

[346] Federal Trade Commission, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business* , 2013 ch Step 1: Determine if Your Company is a Website or Online Service that Collects Personal Information from Kids Under 13. En ligne: <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>. *Children's Online Privacy Protection Act*, *supra* note 38, art § 2038-§2039.

[347] É-U, Federal Trade Commission, *Statement of basis and purpose: Children's Online Privacy Protection Rule; Final Rule* , 16 CFR §312, vol 78, No. 12, 2013. En ligne: https://www.ftc.gov/system/files/2012-31341.pdf

[348] *COPPA Rule*, *supra* note 345.

[349] Virginia A M Talley, « Major Flaws in Minor Laws: Improving Data Privacy Rights and Protections for Children under the GDPR Note » (2019) 30:1 Indiana Int Comp Law Rev [xi]-162 à la p 145.Un identifiant persistant peut être utilisé pour suivre les activités du mineur au fil du temps via différents sites web et services en ligne. Par exemple, un numéro de client contenu dans un cookie; une adresse IP; un numéro de série d'un équipement, un identifiant unique d'un dispositif. Par conséquent, sont également considérées comme des informations personnelles toutes les informations que l'opérateur recueille en ligne sur le mineur ou les parents et les combine avec un identifiant persistant permettant l'identification ou la localisation du mineur.

[350] É-U, Bill HR 5573, *PROTECT Kids Act*, 116th Cong, 2019-2020. En ligne: <https://www.congress.gov/bill/116th-congress/house-bill/5573>.

inclure quelques paramètres de sécurité par rapport à *l'Internet des objets* (IdO), « permettant aux familles de faire des choix judicieux et sécuritaires dans la sélection des produits »[351].

La collecte d'informations personnelles auprès d'un mineur de moins de 13 ans suit les règles énoncées par la COPPA, mais cette collecte s'opère sans trop de rigidité, souvent en utilisant divers moyens pour y parvenir. Le concept renferme à la fois l'action consistant à demander les données personnelles d'un enfant de moins de 13 ans ou l'encourager à rendre ses données publiques en ligne, et aussi au suivi passif d'un enfant sur l'Internet, par exemple par un identifiant persistant (ex : une adresse IP). Le COPPA ne permet pas la collecte de renseignements personnels des enfants à propos du profilage, de la publicité comportementale ou encore les dispositifs croisés[352].

En tout cas, la collecte des données doit être proportionnée à l'utilisation pour laquelle il est nécessaire sans aucune condition. Ainsi, il est interdit de demander « plus d'informations que celles qui sont raisonnablement nécessaires pour participer à une telle activité » et d'exiger du parent qu'il autorise la divulgation de certaines informations, afin que le mineur puisse accéder à une activité, alors que l'information n'est réellement requise que pour un usage interne.

En outre, en ce qui concerne le champ d'application territorial, il est critiqué que cette loi s'applique aux personnes ou entités relevant de la juridiction des États-Unis, soit parce qu'ils ont leur siège dans le pays, soit parce qu'ils ont leur siège dans un autre pays, mais fournissent des services aux enfants de moins de 13 ans aux États-Unis. Dans la pratique, la FTC n'a jamais pris de mesures d'exécution à l'encontre de sociétés étrangères, et les tentatives pour ce faire montrent qu'elles peuvent être entravées par l'absence de juridiction.

Finalement, d'autres aspects qui sont présentés dans la COPPA et qui sont importants à analyser, sont liés à la majorité d'âge numérique, les services auxquels elle est adressée et le consentement (mécanismes d'obtention, autorité parentale, mécanismes de validation). Dans ce qui suit, nous présentons une brève analyse de ces points

[351] Ariel Fox Johnson, « Improving COPPA: A Road Map for Protecting Kids' Privacy in 2020 and Beyond », (29 janvier 2020), en ligne: <https://www.commonsensemedia.org/kids-action/blog/improving-coppa-a-road-map-for-protecting-kids-privacy-in-2020-and-beyond>.
[352] Talley, « Major Flaws in Minor Laws », *supra* note 349 à la p 148.

1.2. Définition d´enfant : âge numérique

La COPPA définit un enfant comme une personne de moins de 13 ans. Ici on trouve une différence importante avec la LPRPDE, qui en l'absence de toute règle spécifique sur les mineurs, doit se conformer aux règles civiles de capacité et de représentation en général, et aussi aux facteurs subjectifs comme la capacité de compréhension et la maturité du mineur.

Ici se trouve une autre lacune de la COPPA. La loi ne protège que les enfants de moins de 13 ans, car elle les considère moins conscients et plus sensibles. Il est clair que les enfants de moins de 13 ans peuvent avoir cette condition d'immaturité, comme cela a déjà été expliqué dans un autre document, mais il est possible que l'information des mineurs entre 13 et 17 ans (mineurs dans la plupart des législations qui nécessitent généralement le consentement de leurs parents), peut avoir une plus grande valeur commerciale pour les sites web et les applications.

Il convient de noter que, dans les dernières propositions de réforme des règles de la COPPA en 2012, il a été demandé d'élargir la limite d'âge afin de protéger les mineurs de moins de 18 ans. Cependant, la FTC a déclaré que les mineurs âgés de 13 à 17 ans ont plus de facilité pour accéder à l'Internet en dehors de leur domicile, qu'ils sont moins susceptibles de fournir les coordonnées de leurs parents et beaucoup plus de falsifier ces informations ou de mentir sur leur âge[353]. Or, à ce jour, la décision finale appartient au Congrès des États-Unis, étant donné que le projet de loi *PROTECT Kids Act* vise à porter l'âge de la majorité numérique à 16 ans.

On trouve également des positions contre l'efficacité de la norme comme celle de la chercheuse de médias sociaux Danah Boyd, qui critique la façon dont la COPPA tente de protéger la vie privée des enfants de moins de 13 ans, en mettant en évidence le conflit qui peut se produire entre les règles de protection des données et les droits à la liberté d'expression et d'opinion reconnus par le Premier amendement à la Constitution des États-Unis[354]. Toutefois, rappelons-nous que les

[353] Federal Trade Commission, *Proposed Rule; Request for Comment on Proposal to Amend Rule to Respond to Changes in Online Technology: Children's Online Privacy Protection Rule* , 16 CFR §312, vol 76, No. 187, 2013 à la p 59805. En ligne: *Fed Trade Comm* <https://www.ftc.gov/policy/federal-register-notices/16-cfr-part-312-childrens-online-privacy-protection-rule-proposed>.

[354] Danah Boyd et al, « Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act' » (2011) 16:11 First Monday, en ligne: <https://journals.uic.edu/ojs/index.php/fm/article/download/3850/3075>.

adolescents âgés de 13 à 17 ans sont encore en cours de développement[355] et d'exposition numérique sans les contrôles gouvernementaux appropriés, peut être préjudiciable à leur développement en termes de risques physiques et psychologiques qu'ils peuvent rencontrer[356].

1.3. Services concernés

La loi vise[357] tout i) sites web ou services en ligne à des fins commerciales qui s'adressent exclusivement aux enfants de moins de 13 ans; ii) sites web ou des services en ligne qui, bien qu'ils s'adressent à un public en général, ont une connaissance réelle qu'ils collectent des informations personnelles auprès de mineurs.[358] Dans ce cas, ils doivent uniquement notifier et obtenir le consentement des parents des utilisateurs qui s'identifient comme étant âgés de moins de 13 ans et; iii) entreprises qui exécutent un service tiers (tel qu'un réseau publicitaire ou un complément) et recueillent des informations auprès des utilisateurs d'un site ou d'un service destiné aux enfants de moins de 13 ans.

En ce qui concerne le concept de « *services en ligne* », la FTC indique qu'il se réfère à « tout service disponible via Internet, ou qui se connecte à Internet ou à un réseau à grande surface »[359], parmi lesquels elle cite [360]: les applications mobiles qui envoient ou reçoivent des informations en ligne telles que les plateformes de jeux vidéo en ligne, les réseaux sociaux comme *Facebook* et *Instagram* ou encore les applications proposant des publicités comportementales; les services de boutiques en ligne, de publicité, de musique et de vidéos tels que *Spotify* ou *Youtube*; les services de communication vocale et d'imagerie et les services de messagerie comme *Whatsapp*; les services de recherche géolocalisés activés sur internet; les jouets connectés ou autres dispositifs internet des objets; et les haut-parleurs intelligents.

---

[355] Lawford, *supra* note 242 à la p 61.
[356] Donald Gilliland, « It's time to rethink children's privacy protection », (8 août 2020), en ligne: *TheHill* <https://thehill.com/opinion/cybersecurity/511162-its-time-to-rethink-childrens-privacy-protection>.
[357] « Children's Online Privacy Protection Rule: Not Just for Kids' Sites », (2 avril 2013), en ligne: *Fed Trade Comm* <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites>. who's covered by COPPA?
[358] *Children's Online Privacy Protection Act*, *supra* note 38, art §6501 (2) Definitions.
[359] « Complying with COPPA: Frequently Asked Questions », (20 juillet 2020), en ligne: *Fed Trade Comm* <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0>.
[360] Federal Trade Commission, *supra* note 346 ch Step 1: Determine if Your Company is a Website or Online Service that Collects Personal Information from Kids Under 13. En ligne: <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>.

Or, l'application de la règle dans la vie réelle a ses nuances, puisque la notion de si un site ou un service est "dirigé" ou non vers des enfants de moins de 13 ans est bien sûr ambiguë. Bien que la FTC considère que le site web ou service en ligne s'adresse aux moins de 13 ans lorsque plusieurs des facteurs se conjuguent, notamment l'audience prévue du site, le sujet et le contenu visuel qu'il développe, la langue utilisée, l'utilisation de graphismes ou de fonctions destinés aux mineurs, l'utilisation de personnages animés, contenu de musique et/ou audio et présence de célébrités enfantines ou de célébrités qui attirent les mineurs[361].

Le problème est que les sites d'audience générale qui ont « une connaissance réelle » que leurs services sont utilisés par un mineur ignorent délibérément l'âge du consommateur. C'est le cas de YouTube qui a affirmé que ses politiques stipulaient que le service n'est pas destiné aux personnes de moins de 13 ans et que certains de ses acteurs ne savaient pas que son service était attrayant pour les enfants[362].

Il est donc considéré que la COPPA devrait être modifiée dans les termes de la loi « *California Consumer Privacy Act* (CCPA) »[363], qui prévoit explicitement que pour ne pas « ignorer intentionnellement » l'âge d'un consommateur, l'entreprise doit vérifier l'âge une fois qu'elle a des raisons [364] (absence de connaissance réelle) de croire qu'un mineur fait usage de ses services (moins de 16 ans). En ces termes, l'opérateur n'ignore pas délibérément le respect de la loi.

Le projet de loi PROTECT Kids Act propose un standard alternatif basée sur la « connaissance constructive », dans lequel les sites sont responsables d'analyser leur propre base d'utilisateurs pour déterminer s'ils ont des informations destinées aux moins de 13 ans. Pour certains, cela peut être au-delà des capacités de nombreuses petites entreprises

[361] note 359 nº 10.
[362] Stuart Cobb, « It's COPPA-cated: Protecting Children's Privacy in the Age of YouTube » (2021) 58:4 Houst Law Rev 22277 à la p 974.
[363] *California Consumer Privacy Act of 2018 (CCPA)*, Cal AB-375, §1798.100-1798.199 (2018).
[364] *Ibid*, art 1798.120(c).

1.4. Consentement

À l´instar des normes de protection des données d'autres pays, COPPA fonde la protection de la vie privée et la sécurité des données à caractère personnel des mineurs de moins de 13 ans sur les principes des pratiques équitables en matière d'information[365], notamment de publicité, de légalité du consentement préalable du ses parents ou tuteur légal, les droits d'accès et de connaissance des informations personnelles de l'enfant à traiter, les exercices d'effacement des données et le refus du traitement, la confidentialité, la sécurité et l'intégrité des données à caractère personnel.

En ce qui concerne le traitement des données du mineur, l'article 6502 (b.1.B.ii)[366] de la loi COPPA impose l'obligation, à la charge de l'opérateur, d'obtenir le consentement vérifiable des parents avant de recueillir ou de faire usage des informations personnelles d'un mineur de 13 ans.

En tout état de cause, le consentement parental doit être vérifiable, de sorte que le contrôle des informations du mineur incombe à celui-ci. Toutefois, le consentement vérifiable est défini non pas dans l'autorisation elle-même, mais dans l'effort raisonnable pour l'obtenir[367], compte tenu de la technologie disponible. Fait qui nuance considérablement l'obligation de l'opérateur. Toutefois, on trouve plusieurs exceptions aux règles de consentement parental dans la loi[368], À titre d'exemple, lorsque le seul but de la collecte est d'informer et d'obtenir le consentement des parents, quand l'adresse électronique du mineur est recueillie pour des actions concrètes et isolées, lorsqu'un opérateur collecte un identifiant persistant dans le seul but de soutenir le site web ou les opérations internes du service en ligne, quand le but de la collecte est de protéger la sécurité du mineur.

---

[365] Rescue digital media, « Politique de confidentialité », en ligne: <https://fr.rescuedigitalmedia.com/politique-de-confidentialite>. « Les principes des pratiques équitables en matière d'information constituent l'épine dorsale du droit à la vie privée aux États-Unis et les concepts qu'ils contiennent ont joué un rôle important dans l'élaboration de lois sur la protection des données dans le monde entier »

[366] *COPPA Rule*, *supra* note 345, art §312.5 (a.1).COPPA Rule *Ibid*, art §312.5 (a.1).

[367] *Children's Online Privacy Protection Act*, *supra* note 38, art §6502. (8. Personal information) (9. Verifiable parental consent) (10-Website or online service directed to children). (point 8) Personal information, (point 9) Verifiable parental consent et (point 10) Website or online service directed to children.

[368] *COPPA Rule*, *supra* note 345, art § 312.5(c).*COPPA Rule*, *supra* note 313, art § 312.5(c).

Dans le cas des sites web et des services en ligne destinés aux enfants et d'audience mixte, on ne trouve pas de grands problèmes. En ce qui concerne les sites qui s'adressent à un public mixte, le nombre de mineurs, bien que considérable, n'est pas suffisant pour que le site soit catalogué comme s'adressant à des mineurs. Ils doivent demander l'âge à tous ses utilisateurs, et il ne doit pas inclure d'avertissement qui permette au mineur de savoir que certaines fonctionnalités et contenus du site ou des services seront bloqués s'il a moins de 13 ans, étant nécessaire d'inclure des cookies pour bloquer la possibilité de revenir en arrière par le mineur afin changer sa date de naissance.

Bien au contraire, les sites web et des services en ligne destinés à un public en général ne doivent obtenir le consentement du parent que s'il a une « connaissance effective » que les enfants de moins de 13 ans utilisent son site ou son service. D'abord, COPPA établit que pour qu'un site web d'audience générale puisse être considéré comme « destiné à un enfant », il doit être « disponible pour tous les utilisateurs sans restriction d'âge ». En plus, selon COPPA, l'opérateur ne dispose d'une connaissance réelle que son site ou service est utilisé par un mineur, lorsqu'il est informé de l'âge du mineur, ou de son degré scolaire à travers l'enregistrement du mineur ou de son parent ou tuteur. Dans le cas contraire, l'opérateur n'est pas tenu de demander ou de vérifier l'âge du mineur, mais il peut supprimer le « *Veil of Ignorance* »[369] en utilisant des questions proxy pour un âge spécifique, par exemple en demandant au mineur dans quelle année il est scolarisé. À ce sujet, en fonction du contexte et de la validation d'autres exigences, on peut raisonnablement suggérer qu'il s'agit de services offerts aux enfants, même si le contenu et les plans de marketing prévoient un public différent.

§ ***Mécanismes pour obtenir le consentement parental***

À l'égard de l'obtention du consentement parental vérifiable, la règle COPPA dote les opérateurs d'une série de mécanismes pour recueillir le consentement et pour valider le respect légal des conditions du traitement des données. Ainsi, l'exploitant doit choisir une méthode

[369] É-U, Federal Trade Commission, *Statement of Basis and Purpose: Children's Online Privacy Protection Rule; Final Rule* , 16 CFR §312, vol 64, No. 12, 1999 à la p 59893. En ligne: https://www.ftc.gov/sites/default/files/documents/federal_register_notices/childrens-online-privacy-protection-rule-16-cfr-part-312/991103childrensonlineprivacy.pdf

raisonnable pour s'assurer que la personne qui donne le consentement est le parent ou le tuteur, en faisant usage de la technologie disponible.

À cet égard, les mécanismes réglementés par la FTC pour obtenir le consentement consensuel du parent ou qui a l'autorité parentale [370] sont fondés, au début, sur une « *Sliding scale* »[371] qui tient compte de la manière dont les informations sont collectées et de l'utilisation que l'exploitant du site web ou du service donnera aux informations personnelles de l'enfant. Ainsi, des mécanismes plus flexibles (Système de « Email plus » ou de double vérification[372], méthode « *print-and-send consent form* »[373]), sont mis en place si l'information est destinée à l'usage interne de l'entreprise et les données ne seront pas divulguées ou partagées avec des tiers, ou des mécanismes plus robustes (carte de credit, Social Security Number, magasin d'applications public[374], le « *face match to Verified photo Identification* »[375]) si les données du mineur seront communiquées à des tiers ou publiées sur un site web[376].

Or, malgré la liste de méthodes proposées par la COPPA, la mise en œuvre de ces mécanismes est l'un des aspects les plus critiqués. Les opérateurs soulignent que les mesures de réglementation de la FTC visant à vérifier l'âge des mineurs et leur véracité ainsi que l'autorisation

---

[370] Federal Trade Commission, *supra* note 346 ch Step 4: Get parents' verifiable consent before collecting personal information from their kids..

[371] É-U, Federal Trade Commission, *supra* note 317 à la p 3991. Selon la FTC « under the sliding scale, an operator, when collecting personal information only for its internal use, may obtain verifiable parental consent through an email from the parent, so long as the email is coupled with an additional step… The purpose of the additional step is to provide greater assurance that the person providing consent is, in fact, the parent. This consent method is often called ''email plus'' »

[372] É-U, Federal Trade Commission, *supra* note 347 à la p 3991. La FTC « continues to believe that email plus is less reliable than other methods of consent, and is concerned that, twelve years after COPPA became effective, so many operators rely upon what was supposed to be a temporary option ». Par ce système l'exploitant transmet un courriel au compte du parent fourni par le mineur, qui doit donner son consentement dans un message de retour et à travers un autre mécanisme proposé par l'opérateur, soit sous la forme d'un appel téléphonique, un fax, un autre compte courriel ou la confirmation par le biais d'une lettre. Après un délai raisonnable, l'opérateur doit envoyer un autre message en utilisant les coordonnées en ligne des parents pour confirmer le consentement.

[373] L'opérateur transmet un formulaire de consentement, qui doit être signé par le parent et renvoyé par tout moyen.

[374] Il convient de noter que le magasin d'applications n'est pas directement soumis au champ d'application de la COPPA, car ces plates-formes ne sont pas considérées comme des « opérateurs » au regard de la loi. Toutefois, comme ils sont soumis au régime général de protection des consommateurs de la FTC, les personnes visées pourraient être tenus responsables pour avoir induit en erreur ou exercé une surveillance inadéquate sur une application soumise à la COPPA.

[375] Cette méthode est basée sur un processus en deux étapes :1. le parent envoie pour l'authentification une copie d'un document avec photo (permis de conduire, lettre de sécurité sociale, etc.) et 2. le parent doit envoyer une photo improvisée via un appareil mobile ou une webcam, qui sera comparée à la photo d'identité.

[376] Bureau de l'Ombudsman et du défenseur des enfants et de la jeunesse, *supra* note 100 à la p 14.

parentale sont lourdes et moins souples, étant donné que leur mise en œuvre entraîne des coûts élevés[377] pour les entreprises et constitue une barrière à l'entrée pour les nouveaux opérateurs qui n'ont pas la capacité économique de mettre en œuvre ces méthodes dans un premier temps[378].

Face à ces coûts, qui selon certains experts peuvent s'élever à $100.000 USD par an chez un opérateur moyen, certains sites comme Amazon ont décidé de ne pas vendre de produits aux mineurs et d'autres ont été contraints de limiter l'accès aux mineurs de moins de 13 ans et/ou de bloquer des fonctionnalités telles que les salles de chat, comme dans le cas de Disney. Selon Godbey « The goals of COPPA are no doubt admirable. The implementation, however, can be daunting »[379].

Un autre critique est la conséquence directe de la décision des grands opérateurs de limiter l'accès des mineurs à leurs services. Selon les opérateurs et certains rétracteurs de la norme, la COPPA incite les mineurs à commettre des fraudes en les obligeant à mentir sur leur âge et/ou en trouvant le moyen de fournir le consentement paternel à travers l'utilisation de la technologie[380].

Il est clair que ce n'est pas l'objectif de la COPPA, puisque la loi n'interdit en aucun cas aux opérateurs de fournir des services à des mineurs de moins de 13 ans, mais qu'elle réglemente selon les paramètres de la loi la collecte des données des mineurs. Dans ce cas, ce sont les prestataires de services qui limitent les droits des mineurs en n'investissant pas dans l'adaptation de méthodes fiables pour obtenir le consentement des parents des mineurs sans limiter l'accès aux services offerts.

Nous soutenons la position exprimée dans une interview par Alison Pohn, directrice marketing d'un site web pour enfants, en indiquant que, dans la vie offline, toute activité destinée

---

[377] Advertising Education forum, *Children's data protection and parental consent* , Research & Publication, 2013 à la p 18; *The Internet of Children: Protecting Children's Privacy in A Hyper-Connected World*, SSRN Scholarly Paper, by Eldar Haber, papers.ssrn.com, SSRN Scholarly Paper ID 3734842, Rochester, NY, Social Science Research Network, 2020 à la p 1227; Cole Watson, « Protecting Children in the Frontier of Surveillance Capitalism » (2021) 27:2 Stud Scholarsh 1-41 à la p 30; Boyd et al, *supra* note 354.

[378] Danah Boyd et al, « Why parents help their children lie to Facebook about age: Unintended consequences of the ‘Children’s Online Privacy Protection Act&rsquo »; (2011) First Monday, en ligne: <https://firstmonday.org/ojs/index.php/fm/article/view/3850>.

[379] Robert Carson Godbey, « The Law of the Line » *Hawaii Bus* (novembre 2000), en ligne: <https://www.thefreelibrary.com/The+Law+of+the+Line.-a066812174>.

[380] Alliance médias jeunesse, *supra* note 295 à la p 94; Lawford, *supra* note 242 à la p 53; Boyd et al, « Why parents help their children lie to Facebook about age », *supra* note 378.

aux mineurs investit dans les outils et les mécanismes qui garantissent la sécurité du mineur à tout prix[381]. Ne devrait-il pas en être de même pour les services en ligne?

En terminant, rappelons que ces méthodes ne sont pas exhaustives et qu'au moyen de l'autorégulation, les opérateurs pourront demander l'approbation de nouvelles méthodes de consentement parental. À cet égard, ils devront envoyer à la FTC une description détaillée de la méthode à travers laquelle ils obtiendront le consentement des parents, puis cette proposition sera publiée pour recevoir des commentaires du public dans le registre fédéral, et si elle est approuvée par la FTC[382], le fournisseur bénéficiera d'un « safe harbour » [383] de consentement parental[384].

1.5. Conclusion

En résumé, la COPPA renforce les principes de contrôle parental et de vérification du consentement des parents, elle est exhaustive dans ses exigences tout en permettant une mise à jour de celles-ci en fonction du principe de l'effort raisonnable, en tenant compte de la technologie du moment.

Au fil du temps, la FTC a indiqué que la mise en œuvre et la réalisation des objectifs de la COPPA ont été satisfaisantes. À cette fin, la FTC applique des sanctions civiles pour non-respect allant jusqu'à $43,280 USD pour violation. Le montant final de la sanction dépendra d'un certain nombre de facteurs tels que le nombre de mineurs impliqués et/ou la quantité et le type d'informations personnelles recueillies, l'utilisation qui a été donnée à l'information, etc[385]. En 2019, la FTC a condamné *Google* et sa filiale *Youtube* à une amende de 170 millions de dollars pour avoir illégalement collecté des informations personnelles sur des enfants sans le consentement

[381] Melisa Rogers, « Kids' Privacy Act Stings Web » *Crains Chic Bus* (14 mai 2000), en ligne: <https://www.chicagobusiness.com/article/20000514/HOLD/100014067/kids-privacy-act-stings-web-sites>.
[382] Actuellement, la FTC a approuvé 7 programmes de « Safe Harbor » gérés par TRUSTe, Privacy Vaults Online, Inc. (PRIVO), Entertainment Software Rating Board (ESRB), Aristotle International Inc, Privacidad de Samet (kidSAFE), Internet Keep Safe Coalition (iKeepSafe) et Children's Advertising Review Unit (CARU).
[383] É-U, Federal Trade Commission, *supra* note 369, art §312.11. Les « Safe Harbor Programs » permettent aux entreprises ou groupes de développer des codes d'autoréglementation obligatoires pour ceux qui adhèrent (« Self-regulatory Guidelines ») qui précisent les critères pour le traitement des données relatives aux mineurs.
[384] É-U, Federal Trade Commission, *supra* note 347.
[385] note 359.note

de leurs parents[386]. En outre, la plus grande amende de la FTC, est celle imposée à *TikTok* en 2019, pour 5,7 millions de dollars américains[387].

Or, selon les opérateurs, le montant fixé par la FTC est clairement susceptible de faire sortir du marché une petite entreprise et au contraire de favoriser les entreprises à revenus élevés, étant donné que, selon Rohit Chopra, commissaire de la FTC, les grandes entreprises technologiques ne sont pas sanctionnées avec la sévérité suffisante pour leurs violations de la loi par rapport à leurs revenus. Une méthode plus juste est celle proposée dans le RGPD, qui sanctionne les entreprises jusqu'à 4 % de leurs revenus annuels.

Bref, bien que la COPPA ait fait l'objet de nombreuses critiques, il est également vrai que cette loi américaine offre une certitude quant aux exigences légales, mais en même temps elle est flexible et réceptive dans son approche pour faire face aux risques potentiels auxquels le droit à la protection des données des mineurs peut être exposé.

La COPPA a renforcé la protection de la vie privée des mineurs en intégrant des principes de transparence et de vérification du consentement parental, des principes sur la nature de la collecte, de l'utilisation et de la divulgation des données relatives aux mineurs, l'inclusion de limitations substantielles à la collecte de données à caractère personnel, y compris l'incorporation du principe de proportionnalité, une définition claire des sujets cibles de la norme, des méthodes explicites d'obtention du consentement, en permettant aux opérateurs de proposer des mécanismes supplémentaires en tirant parti des nouvelles technologies, des procédures d'accès et de rectification des données, ainsi que des exigences en matière de sécurité et d'intégrité des données.

[386] « Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law », (3 septembre 2019), en ligne: *Fed Trade Comm* <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations>.
[387] Federal Trade Comission, « Largest FTC COPPA settlement requires Musical.ly to change its tune », (27 février 2019), en ligne: *Fed Trade Comm* <https://www.ftc.gov/news-events/blogs/business-blog/2019/02/largest-ftc-coppa-settlement-requires-musically-change-its>.

Chapitre 2 – l'Union européenne : Règlement général (UE) 2016/679 sur la protection des données (RGPD)

Le RGPD en vigueur depuis le 25 mai 2018 établit pour la première fois au niveau communautaire une réglementation spécifique concernant le traitement des données des mineurs en ligne. Ce règlement s'applique non seulement aux États membres, mais aussi aux opérateurs qui ne se trouvent pas sur le territoire de l'Union, mais qui offrent un service ou un produit à l'intérieur de l'Union.

Le règlement reconnaît explicitement que les mineurs ont besoin de plus de protection que les adultes, en établissant au considérant 38 que :

> « 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… ».

De même, le RGPD fait référence au statut spécial des mineurs au considérant 58, en indiquant par rapport au principe de transparence que « …[l]es enfants méritant une protection spécifique… », et aussi au considérant 75[388] en citant les critères d'une approche fondée sur les risques, indique que les enfants sont des personnes physiques vulnérables. S'il est vrai que les considérants ne sont pas contraignants, ils reflètent l'esprit de la réglementation et servent de guide pour l'application des dispositions obligatoires.

Un premier aspect à noter est qu'il n'y a pas de définition « [d']enfant » dans le Règlement, et la seule référence spécifique à l'âge se trouve à l'article 8 concernant l'offre directe de services de la société de l'information et le consentement des parents. Par conséquent, si l'on considère que: i) dans une première version du règlement, le RGPD présente la définition d'enfant, qui fait

[388] *RGPD*, *supra* note 39. considérant 75. « Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier: … lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants… ».

référence à une personne de moins de 18 ans [389]; ii) que dans le guide « *children and the RGPD* »[390] publié par *l'Information Commissioner's Office* du Royaume-Uni (ci-après « ICO UK »)[391] indique qu'un enfant s'entend de toute personne âgée de moins de 18 ans et utilise la définition de la Convention des Nations Unies sur les droits de l'enfant [392] comme référence; et iii) que tous les États membres ont signé la convention.

En principe, on peut conclure qu'à l'exception de l'article 8, toutes les autres dispositions du RGPD qui ont un impact sur les enfants concernent les mineurs de moins de 18 ans ou qui n'ont pas atteint la majorité selon les lois de l'État membre dans lequel ils résident. Or, il est clair que l'UE ne fait pas partie du CIDE et que le RGPD ne la cite nulle part, et des auteurs comme Milda Macenaite et Eleni Kosta considèrent que l'inclusion de l'incapacité légale jusqu'à l'âge de 18 ans peut facilement être considérée comme une surprotection[393].

La question se pose donc de savoir si la définition d'« enfant » donnée dans l'Art. 8 du Règlement peut être étendu à toutes les autres dispositions du RGPD, comme l'interdiction du profilage et le droit à l'effacement[394]. Il s'agit d'un premier aspect qui est considéré important d'être défini par le législateur du RGPD [395]. Il convient aussi de noter que, bien que le terme « enfants » soit utilisé dans le règlement pour désigner les mineurs, nous utiliserons le terme mineur ou enfant de manière indistincte dans ce chapitre.

Le RGPD s'efforce, mais sans être suffisant, de garantir la protection des données relatives aux mineurs. En général, comme on peut le voir, le Règlement comprend plusieurs dispositions

---

[389] C.E, *Proposition de Règlement du Parlement Européen et du Conseil 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 (règlement général sur la protection des données)*, [2012], COM (2012) 11 final, art 4 (18). En ligne : <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012PC0011>.

[390] R-U, Information Commissioner's Office, *Guide: Children and the UK GDPR*, ICO, 2020, publisher: ICO. En ligne: < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/>.

[391] Il convient de préciser que le Royaume-Uni, après un long processus de négociation, a quitté définitivement l'Union européenne le 1er janvier 2021. En revanche, à l'heure actuelle, la loi britannique sur la protection des données et les guides élaborés par l'ICO sont en vigueur. Pourtant, le guide ICO UK qui donne une portée à la réglementation du RGPD concernant les mineurs reste une référence importante au niveau européen. Par conséquent, il sera cité dans ce mémoire.

[392] R-U, Information Commissioner's Office, *supra* note 390.

[393] Macenaite & Kosta, « Consent for processing children's personal data in the EU », *supra* note 78 à la p 152.

[394] *Ibid* à la p 166.

[395] Krivokapic & Adamovic, *supra* note 95 à la p 208.

importantes relatives au traitement des données personnelles des mineurs, qui soulèvent une série de discussions que nous tenterons de présenter dans ce chapitre:

a. L'obligation de fournir aux enfants des informations appropriées, c'est-à-dire des informations concises, transparentes, intelligibles et facilement accessibles, dans un langage clair et simple (considérant 58 et art. 12);
b. L'inclusion d'un droit d'effacement (art. 17 (1)(f) et considérant 65);
c. La protection des mineurs contre la commercialisation et le profilage (considérant 58);
d. L'interdiction des décisions automatisées (considérant 71 et art. 22);
e. Le pouvoir de rédiger, de modifier ou d'étendre des codes de conduite pour l'application du RGPD lors du traitement des données relatives aux enfants et la manière d'obtenir le consentement du titulaire de la responsabilité parentale (ci-après « TRP ») (art. 40 (2)(g));
f. En assignant des tâches aux autorités chargées de la protection des données afin qu'elles développent en particulier des activités visant à sensibiliser les mineurs aux risques et à les faire mieux comprendre, les normes, garanties et droits relatifs au traitement de ses données (art. 57 (1)(b));
g. La condition du consentement des mineurs en ce qui concerne les services de la société de l'information (ci-après « SSI ») (art. 8).

2.1. Article 8

Comme nous l'avons indiqué précédemment, l'article 8 définit les conditions applicables au consentement des mineurs en ce qui concerne les SSI. Il convient de noter que cette disposition ne s'applique en principe qu'aux services en ligne destinés aux enfants. La question se pose donc de savoir si la disposition de cet article est en harmonie avec les autres dispositions du RGPD et peut être appliquée à tout service destiné à un mineur ?

L'article 8 dispose :

> « 1. Lorsque l'article 6, paragraphe 1, point a), s'applique, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant.

Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans.

2. Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles.

3. Le paragraphe 1 ne porte pas atteinte au droit général des contrats des États membres, notamment aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant ».

On procède ensuite à l'analyse de chacun des paragraphes de l'art. 8.

2.2.1 Consentement du mineur (art. 8, paragraphe 1)

Du paragraphe 1 de cet article, nous pouvons identifier plusieurs aspects importants:

a. Base juridique

Les conditions de cet article ne seront applicables que lorsque le consentement est la base juridique retenue pour le traitement des données des mineurs par le responsable (Article 6 (1.a)).

L'article 6 du RGPD exige que chaque opération de collecte et de traitement de données effectuée par les contrôleurs de données soit supportée au moins dans une « base juridique » de la liste de l'article 6. Toute base juridique figurant sur la liste peut être utilisée pour traiter les données relatives aux mineurs dans des circonstances appropriées. Cependant, c'est le contrôleur qui, de manière discrétionnaire et à ses risques, décide quelle est la base juridique à partir de laquelle il traitera les données en fonction de ses opérations.

Dans certaines situations, des conditions particulières sont exigées pour le traitement des données relatives aux mineurs. Conformément à l'article 6, paragraphe 1(a) du RGPD, le consentement est l'une des bases juridiques dont le contrôleur peut se servir pour traiter des données, mais doit être conforme à l'article 8 qui impose des conditions spécifiques applicables au consentement d'un mineur lorsque le responsable utilise le consentement comme base juridique pour le traitement des données liées à l'offre directe d'un service de la société de l'information au mineur.

L'une des conditions applicables à l'article 8 est l'âge. Le consentement n'est licite que si le mineur a 16 ans ou l'âge légal adopté par l'État membre, qui ne sera en aucun cas inférieur à 13

ans. Si le mineur n'a pas l'âge minimum requis, le responsable des données doit obtenir l'autorisation ou le consentement du responsable de l'autorité parentale. Il convient donc de noter qu'à l'exception de la base juridique du consentement, aucune des autres bases juridiques ne renferme de conditions spécifiques permettant de déterminer qui est un mineur. Devons-nous ainsi comprendre que, pour toutes les autres bases juridiques, on entend par « enfant » une personne de moins de 18 ans?

En ce qui concerne les mineurs, une autre base dont le contrôleur peut faire usage (autre que le consentement) est la base juridique d'intérêt légitime du responsable du traitement (article 6, paragraphe 1, point f). Le RGPD prévoit en effet que le traitement est licite lorsqu'il est nécessaire aux fins des intérêts légitimes du responsable du traitement, sauf lorsque ces intérêts sont annulés par les intérêts ou droits fondamentaux de la personne concernée, en particulier lorsque l'intéressé est un enfant[396]. Dans ce cas, le responsable doit prendre en compte le critère d'équilibre afin de garantir la protection des droits des mineurs, car ce qui est considéré comme proportionné ou requis dans le cas des adultes, il peut s'agir d'illégalité ou d'inutilité dans le cas où des données concernant des mineurs sont traitées.

Milda Macenaite et Eleni Kosta notent que, comme le législateur limite les motifs d'intérêt légitime pouvant être invoqués par les responsables de données, cette base juridique peut protéger les enfants plus que la confiance dans le consentement si le responsable des données prend en compte des facteurs tels que « the nature and source of the legitimate interest, the aim of the data processing, the impact on children and their reasonable expectations, additional safeguards to limit undue impact on children »[397].

Cette déclaration est tout à fait discutable. L'utilisation de la base juridique de l'intérêt légitime ne garantit pas que les mineurs sont mieux protégés, car un contrôleur peut affirmer que leur intérêt commercial légitime pour recueillir les données du mineur dépasse les droits à la vie privée[398]. Dans ce cas, la charge de la preuve d'un traitement inapproprié incombe à la personne concernée et ne garantit pas que le contrôleur cesse le traitement. En revanche, si la personne concernée n'est pas d'accord avec le traitement de ses données lorsque la base juridique est le

[396] *The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society. Roundtable Report.*, by Ingrida Milkaite et al, 2017 à la p 12.
[397] Macenaite & Kosta, « Consent for processing children's personal data in the EU », *supra* note 78 à la p 172.
[398] Talley, « Major Flaws in Minor Laws », *supra* note 349 à la p 150.

consentement, alors elle va tout simplement retirer l'autorisation, ce qui oblige à cesser immédiatement le traitement des données.

En plus de la base de consentement et d'intérêt légitime, le contrôleur ou responsable de données peut être couvert par la base juridique contractuelle comme base pour le traitement des données du mineur (art. 6 al. 1 lit. b). Par exemple, la vente d'un livre en ligne : certaines données de base telles que nom, prénom, adresse d'envoi, « seraient nécessaires à l'exécution d'un contrat auquel l'intéressé est partie »[399]. Dans ce cas, il incombe au contrôleur de vérifier si l'enfant est compétent pour conclure des contrats conformément au droit des États membres. Toutefois, dans le même cas que la vente du livre, si le contrôleur exige également l'adresse électronique pour envoyer des informations ou de la publicité[400], il doit obtenir aussi le consentement du mineur ou du titulaire de la responsabilité parentale s'il est âgé de moins de 16 ans.

Dans tous les cas, le RGPD laisse ouverte à l'interprétation et au choix du contrôleur comme, quand et quelle base juridique il veut utiliser pour traiter les données des mineurs. Il est donc nécessaire de définir des paramètres relatifs à l'âge, au-delà des lignes directrices ou des guides des commissions d'information des États membres, et les conditions d'utilisation des autres bases juridiques dans l'événement qui sont appliquées pour traiter les données des mineurs.

b. Définition du « service de la société de l'information » (SSI)

Aux termes de l'article 4 (25) RGPD, les SSI doivent être entendus au sens de l'article 1(1.b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil [401]. En considération, nous devons comprendre comme SSI « tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services ». La définition est large et vise à couvrir la plupart des services fournis numériquement, tels que les sites web, les applications, les moteurs de recherche, les marchés en ligne, les services de contenu en

[399] *RGPD*, *supra* note 39., Considerant 40.
[400] Federica Persano, « GDPR and Children Rights in EU Data Protection Law » (2020) 2020: Special Issue Eur J Priv Law Technol EJPLT 32-42 aux pp 39-40.
[401] CE*, Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015, prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (texte codifié)*, 2015 JO L2411, art 1 (1(b)). En ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015L1535&from=FR>.

ligne, les appareils sans écran, etc. Les réseaux sociaux, les jeux en ligne et les magasins web sont des exemples de services de la société de l'information.

Pour sa part, la *Cour de justice de l'Union européenne* (ci-après « CJUE ») a déclaré que les contrats et autres services conclus ou transmis en ligne font également partie des SSI [402]. On peut lire dans les lignes directrices 5/2020 sur le consentement du *Comité européen de la protection des données* (ci-après « CEPD ») que, si un service a deux éléments qui sont économiquement indépendants, et l'un est un élément en ligne, seul celui-ci sera considéré comme un SSI aux termes de l'art. 8 du règlement[403]. Or, dans l'arrêt de 2017, la CJUE concernant les services de partage de point à point qui fonctionne par une application basée sur le lieu, a soutenu qu'ils étaient considérés comme un SSI [404]. Il a précisé dans l'affaire contre *UBER* que la composante principale du service était le transport et que l'application en ligne faisait partie intégrante du service général. Aspect fondamental à prendre en compte par les prestataires de services à composantes multiples, notamment par les sites de commerce électronique où l'un des composants est développé par des dispositifs connectés[405].

En outre, la définition de SSI de l'article 8 à l'étude renferme comme condition que le service soit rendu contre « rémunération ». Le terme de rémunération doit être interprété au sens large car, en règle générale, la plupart des SSI ne requièrent pas de frais pour que le destinataire puisse accéder au service; ces prestataires obtiennent une rémunération pour d'autres types d'accords avec d'autres entreprises, par exemple à travers la publicité. À cet égard, la CJUE s'est prononcée en indiquant que ce n'était pas le destinataire du service qui devait nécessairement donner la rémunération, mais qu'il fallait tenir compte du fait que le prestataire a reçu une rémunération pour le service[406].

---

[402] *Ker-Optika bt c ÀNTSZ Dél-dunántúli Regionális Intézete*, C-108/09, [2010] Rec CE I-12213 nos 22 et 28 [*Ker-Optika contre ÀNTSZ*]. En ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A62009CJ0108>.
[403] C.E, Comité européen de la protection des données*, Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679*, 2015 JO L2411 2020 no 129.
[404] *Asociacion Profesional Elite Taxi c Uber Systems Spain SL*, Rec CE général (partie « Informations sur les décisions non publiées ») no 40 [*Elite Taxi c Uber Systems Spain*]. En ligne: <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A62015CJ0434>.
[405] Centre for Information Policy Leadership, *GDPR Implementation in Respect of Children's Data and Consent*, 2018 à la p 8.
[406] *État belge c René Humbel et Marie-Thérèse EdeL*, C-263/86, [1988] Rec CE 1988-05365 [*État belge c Humbel et EdeL*]; *Bond van Adverteerders et autres c État néerlandais*, C-352/85, [1988] Rec CE 1988-02085 [*Bond van*

Enfin, il convient de rappeler que la fourniture de services de prévention ou de conseil directement à un enfant ne nécessite pas le consentement ou l'autorisation du TRP et ne relève donc pas du champ d'application de l'art. 8 du RGPD. Toutefois, cela ne signifie pas que si ces services répondent aux critères énoncés dans la directive 2015/1535 1 (1.b), il s'agira donc d'un SSI et d'une autre base juridique pouvant également être utilisée pour le traitement des données.

c. Service offert « directement » aux mineurs

L'article 8 du RGPD s'applique aux services de la société de l'information qui sont offerts directement à l'enfant, mais le règlement ne contient pas une définition de « offert directement ».

Par conséquent, il est clair que les services conçus et dirigés intentionnellement pour les enfants entrent dans le champ d'application, et que les services conçus exclusivement pour les plus de 18 « fermés par l'âge dur » (comme les casinos en ligne ou d'autres jeux de hasard) sont exclus de l'application de l'art. 8.[407] Cependant, à différence de la COPPA, il n'y a pas de clarté en ce qui concerne les services d'audition mixte ou généraux. Des services que, bien qu'ils ne s'adressent pas explicitement aux mineurs, ne les excluent pas non plus directement et, d'une certaine manière, le prestataire peut apprendre que les mineurs en font également usage.

Toutefois, il est de notoriété publique que les services destinés directement aux mineurs ne représentent qu'une partie de l'ensemble du service auquel ils ont accès quotidiennement. Parmi les sites les plus populaires, on trouve des réseaux sociaux, comme Facebook, Youtube et Instagram, services destinés à un public mixte. Par conséquent, une fois obtenu le consentement du mineur qui a atteint l'âge de la majorité numérique, il recevra les mêmes informations et paramètres pour le traitement des données qu'un adulte, dont la collecte et l'utilisation de ses données ne seront pas adaptées à son âge. La situation est plus grave lorsque le mineur atteint la majorité numérique à un âge plus précoce comme les 13 ans.

À l'heure actuelle, une solution peut être trouvée dans le guide *« children and the RGPD* » de l'ICO UK, qui indique que tout SSI mis à la disposition d'une audience générale est réputé être

Adverteerders c État néerlandais]. En ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A61986CJ0263> et <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A61985CJ0352>, respectivement.

[407] Centre for Information Policy Leadership, *supra* note 405 à la p 9.

offert directement à un mineur quand « it is made available to all users without any age restrictions or when any age restrictions in place allow users under the age of 18 ».[408]

Il est évident que l'ICO UK, à travers le guide précité, élargit le champ d'application de l'art. 8 du règlement et couvre plus de SSI. Certaines entités considèrent que ce concept est trop large, notamment parce qu'il couvrirait des SSI « without stringent age verification mechanisms in place, even where the service is agnostic towards the age of its users (for example, in cases of OTT messaging or email services) »[409].

Cependant, nous estimons qu'en établissant des paramètres raisonnables pour la vérification, il sera possible de trouver un équilibre dans l'application de la norme en ce qui concerne les SSI à audience générale, mais en particulier pour protéger les droits des mineurs. Il s'agit tout d'abord de déterminer si l'important est de valider l'âge des utilisateurs du service ou si le service est offert directement ou mis à la disposition d'un mineur.

La première approche, qui est celle adoptée par l'ICO UK, exige que l'âge soit validé pour tous les SSI qui ne sont pas sûrs si leurs services sont utilisés par des mineurs. L'ICO UK propose une approche prudente fondée sur le risque, toujours en pensant à la tranche d'âge cible pour le traitement des données et à la possibilité pour les mineurs en dehors de cette tranche d'âge de fournir leurs données personnelles[410].

Les détracteurs de cette approche fondée sur la validation de l'âge indiquent qu'il sera toujours nécessaire de recueillir des données auprès des personnes, si elles indiquent qu'elles ont l'âge de la majorité numérique, et donc cette situation serait contraire au principe de minimisation des données. Ils indiquent également que si le RGPD avait voulu inclure cette obligation, il l'aurait établi ainsi que les efforts raisonnables pour valider le consentement donné par le TRP[411].

La seconde approche consiste à interpréter au sens strict l'expression « SSI offerts directement à un enfant » et, par conséquent, seulement dans le cas où le contrôleur déclare qu'il s'adresse aux mineurs, il devra valider l'âge de ses utilisateurs. Toutefois, comme le prévoit la

[408] R-U, Information Commissioner's Office, *supra* note 390.
[409] Centre for Information Policy Leadership, *supra* note 405 à la p 10.
[410] R-U, Information Commissioner's Office, *supra* note 390 à la p 13."
[411] Centre for Information Policy Leadership, *supra* note 405 à la p 11.

COPPA, il ne suffit pas de déclarer que le service n'est pas destiné aux mineurs, car certains services sont conçus pour attirer intentionnellement les mineurs, et s'adresse donc aussi à des opérateurs qui savent réellement qu'un utilisateur de services est âgé de moins de 13 ans[412].

À cet égard, il est important d'établir des critères permettant au responsable du service de valider si son service à audience générale ou une partie de son service s'adresse ou non à un mineur.

d. Âge du consentement numérique et méthodes de vérification de l'âge

Aux fins de l'article 8, on entend par « enfants » les mineurs de moins de 16 ans. Toutefois, le RGPD donne aux États membres la possibilité de fixer un âge légal différent, à condition que celui-ci ne soit pas inférieur à 13 ans. En conséquence, la collecte ou le traitement des données relatives aux enfants de moins de 16 ans, ou selon la définition de chaque État membre, ne sera licite que si le titulaire de la responsabilité parentale donne ou autorise le consentement sur les données relatives à l'enfant, et seulement dans la mesure où il a été donné ou autorisé par celui-ci. Dans le cas où les données collectées en ligne sont destinées à des services de prévention ou de conseils offerts directement aux mineurs, le consentement du TRP ne sera pas nécessaire[413].

Or, il n'y a pas d'uniformité en ce qui concerne l'âge minimum du consentement au traitement des données relatives aux mineurs lorsque des SSI sont offerts[414].

Il est évident qu'il n'existe pas de consensus unifié entre les États. Par conséquent, les controverses concernant le pouvoir discrétionnaire dont disposent les États membres pour choisir indifféremment un âge de consentement au seuil proposé par le règlement ne se sont pas fait attendre. Certains des arguments avancés portent sur les conflits de lois et sur le fait que « the lack of consistency of ages is a significant barrier for companies »[415].

---

[412] Milkaite et al, *supra* note 396 à la p 19.
[413] *RGPD*, *supra* note 39. Considérant 38
[414] Talley, « Major Flaws in Minor Laws », *supra* note 349 aux pp 155-156.
[415] Jasmine Park, « The European Commission Considers Amending the General Data Protection Regulation to Make Digital Age of Consent Consistent - Future of Privacy Forum », en ligne: *https://fpf.org/* <https://fpf.org/blog/the-european-commission-considers-amending-the-general-data-protection-regulation-to-make-digital-age-of-consent-consistent/>; *Kids, Privacy, Free Speech & the Internet: Finding the Right Balance*, SSRN Scholarly Paper, by Adam D Thierer, papers.ssrn.com, SSRN Scholarly Paper ID 1909261, Rochester, NY, Social Science Research Network, 2011 à la p 13.

En ce qui concerne les barrières à l'entrée, les prêteurs de SSI devront investir des sommes d'argent élevées pour implémenter, acquérir et mettre en place des mécanismes permettant de vérifier le seuil minimal autorisé pour les mineurs conformément à chaque norme nationale en vigueur. Ils doivent en outre valider la nationalité et inclure des paramètres permettant de déterminer si l'enfant peut donner son consentement selon la législation de cet État membre et, s'il n'atteint pas l'âge minimum pour pouvoir donner son consentement de manière autonome, le consentement du TRP doit être obtenu.

Cela présuppose, selon certains auteurs[416], un désavantage concurrentiel qui empêche l'entrée de nouveaux fournisseurs qui préféreront renoncer au développement de SSI pour mineurs[417], ou obliger d'autres prestataires à limiter les services offerts uniquement pour les personnes âgées de plus de 16 ans, ce qui se traduit également par une limitation des services destinés aux mineurs[418].

De son côté, la Commission européenne, dans son communiqué du 24 juin 2020, par lequel elle présente le résultat de l'évaluation des deux premières années de validité du RGPD, est consciente de cette problématique en précisant que « [p]our garantir le bon fonctionnement du marché intérieur et éviter qu'une charge inutile pèse sur les entreprises, il est également essentiel que la législation nationale n'aille pas au-delà des marges fixées par le RGPD et n'introduise pas d'exigences supplémentaires lorsqu'aucune marge n'a été fixée »[419].

En plus des barrières d'entrée, nous trouvons la deuxième controverse. Nous parlons des conflits d'application des lois des États membres. Ces conflits sont inévitables, car il n'est pas clair quel âge doit être pris en compte par les contrôleurs qui fournissent des services transfrontaliers, notamment si le responsable devait adapter ses paramètres au pays où il fournissait ses services ou le pays dans lequel réside le mineur. Cette question a été examinée par un groupe d'experts des

[416] Talley, « Major Flaws in Minor Laws », *supra* note 349.
[417] *Ibid* à la p 159.
[418] Macenaite & Kosta, « Consent for processing children's personal data in the EU », *supra* note 98 à la p 192.
[419] CE, *Communication de la Commission au Parlement européen et au Conseil : La protection des données: un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique - deux années d'application du règlement général sur la protection des données*, [2020], JO, C 264/2020 final à la p 8. En ligne : <https://op.europa.eu/es/publication-detail/-/publication/ccb3dc23-b6d5-11ea-bb7a-01aa75ed71a1/language-fr>.

États membres et par le comité européen de la protection des données. À cet égard, deux critères de rattachement ont été initialement proposés [420]:

a. Critère d'établissement : l'État membre dans lequel le responsable du traitement fournit le service pourrait accepter la limite d'âge de l'État membre dans lequel le responsable du traitement est établi, si bien que la limite d'âge est inférieure.

   Nonobstant, si le responsable du traitement est situé dans un autre État membre où il fournit le service, ou s'il déménage son siège dans un autre État membre afin de contourner la limite d'âge parce qu'elle lui est plus bénéfique, mais n'offre de services qu'aux résidents de l'État membre d'où il s'est déplacé, la limite d'âge fixée par l'État membre dans lequel le service est effectivement fourni s'applique à cet événement.

b. Critère de résidence : la loi que doit appliquer le prestataire de services est celle en vigueur sur le territoire de résidence de celui qui reçoit le service, quelle que soit l'origine du service.

Le *Comité européen de la protection des données* précise au paragraphe 131 des lignes directrices que les États membres, lorsqu'ils procèdent à l'analyse pour sélectionner l'un des critères, devront harmoniser leur décision avec le principe de « l'intérêt supérieur de l'enfant ».

En outre, il s'agit de services transfrontaliers offerts par des entreprises établies dans l'UE. Mais rappelons-nous que le RGPD est également applicable aux entreprises qui n'ont pas de siège dans l'UE traitent les données des résidents de l'UE. Dans ce cas, certaines de ces entreprises choisiront de ne fournir de services que dans les États membres qui ont choisi le même âge pour éviter de faire des investissements élevés ou de ne pas respecter le RGPD, ou limiteront le service à ceux qui ont atteint le seuil le plus élevé. *Whatsapp* est un bon exemple, cette entreprise a choisi d'autoriser le service en Europe seulement pour les mineurs qui ont plus de 16 ans[421].

Comme on le constate, la diversité dans l'âge de consentement choisi par chaque État membre en ce qui concerne les SSI destinés aux enfants est un sujet qui, dans la pratique, peut poser des problèmes d'interprétation et d'application de la loi. À cet égard, la Commission européenne a indiqué que:

[420] Milkaite et al, *supra* note 396 à la p 9; *Lignes directrices sur le consentement*, *supra* note 403 à la p 31.
[421] Persano, *supra* note 400 à la p 38.

> « [L]es différences entre les États membres au sujet de l'âge de consentement des enfants en ce qui concerne les services de la société de l'information créent une incertitude pour les enfants et leurs parents quant à l'application de leurs droits en matière de protection des données dans le marché unique. »[422]

On lit également dans le communiqué que le Règlement autorise un degré de fragmentation par l'inclusion de clauses facultatives permettant ainsi aux États membres de légiférer sur certains aspects ou de préciser davantage la disposition du RGPD, ce qui « crée aussi des difficultés en ce qui concerne l'exercice d'activités internationales dans l'UE, l'innovation, en particulier les nouvelles évolutions technologiques, et les solutions en matière de cybersécurité »[423]. Et conclut qu'il pourrait être utile d'harmoniser l'âge du consentement des mineurs [424].

Enfin, il est nécessaire d'unifier l'âge de la majorité numérique à l'intérieur des États membres, pour donner une plus grande sécurité juridique aux contrôleurs, mais surtout pour protéger les droits des mineurs. Aujourd'hui, nous devons nous demander si un enfant qui a atteint l'âge de la majorité numérique obtient réellement les garanties légales suffisantes pour la protection de ses droits ? Ce n'est évidemment pas le cas.

§ Méthodes de vérification de l'âge

Le RGPD comme les législations précédemment étudiées ne reste pas en dehors des problèmes de validation de l'âge des mineurs. Le RGPD ne compte aucune disposition indiquant au responsable des données qu'il doit vérifier et authentifier l'âge du mineur, comme s'il le fait spécifiquement dans le cadre de l'obtention du consentement parental, comme nous le verrons ultérieurement.

Toutefois, comme l'indique le CEPD dans les lignes directrices sur le consentement, toute collecte et tout traitement de données concernant des mineurs qui se trouvent en dehors des paramètres du règlement seront considérés comme illicites[425]. En ce sens, les responsables des données « devront s'efforcer raisonnablement de vérifier que l'utilisateur a dépassé l'âge minimum

[422] CE, *supra* note 419 à la p 8.
[423] *Ibid*.
[424] *Ibid* à la p 19.
[425] *Lignes directrices sur le consentement*, *supra* note 403 nº 133.

de consentement numérique »[426]. Il n'y a pas de référence à ce que l'on entend par « efforts raisonnables ».

De même, l'ICO UK dans le guide « *Children and RGPD* » suggère aux contrôleurs que dans les cas où ils ne sont pas sûrs si les services qu'ils fournissent sont utilisés par des mineurs, ou ne connaissent pas la tranche d'âge dans laquelle ils se trouvent, ils doivent mettre en place des systèmes de vérification d'âge à l'avance et tenir compte du seuil d'âge cible pour le traitement dans son service[427].

À l'heure actuelle, il n'existe pas de procédures harmonisées pour vérifier l'âge d'un mineur, les méthodes de vérification de l'âge qui existent sur la plupart des territoires des États membres reposent sur la preuve que l'utilisateur a plus de 18 ans[428], et ils ne sont pas fiables parce que les mineurs mentent facilement sur leur âge ou prétendent être leurs parents.

On peut citer comme exemple le mécanisme d'autovérification, à travers lequel l'utilisateur inclut sa date de naissance et le responsable lui permet d'accéder au service si l'année indiquée coïncide avec l'âge minimum du service. Dans cette méthode, il est facile de mentir même si les contrôleurs tentent d'inclure des blocages sur l'âge, en anglais « *age gating* », qui sont des cookies qui bloquent l'inscription lorsque vous mettez l'âge ou la date de naissance erronée.

Par ailleurs, l'industrie des SSI s'y oppose en raison des grands investissements qu'elle devra réaliser. Des mécanismes tels que des algorithmes qui identifient les modèles de voix, des questions clés pouvant correspondre à une tranche d'âge, l'utilisation de jetons numériques (ne comprenant pas de données personnelles) ou un numéro d'identification national sont des options proposées par les différents secteurs concernés.

En tout état de cause, les lignes directrices du CPED préviennent que la vérification de l'âge peut à son tour entraîner un traitement excessif des données et recommandent qu'une évaluation des risques du traitement soit effectuée lors de la vérification de l'âge de la personne concernée.

> « 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

[426] *Ibid* nº 132.
[427] R-U, Information Commissioner's Office, *supra* note 390 à la p 13.
[428] Milkaite et al, *supra* note 396 à la p 20.

traitement devrait réviser ses mécanismes de vérification de l'âge dans un cas donné et évaluer si des méthodes de vérification alternatives sont nécessaires » [429].

D'autres questions soulevées par les opposants à la validation de l'âge concernent l'anonymat sur l'Internet, la liberté d'expression et la vie privée des mineurs en ligne [430]. Ils indiquent que la vérification de l'âge ne doit pas devenir un outil négatif pour que les gens deviennent identifiables à tout moment [431].

En terminant, il est clair que la question de la vérification de l'âge soulève de nombreux aspects délicats et que le CEPD et les agences de protection des données devront donc travailler sur des lignes directrices prévoyant l'obligation de recourir à des mécanismes de vérification de l'âge, les méthodes de vérification de l'âge spécifiques et le niveau de fiabilité acceptable de chacun[432].

2.2.2 Consentement Parental

Le paragraphe 1 de l'article 8 du RGPD stipule que, si l'enfant n'a pas atteint l'âge de la majorité numérique imposé par le RGPD de 16 ans (ou l'adopté par l'État membre), « le titulaire de la responsabilité parentale » doit donner ou autoriser l'enfant à donner son consentement. En l'absence de cela, les données personnelles de l'enfant ne peuvent pas être traitées légalement par le contrôleur.

Sont exemptés de ce mandat les services de prévention ou de conseils offerts directement aux mineurs, pour lesquels le consentement du TRP ne sera pas nécessaire. Selon les termes de l'ICO UK, cela implique que "it will be in the best interests of the child to accept their own consent or that another basis for processing (such as public task or legitimate interests) may be more appropriate"[433].

L'expression « titulaire de la responsabilité parentale » désigne en droit de la famille les personnes qui ont la responsabilité parentale de l'enfant, qui sont elles-mêmes titulaires de l'autorité parentale, qui en règle générale, incombe aux parents ou à un tuteur si un tribunal l'a

[429] *Lignes directrices sur le consentement*, *supra* note 403 nº 135.
[430] Macenaite & Kosta, « Consent for processing children's personal data in the EU », *supra* note 78 à la p 179.
[431] Milkaite et al, *supra* note 396 à la p 20.
[432] Macenaite & Kosta, « Consent for processing children's personal data in the EU », *supra* note 78 à la p 182.
[433] R-U, Information Commissioner's Office, *supra* note 390 à la p 25.

désigné. Nous soutenons ceux qui considèrent que l'art. 8 du RGPD est limité aux parents et tuteurs légaux, et que « s'il n'est pas désigné par le tribunal, il ne peut pas inclure un cercle plus large de membres de la famille ou s'étendre au-delà des parents aux professionnels qui travaillent avec des enfants » [434] (notre traduction).

Une autre question, qui devra être clarifiée par les régulateurs, concerne le pouvoir du TRP d'« autoriser le consentement », ce qui est très différent que de « donner le consentement ». L'article 8 du Règlement n'indique pas dans quelles circonstances le consentement du mineur peut être autorisé. Il n'est pas clair si, lorsqu'il s'agit « d'autoriser le consentement », cela signifie que le TRP peut autoriser le consentement précédemment donné par le mineur ou par une autre personne, par exemple un membre de la famille ou une autre personne à titre professionnel. En ce sens, les chercheurs Mancenati et Kosta se demandent si « a possibility for parents to approve post factum the consent of a child in specific circumstances? Could the circle of holders of parental responsibility include individuals other than parents and legal guardians? » [435].

Il incombera alors au législateur, à la CPED et aux autorités de contrôle des données respectives de chaque État membre de réglementer les conditions dans lesquelles l'autorisation du consentement peut être donnée.

Un autre point de controverse se trouve dans ceux qui s'opposent à ce que le TRP donne le consentement par le mineur, en indiquant que ce sont les enfants qui possèdent les plus grandes capacités numériques, que les parents ne lisent pas ou ne comprennent pas les politiques de confidentialité, que, dans de nombreux cas, il n'est pas dans leur intérêt de restreindre l'accès des mineurs aux SSI, et que les parents sont actuellement négligés avec les données des enfants[436]. Ils indiquent que des phénomènes comme le *sharenting*[437], met en doute la capacité des parents et supporte les idées des critiques sur la nécessité du consentement parental.

Il convient de noter que les raisons invoquées sont les mêmes que celles qui sous-tendent l'inclusion d'une protection spéciale pour les mineurs. Si les adultes, qui sont déjà pleinement

[434] Macenaite & Kosta, « Consent for processing children's personal data in the EU », *supra* note 78 aux pp 175-176.
[435] Macenaite & Kosta, « Consent for processing children's personal data in the EU », *supra* note 98 à la p 175.
[436] Milkaite et al, *supra* note 396 à la p 17.
[437] Option consommateurs, *supra* note 244 à la p vii. « consiste, pour les parents, à publier une multitude de renseignements personnels à propos de leurs enfants sur les réseaux sociaux » souvent sans la connaissance ou le consentement de ceux-ci.

développés, ne comprennent pas l'ampleur de la vie privée, encore moins les mineurs qui sont vulnérables au moment de leur développement. D'une manière générale, l'esprit de l'autorité parentale est fondé sur le fait que le législateur considère comme apte le détenteur, et donc à la lumière de la protection des données, le TRP est censé être en mesure de prendre des décisions éclairées sur ses propres choix en matière de protection de la vie privée, et donc sur celle de l'enfant[438].

Sans préjudice de ce qui précède, il est clair que tant le législateur que les prestataires de SSI ont la responsabilité de soutenir le TRP dans la tâche d'alphabétisation numérique, en fournissant des informations pertinentes aux parents ou tuteurs, à travers, par exemple, la création de programmes ou la mise en place de mécanismes d'information facilement accessibles. L'adoption et la mise en œuvre de règles et de programmes qui protègent les mineurs non seulement des responsables des données, mais aussi de leurs parents lorsque ceux-ci sont à l'origine d'une violation de la vie privée du mineur, que ce soit avec ou sans intention.

Le RGPD n'est pas étranger à cette position. D'ailleurs, l'article 57(1)(b)[439] impose aux autorités de surveillance de promouvoir « la sensibilisation du public et la compréhension des risques », des normes, des garanties et des droits liés au traitement des données; et souligne que les activités visant spécifiquement les mineurs feront « l'objet d'une attention particulière ».

Dans le même ordre d'idées, l'art. 40 (2.g) du règlement prévoit que les États membres, les autorités de surveillance, le Conseil de l'Europe et la Commission agissent par l'intermédiaire d'entités représentant les contrôleurs, le développement de campagnes d'information et l'élaboration de codes de conduite spécifiant « les informations communiquées aux enfants et la protection dont bénéficient les enfants et la manière d'obtenir le consentement des titulaires de la responsabilité parentale à l'égard de l'enfant »; afin d'accroître le niveau d'alphabétisation numérique des parents[440].

Outre les critiques déjà exposées, certains auteurs proposent qu'au lieu de donner au TRP le contrôle des données du mineur par le consentement, ce qu'il convient de faire, c'est d'interdire

[438] *The General Data Protection Regulation: A Partial Success for Children on Social Network Sites?*, SSRN Scholarly Paper, by Karen McCullagh, papers.ssrn.com, SSRN Scholarly Paper ID 2985724, Rochester, NY, Social Science Research Network, 2016 à la p 128.
[439] *RGPD*, *supra* note 39.
[440] McCullagh, *supra* note 438 à la p 129.

de manière spécifique certaines pratiques de collecte de données auprès des mineurs. Dans ce sens, Adam Thierer affirme qu'il existe de meilleurs moyens de protéger la vie privée en ligne des mineurs que d'instaurer le consentement parental et d'étendre la vérification de l'âge dans la législation comme « education, empowerment, and targeted enforcement of unfair and deceptive practices »[441].

L'idée d'une approche hybride se pose dans ce mémoire, dans laquelle, d'une part, le consentement parental est pris en compte comme base juridique pour le traitement des données du mineur, et, d'autre part, l'établissement de politiques interdisant au contrôleur d'exécuter des pratiques de collecte de données potentiellement préjudiciables à la vie privée de l'enfant. Ce serait un scénario plus optimal en matière de protection des données des mineurs.

Force est de constater que, même si le RGPD limite le traitement des données relatives aux mineurs à l'intérêt légitime, nous avons déjà présenté certaines de ses lacunes au début de ce chapitre. Par ailleurs, le considérant 38 du règlement indique que les enfants doivent bénéficier d'une protection spécifique contre le marketing ou le profilage, mais il ne l'interdit pas explicitement et ne précise pas les conditions de la manière et du moment de le faire. Pour sa part, le considérant 71 de la même règle stipule que la prise de décision automatisée fondée sur le profilage ne devrait pas affecter les enfants. Toutefois, il est évident que cette activité n'est interdite que si elle affecte de manière significative le mineur[442].

Enfin, l'exigence du consentement paternel de l'art. 8 s'applique uniquement aux SSI et, par conséquent, la collecte de données hors ligne des enfants est soumise aux exigences générales de consentement du RGPD et à la législation nationale pertinente. Il n'y a pas de disposition spécifique à cet égard dans le règlement.

a. Consentement parental vérifié et méthodes de vérification (art. 8, paragraphe 2)

Comme nous l'avons vu plus tôt, lorsqu'un mineur n'est pas compétent pour donner son consentement parce qu'il n'a pas atteint le seuil de l'âge minimum requis dans l'État membre où il réside, le contrôleur qui utilise le consentement comme base légitime pour le traitement des

[441] Thierer, *supra* note 415 à la p 2.
[442] Macenaite & Kosta, « Consent for processing children's personal data in the EU », *supra* note 98 à la p 188.

données d'un mineur doit obtenir le consentement ou l'autorisation d'une personne ayant autorité parentale sur le mineur et prendre des mesures pour vérifier ce consentement, le cas échéant.

A cette fin, le paragraphe 2 de l'art. 8 du RGPD prévoit que :

> « 2. Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles ».

Selon le CPED, lorsque le mineur affirme avoir atteint l'âge du consentement numérique, le responsable du traitement devra faire tous les efforts raisonnables pour vérifier la véracité de la déclaration. En revanche, si le mineur déclare ne pas avoir atteint l'âge du consentement numérique, le responsable accepte la déclaration sans autre vérification, mais doit obtenir l'autorisation du TRP et vérifier que la personne qui donne le consentement est le titulaire de l'autorité parentale ou de la tutelle[443].

Bien que l'art. 8 introduit de manière exhaustive les notions de « vérification » et « effort raisonnable », il n'inclut pas les critères nécessaires pour établir la configuration du « consentement vérifié » ou qui constitue un « effort raisonnable ». Cela signifie que le Règlement ne prévoit pas de méthodes pour obtenir le consentement du TRP, déterminer si la personne qui donne le consentement a le droit ou la tutelle de le remettre[444], ainsi que des lignes directrices permettant de déterminer la qualité ou le niveau de l'effort pour qu'il soit considéré comme raisonnable.

Il est clair que l'exigence de faire des « efforts raisonnables » pour vérifier le consentement du TRP n'implique pas un « engagement de résultat »[445]. Les contrôleurs, lorsqu'ils font des efforts raisonnables pour obtenir le consentement du TRP, ne peuvent pas garantir comme résultat final l'obtention du consentement vérifié du TRP, soit pour des causes qui échappent à leur contrôle, soit en raison de l'absence de mécanismes techniques.

Il est important de préciser que, en principe, le texte de l'art. 8 du RGPD exigeait un « consentement vérifiable », mais dans la version finale il a été opté pour la formule du « consentement vérifié ». Si la proposition initiale avait été retenue, elle aurait été avantageuse pour

---

[443] *Lignes directrices sur le consentement*, *supra* note 403 nº 134.
[444] *Ibid* nº 136.
[445] Eva Lievens & Valerie Verdoodt, «Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation» (2018) 34:2 Comput Law Secur Rev 269-278 à la p 274.

la protection des droits des mineurs, car exiger que le consentement soit vérifiable impose l'obligation de vérifier le consentement à tout moment de la relation avec le mineur. En revanche, la validation du consentement sur la base d'un « consentement vérifié » présuppose que la vérification soit effectuée en un seul moment[446].

En conséquence, le responsable des données peut faire valoir que même s'il a fait un « effort raisonnable » il n'a pas été possible de valider le consentement du TRP, il serait qualifié pour traiter les données du mineur.

Par conséquent, il incombera aux agences de protection des données des États membres et/ou aux institutions qu'elles exercent au niveau communautaire d'élaborer des lignes directrices claires et pratiques pour l'application du consentement vérifié et des méthodes de vérification, afin que les responsables puissent prendre des mesures raisonnables pour s'assurer que le consentement est donné ou autorisé par le TRP. De leur côté, les contrôleurs doivent prendre toutes les mesures nécessaires pour mettre en œuvre cette exigence et utiliser les mécanismes (peu nombreux) prévus dans le RGPD, tels que la possibilité d'élaborer des codes de conduite (article 40 (2.g)).

A cet égard, la CEPD recommande aux contrôleurs d'adopter une approche proportionnée, parmi les paramètres de consentement de l'art. 8 et la minimisation des données de l'art. 5 (1.c)[447]. Cela signifie une approche centrée sur l'obtention d'une quantité limitée d'informations. Il indique en outre que la vérification de l'âge du consentement du mineur ou du consentement du TRP dépendra des risques (risque faible ou risque élevé) inhérents au traitement et de la technologie disponible pour effectuer ces vérifications [448]. Il conclut que plus le risque est élevé, plus le responsable doit obtenir des preuves et conserver les informations conformément à l'art. 7 (1) du Règlement. L'ICO UK dans le guide "Children and the RGPD" donne quelques exemples qui peuvent servir de guide [449].

Malgré les recommandations du CPED et de l'ICO UK (qui ne sont appliquées que sur leur territoire), il n'existe pas de directives spécifiques sur la manière d'évaluer si les efforts ont été raisonnables, ni l'inclusion de méthodes permettant de déterminer dans quelles circonstances un

[446] Macenaite & Kosta, «Consent for processing children's personal data in the EU», *supra* note 78 à la p 177.
[447] *Lignes directrices sur le consentement*, *supra* note 403 nº 136.
[448] *Ibid* nº 137; R-U, Information Commissioner's Office, *supra* note 390.
[449] R-U, Information Commissioner's Office, *supra* note 390 à la p 26.

mécanisme ou un outil technique de vérification du consentement est jugé suffisant, ou la pondération du risque par rapport aux intérêts du responsable du traitement.

Pourtant, il est recommandé que le responsable des données effectue une évaluation d'impact afin d'évaluer et atténuer les risques liés au traitement des données à caractère personnel concernant les enfants, et décide si le traitement est justifié, veiller à ce que le processus décisionnel soit documenté et utilisé comme preuve si l'entité de protection des données effectue une enquête.

L'approche présentée par la COPPA des États-Unis peut servir de guide dans ce processus de réglementation, étant donné qu'il comprend plusieurs options non exhaustives parmi lesquelles l'exploitant peut effectuer une sélection de la méthode de vérification en fonction de l'utilisation qu'il fait des données de l'enfant, soit à des fins internes, soit pour les partager avec des tiers. De même, dans le processus de corégulation, les entreprises peuvent utiliser de nouvelles méthodes de vérification, sous réserve de l'approbation du code d'autorégulation contenant les mécanismes par la FTC.

Si nous transposions ces mécanismes dans le RGPD, nous pourrions trouver une base pour leur application. D'une part, l'échelle mobile sur la base de l'analyse de risque proposée par le CEPD à la suite de l'analyse d'impact[450]. Ainsi, des mécanismes plus robustes seraient mis en place si le risque est à l'extrême le plus élevé et plus flexibles si le risque est faible. D'autre part, le RGPD exhorte les contrôleurs à travers l'art. 40 (2.g) à adhérer à des codes de conduite des associations industrielles contenant les outils nécessaires pour protéger les droits des mineurs. À partir du guide offert par le COPPA, le RGPD peut continuer à travailler à la recherche d'une approche globale de la protection des données et de la vie privée des mineurs[451].

b. Confirmation, modification ou retrait du consentement parental

Puisque l'article 8 et le RGPD en général gardent le silence sur ces aspects, nous tiendrons compte des lignes directrices du CEPD dont il a reconnu que le consentement donné par un TRP peut être confirmé, modifié ou retiré[452], lorsque le mineur atteint l'âge du consentement

[450] Macenaite & Kosta, « Consent for processing children's personal data in the EU », *supra* note 98 à la p 192.
[451] Talley, « Major Flaws in Minor Laws », *supra* note 349 à la p 157.
[452] *RGPD*, *supra* note 39, art 8 (para. 3).

numérique[453]. Par conséquent, le traitement des données d'un mineur qui a acquis la majorité numérique continuera à être valable s'il ne réalise aucune des actions indiquées [454]. Cela a un sens, si l'on considère que le droit à la protection des données appartient au mineur et que le TRP est un simple désigné pour exercer au nom du mineur ses droits.

2.2.3 Non-ingérence dans le droit des contrats des États (paragraphe 3 art. 8)

Cette dernière section de l'article 8 établit que les règles relatives au consentement au traitement des données des mineurs « ne porte pas atteinte au droit général des contrats des États membres, notamment aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant. »[455]

Le législateur a expressément voulu faire la distinction entre le consentement relatif aux contrats et le consentement nécessaire pour protéger le traitement des données relatives aux mineurs. En tout cas, l'article 8 fixe les conditions de légalité du consentement aux fins du traitement des données et n'affecte pas la validité des contrats conformément au droit des contrats de chaque État membre. Les deux régimes étant donc indépendants l'un de l'autre, mais d'application simultanée[456].

Par ailleurs, rappelons-nous que les dispositions de l'article 8 du RGPD ont champ d'application limité, car elle ne s'applique que lorsque la base juridique choisie par le contrôleur est le consentement et ne couvre que les données personnelles traitées par les contrôleurs qui offrent directement des SSI aux mineurs. De ce fait, si le service offert n'entre pas dans la description de cet article et/ou si le contrôleur décide d'utiliser une base juridique différente, telle que la base juridique des contrats, le traitement des données sera licite à condition qu'il respecte les exigences légales en vigueur, et l'application de l'article 8 ne serait pas nécessaire.

De cette façon, si le libellé du paragraphe 3 (art.8) est étudié ensemble avec les dispositions de l'article 6 (b) du Règlement, on peut conclure que le traitement des données qui sont «

---

[453] *Lignes directrices sur le consentement*, *supra* note 403 n^os^ 147 et 149.
[454] *Ibid* n^o^ 148.
[455] *RGPD*, *supra* note 39, art 7(3).
[456] *Lignes directrices sur le consentement*, *supra* note 403 n^o^ 151.

nécessaires » à la prestation du service engagé par un mineur est licite, à condition qu'il soit légalement habilité à conclure pour son compte un contrat conformément au droit des contrats de l'État membre. Au paragraphe 3.1. « Base juridique » de ce mémoire, vous pouvez trouver des informations concernant cette base juridique.

En conclusion, comme l'indique la CEPD, ni le RGPD ni les lignes directrices sur le consentement ne couvrent des questions telles que l'éventuelle harmonisation de la législation des États membres en matière de contrats avec l'article 8 du Règlement, ou s'il est licite qu'un mineur signe des contrats en ligne[457]. Il est donc nécessaire d'harmoniser les règles afin de garantir une plus grande sécurité juridique pour toutes les parties et de réduire les possibilités d'interprétation. Il se peut que le traitement des données soit licite parce qu'il est conforme aux termes de l'article 8, mais invalide aux fins du droit des contrats, et vice versa.

2.2.4 Principe de transparence

L'article 8 n'établit pas de manière exhaustive une référence à ce principe, mais l'une des conditions essentielles pour que le consentement de toute personne soit considéré comme valable est que le consentement soit informé.

En ce sens, le RGPD en son article 12, conformément au considérant 58, exigent des mesures de transparence spécifiques pour assurer une protection spéciale des droits des mineurs. Ainsi, toute méthode de communication et toute information que le contrôleur adresse à un mineur en ce qui concerne le traitement de ses données doivent être présentées de manière concise, exhaustive, transparente, intelligible et aisément accessible, dans un langage clair, simple et adapté à l'âge du mineur.

Le contrôleur doit donc veiller à ce que le mineur puisse facilement comprendre quelles sont les données personnelles qui sont impliquées et comment ses données seront utilisées. Cela permet au mineur de peser les bénéfices et les risques, en plaçant d'un côté de la balance la remise de ses données personnelles et de l'autre l'accès et l'interaction dans un SSI. Le responsable doit

[457] *Ibid*.

également informer le mineur qu'il a le droit de retirer le consentement à tout moment, même si c'est le TRP qui l'a accordé en son nom.

Par ailleurs, cela donne les premières lignes directrices pour la rédaction des avis de confidentialité et les avertissements de possibles failles de sécurité. Rappelons que les avis de confidentialité ne sont généralement pas rédigés de manière à ce que les mineurs puissent comprendre leur contenu et donc les accepter sans procéder à leur lecture[458]. La question des avertissements pour les failles de sécurité dans le contrôle des données est encore plus critique. Ces avis contiennent des informations techniques qui ne sont pas faciles à comprendre. En outre, les problèmes de transparence sont exacerbés lorsqu'il s'agit de sites destinés à un public mixte ou général[459].

2.2. Droit à l'effacement

Le RGPD dispose dans son article 17 les cas dans lesquels une personne concernée a le droit de retirer son consentement afin que ses données à caractère personnel soient définitivement supprimées d'Internet et, par conséquent, que le traitement cesse sans qu'il soit nécessaire de fournir plus d'informations que la demande d'effacement. À cet effet, le responsable des données doit mettre en place un processus permettant à la personne de faire la demande facilement.

De son côté, le responsable du traitement traitera la demande au plus tard un mois après la réception et informera oralement ou par écrit de la décision[460]. S'il n'y a pas d'exception applicable, il supprimera tout lien, copie et/ou réplication des données supprimées et fera des efforts raisonnables pour informer de la demande d'autres responsables du traitement avec lesquels il a partagé ou publié les données faisant l'objet de la demande (art. 17(2)), qui doivent également effacer les données.

[458] Macenaite & Kosta, « Consent for processing children's personal data in the EU », *supra* note 98 à la p 185; Centre for Information Policy Leadership, *supra* note 405 aux pp 20-21.
[459] Centre for Information Policy Leadership, *supra* note 405 à la p 21.
[460] *RGPD*, *supra* note 39. Considérant 59.

Étant donné que le droit de suppression n'est pas absolu, dans le cas où l'une des exceptions prévues au paragraphe 3, article 17[461], le responsable du traitement des données peut, sur justification, s'opposer à la suppression des données et rejeter la demande. L'article 17 (3) cite comme exceptions: l'exercice de la liberté d'expression ; le respect d'une obligation légale ; le motif d'intérêt public dans le domaine de la santé publique ; les fins d'archivistes dans l'intérêt public, la recherche scientifique, historique ou statistique ; la constatation, l'exercice ou la défense des droits en justice.

En ce qui concerne le droit d'effacement des données à caractère personnel des mineurs, le règlement fait expressément référence dans l'hypothèse finale de l'article 17, que l'un des motifs pour demander la suppression se présente lorsque les données du mineur ont été recueillies en relation avec l'offre de SSI visée à l'article 8 (1) du RGPD. Pour sa part, le considérant 65 note que ce droit est d'une grande importance dans le cas où le mineur souhaite supprimer ses données personnelles lorsqu'il estime qu'il donne son consentement sans être pleinement conscient des risques que comporte le traitement.

Le champ d'application de cette hypothèse comprend les personnes qui ont donné leur consentement, soit par elles-mêmes, soit par l'intermédiaire du TRP, à ce que leurs données à caractère personnel soient utilisées ou collectées alors qu'elles n'avaient pas encore atteint l'âge du consentement numérique. Cela signifie que les adultes et les mineurs peuvent exercer ce droit. Or, dans la pratique se posent des questions comme : si les conditions de l'âge numérique établies dans l'article 8 du RGPD seront par défaut appliquées pour le droit d'effacement? Si, par analogie, il n'est pas possible d'appliquer la même condition, alors on comprendra que la demande de suppression des données de tout enfant de moins de 18 doit-elle être présentée par le TRP?

Il convient de noter que le règlement n'exige pas que le mineur ait atteint l'âge de la majorité numérique, mais qu'il ait été mineur au moment de la récolte, et l'article 8 ne concerne que les conditions de consentement. À cet égard, certaines agences de protection des données, comme

[461] « Droit à l'effacement | Autorité de protection des données », en ligne: <https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/droits-des-citoyens/droit-a-l-effacement>.

celles d'Espagne et du Royaume-Uni[462] ont indiqué que les personnes ayant atteint l'âge de la majorité numérique pourront exercer les droits du RGPD sans avoir besoin de tuteur.

En bref, le responsable des données doit faire preuve de plus de prudence lorsqu'il examine une demande d'effacement concernant les données d'un mineur plutôt que d'une demande d'effacement concernant un adulte. Pour prendre la décision, le contrôleur doit mettre en balance les droits et libertés des parties concernées, d'une part, du responsable des données et/ou du parent ou tiers qui a effectué la publication et, d'autre part, les droits du mineur. En tout état de cause, sans être absolu, il doit déterminer ce qui est le mieux pour le mineur selon le principe de l'intérêt supérieur du mineur[463].

En outre, l'ICO UK note que lorsque le parent au tuteur n'est pas en accord avec le mineur quant à la nécessité d'effacer des données, ou lorsqu'il y a plus d'un TRP en désaccord entre eux, ou encore dans le cas où l'enfant veut que les données soient effacées sans le consentement du TRP, le responsable des données doit tenir compte de l'opinion et du niveau de compréhension du mineur, et privilégier l'intérêt supérieur de l'enfant[464].

L'exercice de ce droit ne sera pas facile à mettre en œuvre, des facteurs tels que les intérêts légitimes des entreprises, les abus de l'autorité parentale, les intérêts de la société entreront en jeu lorsque les mineurs deviennent des personnalités publiques, et en particulier la méconnaissance des données collectées par les prestataires de services sans que le mineur ait réellement connaissance que des données circulent sur l'Internet. En tout état de cause, l'inclusion du droit de suppression constitue une avancée pour la protection des données relatives aux mineurs.

[462] R-U, Information Commissioner's Office, *supra* note 390 aux pp 44-45.
[463] Anna Bunn, « Children and the 'Right to be Forgotten': what the right to erasure means for European children, and why Australian children should be afforded a similar right » (2019) 170:1 Media Int Aust 37-46 aux pp 38-39.
[464] R-U, Information Commissioner's Office, *supra* note 390.

Conclusion

Dans le contenu de ce mémoire de maîtrise, il nous est apparu que le traitement des données à caractère personnel est une activité qui a une grande incidence sur la vie des mineurs, d'autant que ces derniers ne sont pas pleinement conscients des risques et des conséquences qui peuvent résulter de la transmission de renseignements personnels.

Certes, les enfants devraient saisir toutes les opportunités offertes par les TIC et Internet en apprenant à surmonter les risques constants. Il est clair que la solution n'est pas d'interdire aux mineurs, en particulier des plus jeunes, l'utilisation d'Internet et des nouvelles technologies, mais de prendre des mesures permettant d'atténuer ou de contrôler les risques éventuels liés au traitement des données des mineurs, et de trouver un équilibre prudent entre les risques et opportunités offertes par Internet. À ce sujet, certains systèmes juridiques du monde se sont attaqués à cette problématique, notamment aux États-Unis avec la *Children s Online Privacy Protection Act* (COPPA) et en Union européenne par certaines dispositions du *Règlement général (UE) 2016/679 sur la protection des données* (RGPD) notamment.

En guide de conclusion, nous voulons faire part d'un certain nombre de réflexions finales :

Premièrement, le traitement des données relatives aux mineurs et leur utilisation par les responsables du traitement sont de plus en plus fréquents. Les mineurs déposent jour après jour sur le net toutes sortes d'informations personnelles qui en font des sujets facilement identifiables : vidéos et photos révélant leur identité, textes et audio décrivant leur personnalité et leurs habitudes ainsi que des coordonnées GPS précisant leur emplacement.

En profitant de cette situation, les entreprises stockent les données de mineurs par le biais des jouets intelligents, des réseaux sociaux, des études de marché, salle de chat, entre autres médias, dans le but de créer des profils de mineurs pour les exposer au marketing ciblé ou à la publicité personnalisée, et donc obtenir de grands avantages économiques.

Certes, nous constatons que le plus grand problème auquel sont confrontés les mineurs pour la violation des données personnelles, l'utilisation abusive des informations et la mauvaise gestion de la vie privée, est lié à l'exposition à des risques de contact, comme le vol d'identité, la

cyberintimidation, le leurre par Internet et le sextage. Ces comportements portent directement atteinte à leurs droits fondamentaux, en particulier leur vie privée, leur intégrité, leur honneur et leur dignité.

Deuxièmement, on sait que les risques liés au traitement et à la collecte de données circulent de manière démesurée sur Internet, mais dans le cas des mineurs, comme on l'a déjà mentionné, il faut également tenir compte du fait qu'il existe un certain nombre de facteurs qui augmentent ces risques, notamment l'absence d'un développement et d'une maturité complets, étant donné qu'ils sont en phase d'apprentissage. Cette condition les rend vulnérables aux risques et en fait un groupe nécessitant une attention prioritaire. Ce qui exige aussi une protection spéciale de leurs droits.

Troisièmement, à propos de la protection des données personnelles des mineurs en ligne, nous trouvons qu'en général, dans les législations analysées, il existe des similitudes par rapport aux principes de traitement d'informations de mineurs, telles que l'obligation d'informer et d'obtenir le consentement des parents ou de représentants légaux (entre 13 et 16 ans). De même, il est reconnu dans les différents législations le droit d'accès, de rectification, d'annulation ou d'opposition au traitement de données des enfants.

Quatrièmement, de l'étude comparative entre les dispositions de la LPRPDE canadienne, la COPPA américaine et les règles du RGPD de l'Union européenne, relative à la protection des données personnelles des mineurs en ligne, il a été démontré que chacune de ces trois législations a un périmètre différent, notamment le champ d'application, le concept de données personnelles, la définition de l'enfant et l'âge spécifique pour donner le consentement; le type de services couverts; les conditions et méthodes d'obtention du consentement comme l'âge de la majorité numérique et les mécanismes de validation, ainsi que les mécanismes d'obtention et de validation du consentement parental.

En dernière lieu, nous constatons que les critiques à l'égard des dispositions relatives à la protection des données des mineurs sont généralement communes à la COPPA, au RGPD et aux directives/conseils du CPVP sur la collecte des données des mineurs au Canada. À ce sujet, les critiques indiquent que la mise en place des mécanismes de validation de l'âge et de l'identité de la personne qui donne le consentement parental est onéreuse, ce qui crée des obstacles à l'entrée sur le marché et/ou entraîne la limitation des services aux mineurs. D'autres notent que le paramètre

de l'âge est arbitraire, et il n'y a pas d'harmonie dans la désignation de l'âge minimum de consentement. Rappelons-nous que ce n'est pas seulement le cas de l'Union européenne ou du Canada. Aux États-Unis, la CPPA de l'État de Californie a relevé l'âge du consentement de 13 à 16 ans. Certains ont mentionné[465] que légiférer de manière spécifique sur les données des mineurs viole d'autres droits fondamentaux, comme la liberté d'expression et d'opinion, la liberté d'information et le libre développement de la personnalité des enfants.

En bref, bien qu'il y ait des règles qui régissent la question de la protection des données des mineurs, ces mécanismes s'avèrent insuffisants, incertains et peu précis pour répondre aux nouvelles questions qui se posent sur la scène en ligne. Dans ce nouveau contexte, les lacunes juridiques entraînent des défis pour le législateur.

Par conséquent, l'analyse de la COPPA, du RGPD et de la LPRPDE révèle qu'il sera nécessaire de réaliser différents types d'actions de la part des institutions publiques afin de lutter contre certains problèmes de sécurité juridique. En particulier, il convient de promouvoir une réforme législative de chacune de ces dispositions; l'élaboration de directives et de politiques uniformes et sans équivoque par les organismes chargés de la protection des données; des initiatives d'éducation et de sensibilisation des différentes parties concernées au développement des mineurs (parents, éducateurs, établissements d'enseignement); et l'autorégulation du secteur.

Les législateurs européen et américain, par exemple, doivent modifier l'âge du consentement et l'harmoniser de manière obligatoire pour l'ensemble de leur territoire. Établir de manière détaillée la procédure d'obtention du consentement parental et inclure les mécanismes techniques pour valider l'âge de la personne et, à défaut, l'identité du titulaire de la responsabilité parentale. Pour sa part, le Canada devra promouvoir la réforme de la LPRPDE afin d'inclure de manière exhaustive les droits des mineurs, en définissant au moins les aspects suivants : la notion de mineur, l'âge du consentement numérique, les conditions et événements dans lesquels le consentement parental peut être obtenu, les mécanismes techniques pour valider l'identité du parent ou tuteur, les mécanismes de validation de l'âge et les obligations du contrôleur.

[465] Krivokapic & Adamovic, *supra* note 95 aux pp 209-211; Boyd et al, *supra* note 354; Benyekhlef, *supra* note 233 à la p 239.

Références bibliographiques

Législation et réglementation

Au Canada

Charte Canadienne des Droits et Libertés, art 2(b), partie I de la Loi constitutionnelle de 1982, constituant l'annexe B de la Loi de 1982 sur le Canada (R-U), 1982, c 11.

Code criminel, LRC 1985, c C-46.

Loi sur la protection des renseignements personnels et les documents électroniques, LC 2000, c 5.

Loi sur la protection du consommateur, RLRQ c P-40.1.

Association canadienne du marketing (ACM), Code de déontologie et normes de pratique, Toronto, Ontario, TheCMA.ca, 2019.

Au provincial

Charte des droits et libertés de la personne, RLRQ c C-12

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

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

Personal Information Protection Act, SBC 2003, c. 63.

Personal Information Protection Act, SA 2003, c. P-6.5.

PL 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, 1re sess, 42e lég, Québec, 2020.

RLRQ c P-401, r 3.

À l'international

CE, Règlement (CE) 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), 2016 JO L1191.

Avis sur l'article 23 de la Convention de Lanzarote et sa note explicative, Adopté 17 Juin 2015.

California Consumer Privacy Act of 2018 (CCPA), Cal AB-375, §1798.100-1798.199 (2018).

Crimes and criminal procedure, 18 USC, part I ch 115 § 2422(b) (1940).

É-U, Bill HR 5573, PROTECT Kids Act, 116th Cong, 2019-2020.

CcQ.

C.E, Comité européen de la protection des données, Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, 2015 JO L2411 2020.

CE, Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015, prévoyant une procédure d'information dans le domaine des réglementations techniques et

des règles relatives aux services de la société de l'information (texte codifié), 2015 JO L2411.
Children's Online Privacy Protection Act, 15 USC §§ 6501–6506, (1998).
Children's Online Privacy Protection Rule, 16 CFR §312 1999.
Code pénal de France, Version Consolidée Au 1 Janvier 2020.
Privacy Rights for California Minors in the Digital World, California S.B. 568, 22580-82 (2015).
C.E, Proposition de Règlement du Parlement Européen et du Conseil 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 (règlement général sur la protection des données), [2012], COM (2012) 11 final.
Sexual Offences Act 2003, (R-U), 2003 Ch. 42.

Instruments internationaux

Convention C182 concernant l'interdiction des pires formes de travail des enfants et l'action immédiate en vue de leur élimination, Organisation international du travail [OIT], 17 juin 1999, Doc OIT C182/1999, 87ème session (entrée en vigueur : 19 novembre 2000).
Convention du Conseil de l´Europe: La protection des enfants contre l'exploitation et les abus sexuels (Convention de Lanzarote), 2007, STCE 201.
Convention internationale relative aux droits de l'enfant, Rés AG 44/25, 20 novembre 1989, R.T. Can. 1992, n° 3 Annexe, (entré en vigueur le 2 septembre 1990, accession par le Canada le 12 janvier 1992).
Le droit à la vie privée à l'ère du numérique, Doc off AG NU, 75e Sess, Doc NU A/RES/75/176 (2020).
Le droit à la vie privée à l'ère du numérique, Doc off AG NU, 69e Sess, 73e Séance, Doc NU A/RES/69/166 (2014).
Le droit à la vie privée à l'ère du numérique, Doc off AG NU, 68e sess, 70a séance, Doc NU A/RES/68/167 (2013).
Mémorandum de Montevideo: Mémorandum sur le droit à la protection des renseignements personnels et la vie privée dans les réseaux sociaux sur l'Internet, en particulier ceux des enfants et des adolescents, Instituto de investigación para la justicia, IIJusticia, 2009.
Observation générale no 14 (2013) sur le droit de l'enfant à ce que son intérêt supérieur soit une considération primordiale (art. 3, par. 1), Doc off CDE NU, 62e Sess, Doc NU CRC/C/GC/14 (2013).
Observation générale no 16: Article 17 (Droit au respect de la vie privée), Doc off HCDH NU, 32e sess (1988), Doc NU HRI\GEN\1\Rev.1 (1994).
Principes directeurs pour la réglementation des fichiers personnels informatisés, Doc off AG NU, 45e sess, 68e séance, Doc NU A/RES/45/95 (1990).

Jurisprudence nationale et internationale, et autres documents

AB c Bragg Communications Inc, [2012] 2 RCS 567.

Asociacion Profesional Elite Taxi c Uber Systems Spain SL, Rec CE général (partie « Informations sur les décisions non publiées »).

Bond van Adverteerders et autres c État néerlandais, C-352/85, [1988] Rec CE 1988-02085.

CanLII QCCS 5769-2019

État belge c René Humbel et Marie-Thérèse EdeL, C-263/86, [1988] Rec CE 1988-05365.

ETHI, Témoignages, 1re session, 42e législature, 16 mai 2017, 1555 (Dennis Hogarth, vice-président, Conseil des consommateurs du Canada).

———, Témoignages, 1re session, 42e législature, 25 septembre 2017, 1535 (Owen Charters, président directeur général, Repaires jeunesse du Canada).

———, Témoignages, 1re session, 41e législature, 19 juin 2012, 1100 (Sara Grimes, Université de Toronto).

———, Témoignages, 1re session, 41e législature, 16 octobre 2012, 1700 (David Elder, ACM).

Gordon c Canada (Santé), 2008 Cour fédérale.

Irwin Toy Ltd c Québec (Procureur général), [1989] 1 RCS 927.

Ker-Optika bt c ÀNTSZ Dél-dunántúli Regionális Intézete, C-108/09, [2010] Rec CE I-12213.

Morgan c Alta Flights (Charters) Inc, 2006 Cour d'appel fédérale.

R c Sharpe, [2001] 1 RCS 45.

R.c Morrison, [2019] CSC 15.

Doctrine

Monographies et ouvrages collectifs

Andreu Martínez, Mª Belén, La protección de datos personales de los menores de edad, 1e éd, Navarra, España, Thomson Reuters Aranzadi S.A, 2013.

Boyd, Danah, It's Complicated: The Social Lives of Networked Teens, Yale University Press, 2014.

Brown, Jon, Online Risk to Children: Impact, Protection and Prevention, 1e éd, John Wiley & Sons Ltd, 2017.

Deursen, Alexander J A M van & Jan A G M van Dijk, Digital Skills: Unlocking the Information Society, Digital Education and Learning, New York, Palgrave Macmillan Ltd., 2014.

Gil Antón, Ana María, El derecho a la propia imagen del menor en Internet, Madrid, España, Dykinson S.L., 2013.

———, ¿Privacidad del menor en internet?: « me gusta », !!!todas las imágenes de mis amigos a mi alcance con un simple click!!!., 1e éd, Monografía - Revista Nuevas Tecnologías 13, Cizur Menor (Navarra), España, Aranzadi Thomson Reuters, 2015.

Hernandéz Ramírez, Sergio, La protección de datos personales de menores en redes sociales: desafíos y recomendaciones Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación [INFOTEC], 2018) [unpublished].

International centre for missing & exploited children (ICMEC), Online grooming of children for sexual purposes: Model legislation & global review, 1e éd, États-Unis, The Koons Family Institute on International Law & Policy, 2017.

Kowalski, Robin M, Cyber bullying: bullying in the digital age, Malden, MA., Blackwell Pub, Blackwell, 2008.

Tétreault, Cathy, En tant que... victime, auteur ou témoin. Guide d´accompagnement pour le personnel scolaire qui ouvre auprès des victimes, auteurs ou témoins de sextos, de sextorsion et de cyberagression sexuelle, la collection de la chaire éd, Québec, 2019.

Tisseron, Serge, Sylvain Missonnier & Michaël Stora, L'enfant au risque du virtuel, Dunod, 2012.

UNESCO, Au-delà des chiffres: en finir avec la violence et le harcèlement à l'école, n. ED/477/0000368997, Paris, UNESCO, 2019.

Vallet, Caroline, La protection des mineurs face à la cyberpédopornographie : étude comparée entre le droit criminel canadien et français, yvon blais éd, Minerve, Montréal, Québec, 2011.

Benyekhlef, Karim, « Minors, Social Network Sites And Le Droit Á L'oubli » dans Soc Netw Child Priv, Editorial Reus, 2011 229.

Calvo Caravaca, Alfonso-Luis & Javier Carrascosa González, « Protección de menores » dans Derecho Int Priv, 18e éd, Granada, España, 2018 1496.

Dearden, Lizzie, « 'Radical rethink' on grooming gangs needed after 19,000 children sexually exploited in year », The Independent (30 décembre 2019), en ligne: <https://www.independent.co.uk/news/uk/crime/grooming-gangs-child-sex-abuse-victims-rotherham-rochdale-latest-a9264656.html>.

Díaz cortés, Lina Mariola, « Menores e Internet: Entre las oportunidades y los riesgos. Un punto de partida para entender las políticas criminales » dans Algunos Desafíos En Protección Datos Pers D° Sociedad de la información 26, Comares, 2018 136.

Godbey, Robert Carson, « The Law of the Line » Hawaii Bus (novembre 2000), en ligne: <https://www.thefreelibrary.com/The+Law+of+the+Line.-a066812174>.

Harding, Dido, « Staying Safe Online » dans Jon Brown, dir, Online Risk Child Impact Prot Prev, 1e éd, John Wiley & Sons, Ltd, 2017 177.

lazatin, Emily, « Appeal case to begin in Netherlands for Amanda Todd's alleged tormentor », Glob News (22 octobre 2018), en ligne: <https://globalnews.ca/news/4581300/amanda-todd-dutch-accused-criminal-appeal/>.

Livingstone, Sonia, « Children's and Young People's Lives Online » dans Online Risk Child, 1e éd, John Wiley & Sons, Ltd, 2017 23.

———, « Enabling media literancy for "Digital Natives" – A contradiction in terms? » (2009) Digit Nativ Myth (London School of Econo), en ligne: <http://www2.lse.ac.uk/media@lse/POLIS/home.aspx>.

Livingstone, Sonia & Leslie Haddon, « Introduction: kids online: opportunities and risks for children » dans Sonia Livingstone & Leslie Haddon, dir, Kids Online Oppor Risks Child, Bristol, UK, The Policy Press, 2009 1.

Mail on sunday report, « Nearly 19,000 children in England are exploited in a year », Dly Mail Online (28 décembre 2019), en ligne: <https://www.dailymail.co.uk/news/article-7833493/Nearly-19-000-children-sexually-groomed-England-past-year.html>.

Milkaite, Ingrida & Eva Lievens, « Children's Rights to Privacy and Data Protection Around the World: Challenges in the Digital Realm » (2019) 10:1 Eur J Law Technol, en ligne: <https://ejlt.org/index.php/ejlt/article/view/674>.

Ornelas, Lina, « El derecho de las niñas, niños y adolescentes a la protección de sus datos personales: evolución de derechos y su exigencia frente a las redes sociales » dans Protección Datos Pers En Las Redes Soc Digit En Part Niños Adolesc, Buenos Aires, Argentina : Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) y del Instituto de Investigación para la Justicia (IIJusticia), 2011.

Phippen, Andy, « Cyberbullying and Peer-Oriented Online Abuse » dans Online Risk Child The NSPCC/Wiley Series, 1e éd, John Wiley & Sons, Ltd, 2017 37.

Piñar Mañas, José Luis, « The fundamental right of data protection and privacy of minors in social networks » dans Soc Netw Child Priv, Editorial Reus, 2011 61.

Rodota, Stefano, « Contemporary society, the privacy of minors and social networks » dans Soc Netw Child Priv, Madrid, España, Editorial Reus, 2011 47.

Rogers, Melisa, « Kids' Privacy Act Stings Web » Crains Chic Bus (14 mai 2000), en ligne: <https://www.chicagobusiness.com/article/20000514/HOLD/100014067/kids-privacy-

« L'homme qui a cyberintimidé Amanda Todd condamné à 11 ans de prison au Pays-Bas », (16 mars 2017), en ligne: <https://www.lapresse.ca/actualites/201703/16/01-5079235-lhomme-qui-a-cyberintimide-amanda-todd-condamne-a-11-ans-de-prison-au-pays-bas.php>.

Articles de revue, de journaux, colloques, blogs et communiqués de presse

Acedo Penco, Ángel & Alejandro Platero Alcón, « The Privacy of Children and Adolescents in Social Networks: Special Reference to the European and Spanish Regulatory Regime, with some Considerations on the Chilean » (2016) 5:2 Rev Chil Derecho Tecnol 63-94.

Barrera Ibañez, Silvia, XV. Investigación criminal de los delitos cometidos contra menores como usuarios de internet, España, Thomson Reuters Aranzadi, 2013.

Boyd, Danah et al, « Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act' » (2011) 16:11 First Monday, en ligne: <https://journals.uic.edu/ojs/index.php/fm/article/download/3850/3075>.

Bunn, Anna, « Children and the 'Right to be Forgotten': what the right to erasure means for European children, and why Australian children should be afforded a similar right » (2019) 170:1 Media Int Aust 37-46.

Cobb, Stuart, « It's COPPA-cated: Protecting Children's Privacy in the Age of YouTube » (2021) 58:4 Houst Law Rev 22277.

Deleury, Edith, Michèle Rivet & Jean-Marc Neault, « De la puissance paternelle à l'autorité parentale : Une institution en voie de trouver sa vraie finalité » (1974) 15:4 Cah Droit 779-870.

Englander, Elizabeth & Meghan McCoy, « Sexting—Prevalence, Age, Sex, and Outcomes » (2018) 172:4 JAMA Pediatr 317-318.

Forbes France, « Cyberharcèlement : Comment Lutter Efficacement Contre Ce Fléau Digital ? », Forbes Fr (23 octobre 2019), en ligne: <https://www.forbes.fr/technologie/cyberharcelement-comment-lutter-efficacement-contre-ce-fleau-digital/>.

Garmendia, Maialen et al, « Los menores en internet. Usos y seguridad desde una perspectiva europea » (2012) 15:38 Quad CAC 37-44.

Gautrais, Vincent & Adriane Porcin, « Les 7 pêchés de la LPC : actions et omissions applicables au commerce électronique » (2009) 43:3 Thémis (R.J.T) 559.

Gilliland, Donald, « It's time to rethink children's privacy protection », (8 août 2020), en ligne: TheHill <https://thehill.com/opinion/cybersecurity/511162-its-time-to-rethink-childrens-privacy-protection>.

González, Nicolás Antúnez, Fortalecimiento de herramientas para la protección de datos personales frente al debilitamiento del principio del consentimiento, Salamanca, España, Ratio Legis, 2016.

« Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law », (3 septembre 2019), en ligne: Fed Trade Comm <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations>.

Hango, Darcy, « La cyberintimidation et le cyberharcèlement chez les utilisateurs d'Internet âgés de 15 à 29 ans au Canada » (2016) 75-006-X Stat Can (Regards sur la societé canadienne) 20.

Hearn, Bill, « Canada: Canadian Advertising & Marketing Law: An Overview of the Rules, The Regulators And Their Powers », Fogler Rubinoff LLP (14 février 2017), en ligne: <https://www.mondaq.com/canada/advertising-marketing-branding/568494/canadian-advertising-marketing-law-an-overview-of-the-rules-the-regulators-and-their-powers>.

Helsper, Ellen Johanna & Rebecca Eynon, « Digital natives: where is the evidence? » (2010) 36:3 Br Educ Res J 503-520.

Henaff, Gaël, « L'enfant, l'âge et le discernement » (2000) 44 Lien Soc Polit 41-50.

IS4K, « Menores de edad y la publicidad en Internet », (17 décembre 2018), en ligne: Internet Segura Kids <https://www.is4k.es/blog/menores-de-edad-y-la-publicidad-en-internet>.

Johnson, Ariel Fox, « Improving COPPA: A Road Map for Protecting Kids' Privacy in 2020 and Beyond », (29 janvier 2020), en ligne: <https://www.commonsensemedia.org/kids-action/blog/improving-coppa-a-road-map-for-protecting-kids-privacy-in-2020-and-beyond>.

Krivokapic, Djordje & Jelena Adamovic, « Impact of general data protection regulation on children's rights in digital environment » (2016) 64 Anali Pravnog Fak U Beogr 205-220.

Lenhart, Amanda, « The challenges of conducting surveys of youth », (21 juin 2013), en ligne: Pew Res Cent <https://www.pewresearch.org/fact-tank/2013/06/21/the-challenges-of-conducting-surveys-on-youths/>.

Lievens, Eva & Valerie Verdoodt, « Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation » (2018) 34:2 Comput Law Secur Rev 269-278.

Macenaite, Milda & Eleni Kosta, « Consent for processing children's personal data in the EU: following in US footsteps? » (2017) 26:2 Inf Commun Technol Law 146-197.

———, « Consent for processing children's personal data in the EU: following in US footsteps? » (2017) 26:2 Inf Commun Technol Law 146-197.

Menin, Damiano et al, « Was that (cyber)bullying? Investigating the operational definitions of bullying and cyberbullying from adolescents' perspective » (2021) 21:2 Int J Clin Health Psychol 100221.

Moreau, Thierry, « Cent septante-cinq ans de regards sur l'enfant » (2005) 175-25:6205 J Trib 814-815.

Oswell, David, « The Place of 'Childhood' in Internet Content Regulation: A Case Study of Policy in the UK » (1998) 1:2 Int J Cult Stud 271-291.

Park, Jasmine, « The European Commission Considers Amending the General Data Protection Regulation to Make Digital Age of Consent Consistent - Future of Privacy Forum », en ligne: https://fpf.org/ <https://fpf.org/blog/the-european-commission-considers-amending-the-general-data-protection-regulation-to-make-digital-age-of-consent-consistent/>.

Perreault, Denyse, « La cyberintimidation : "please, no hate" » (2016) 13:4 Perspect Infirm 21-24.

Persano, Federica, « GDPR and Children Rights in EU Data Protection Law » (2020) 2020:Special Issue Eur J Priv Law Technol EJPLT 32-42.

Prensky, Marc, « Digital Natives, Digital Immigrants Part 1 » (2001) 9:5 Horiz 1-6.

———, « H. Sapiens Digital: From Digital Immigrants and Digital Natives to Digital Wisdom » (2009) 5:3 Innov J Online Educ 1-11.

Raymond, Guy, « L'autorité parentale sous contrôle ? » (2003) 22:2 Enfances Psy 25-37.

Siag, Jean, « Montrez-moi cette pub que je ne saurais voir ! », La Presse+ (23 mai 2016), en ligne: <https://plus.lapresse.ca/screens/859375cb-a6d8-425c-bd30-a8361299c173__7C___0.html>.

Staksrud, Elisabeth & Sonia Livingstone, « Children and online risk: Powerless victims or resourceful participants? » (2009) 12:3 Inf Commun Soc 364-387.

act-stings-web-sites>.

Strasburger, Victor C et al, « Teenagers, Sexting, and the Law » (2019) 143:5 Pediatrics, en ligne: <https://pediatrics.aappublications.org/content/143/5/e20183183>.

Talley, Virginia A M, « Major Flaws in Minor Laws: Improving Data Privacy Rights and Protections for Children under the GDPR Note » (2019) 30:1 Indiana Int Comp Law Rev [xi]-162.

Temple, Jeff & Sheri Madigan, « One in seven teens are “sexting,” says new research », en ligne: The Conversation <http://theconversation.com/one-in-seven-teens-are-sexting-says-new-research-92170>.

Watson, Cole, « Protecting Children in the Frontier of Surveillance Capitalism » (2021) 27:2 Stud Scholarsh 1-41

Youf, Dominique, « Seuils juridiques d’âge : du droit romain aux droits de l’enfant » (2011) n°11 Sociétés Jeun En Diffic Rev Pluridiscip Rech, en ligne: <http://journals.openedition.org/sejed/7231>.

Zapal, Haley, « State-by-State Differences in Sexting Laws », (9 avril 2019), en ligne: Bark <https://www.bark.us/blog/state-by-state-differences-in-sexting-laws/>.

Rapports

Barreau du Québec, Mémoire sur le projet de loi 64 sur la protection des renseignements personnels | BQ Commission des institutions de l’assemblée nationale, 2020) [unpublished].

Blakley, Bob et al, At a crossroads: “Personhood” and digital identity in the information society, by Bob Blakley et al, STI working paper series DSTI/DOC(2007)7, Organisation for Economic Cooperation and Development (OECD) Directorate for Science, Technology and Industry, 2008.

Bureau de l’Ombudsman et du défenseur des enfants et de la jeunesse, Il devrait y avoir une loi : Les sauts périlleux de la vie privée des enfants au 21e siècle, par le Bureau de l’Ombudsman et du défenseur des enfants et de la jeunesse, Ottawa, Ont, Groupe de travail des commissaires à la vie privée et des défenseurs canadiens des enfants et des jeunes, 2009.

Chambre des communes du Canada, Protection de la vie privée et médias sociaux à l’ère des mégadonnées : Rapport du Comité permanent de l’accès à l’information, de la protection des renseignements personnels et de l’éthique, 41e lég, 1re sess, no 5-ETHI (41-1), (avril 2013) (président : Pierre-Luc Dusseault).

Comité permanent de l’accès à l’information, de la protection des renseignements personnels et de l’éthique, Vers la protection de la vie privée dès la conception : examen de la loi sur la protection des renseignements personnels et les documents électroniques, 42e législature, 1re session (Février 2018) (président: Bob Zimmer).

Commissariat à la protection de la vie privée du Canada, Consentement et protection de la vie privée - Document de discussion sur les améliorations possibles au consentement sous le régime de la Loi sur la protection des renseignements personnels et les documents électroniques, 2016.

———, Projet de position du Commissariat sur la réputation en ligne, 2018.

———, Position de principe sur la publicité comportementale en ligne, 2015.

———, Rapport annuel au Parlement 2016-2017 concernant la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur la protection des

renseignements personnels: Des craintes réelles, des solutions pour y remédier : Plan pour rétablir la confiance dans la protection de la vie privée, Gatineau (Québec), 2017.

———, Rapport de conclusions en vertu de la LPRPDE no 2012-001: Nexopia, site de réseautage social pour jeunes, a enfreint la loi canadienne sur la protection des renseignements personnels, par la Commissariat à la protection de la vie privée du Canada, 2012-001, 2013.

———, Ratissage de 2017 du Global Privacy Enforcement Network, 2017.

———, « Survol de la LPRPDE », (9 janvier 2018), en ligne: <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/lprpde_survol/>.

———, Troisième principe relatif à l'équité dans le traitement de l'information de la LPRPDE – Consentement, 2018.

———, Vous recueillez des renseignements auprès des enfants? Voici dix conseils sur les services destinés aux enfants et aux jeunes, 2015.

Commission d'accès à l'information du Québec, Rapport quinquennal 2011. Technologies et vie privée : à l'heure des choix de société., par la Commission d'accès à l'information du Québec, Québec (Canada), 2011.

Commission des droits de la personne et des droits de la jeunesse, Mémoire sur le projet de loi 64 sur la protection des renseignements personnels | CDPDJ Commission des institutions de l'assemblée nationale, 2020) [unpublished]

Das, Ranjana et al, 'Digital Natives': A Myth?, by Ranjana Das et al, London, UK, London School of Economics and Political Science, 2009.

Del Rey, R et al, Protocolo de actuación escolar ante el ciberbullying, por R Del Rey et al, Google Scholar, Bilbao, Equipo multidisciplinario de investigación sobre ciberbullying [EMICI], 2011.

Gouvernement du Québec, Ensemble contre l´intimidation! : Rapport du Comité d'experts sur la cyberintimidation, Québec, 2015.

Haber, Eldar, The Internet of Children: Protecting Children's Privacy in A Hyper-Connected World, SSRN Scholarly Paper, by Eldar Haber, papers.ssrn.com, SSRN Scholarly Paper ID 3734842, Rochester, NY, Social Science Research Network, 2020.

Krzymien, Kasia, Les technologies de surveillance appliquées aux enfants, par Kasia Krzymien, Commissariat à la protection de la vie privée du Canada, 2012.

La cyberintimidation, ça blesse! : respect des droits à l'ère numérique : Rapport du Comité sénatorial permanent des droits de la personne, 9, (décembre 2012) (présidente: Mobina S B Jaffer, vice-président: Patrick Brazeau).

La situation des enfants dans le monde 2017 : Les enfants dans un monde numérique, Fonds des Nations Unies pour l'enfance (UNICEF France), 2017.

Lawford, Counsel John, All in the Data Family: Children's Privacy Online, by Counsel John Lawford, 1-895060-86-9, Ottawa, ON, Public Interest Advocacy Centre.

Le centre de recherche Innocenti (CRI), La sécurité des enfants en ligne : Défis et stratégies mondiaux, par le centre de recherche Innocenti (CRI), Innocenti Insights D, Italie, UNICEF, 2012.

L'intérêt supérieur de l'enfant : signification et mise en application au Canada, Coalition canadienne pour les droits des enfants, 2009.

Livingstone, Sonia, Giovanna Mascheroni & Elisabeth Staksrud, developing a framework for researching children's online risks and opportunities in Europe, by Sonia Livingstone, Giovanna Mascheroni & Elisabeth Staksrud, Zotero, Londres, EU Kids Online, 2015.

Livingstone, Sonia, Mariya Stoilova & Rishita Nandagiri, Children's Data and Privacy Online: Growing Up in a Digital Age An Evidence Review, by Sonia Livingstone, Mariya Stoilova & Rishita Nandagiri, London, London School of Economics and Political Science, 2018.

McCullagh, Karen, The General Data Protection Regulation: A Partial Success for Children on Social Network Sites?, SSRN Scholarly Paper, by Karen McCullagh, papers.ssrn.com, SSRN Scholarly Paper ID 2985724, Rochester, NY, Social Science Research Network, 2016.

Milkaite, Ingrida et al, The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society. Roundtable Report., by Ingrida Milkaite et al, 2017.

Ministère de la Justice du Canada, Cyberintimidation et distribution non consensuelle d'images intimes: Rapport aux ministres fédéraux/provinciaux/territoriaux responsables de la Justice et de la Sécurité publique, Groupe de travail sur la cybercriminalité du Comité de coordination des hauts fonctionnaires, 2013.

OCDE, La publicité et le marketing en ligne visant les enfants, par OCDE, Comité de la politique, Document de travail no. 46, no de doc DSTI/CP(99)1 45 (1999).

Option consommateurs, Enfants sous écoute : la protection de la vie privée dans l'environnement des jouets intelligents, par Option consommateurs, Montréal, Québec, Commissariat à la protection de la vie privée du Canada, 2018.

———, 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, par Option consommateurs, Montréal, Québec, Commissariat à la protection de la vie privée du Canada, 2019.

———, Mémoire sur le projet de loi 64 sur la protection des renseignements personnels Commission des institutions de l'Assemblée nationale, 2020) [unpublished].

———, La publicité destinée aux enfants : Identifier la meilleure protection possible, par Option consommateurs, Montréal, Québec, Bureau de la consommation d'Industrie Canada, 2008.

———, 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?, par Option consommateurs, Montréal, Québec, Bureau de la consommation d'Industrie Canada, 2015.

Roca, Guillermo Escobar, Informe 2016. Tema monográfico: la protección de datos de los menores de edad, por Guillermo Escobar Roca, dialnet.unirioja.es, Madrid, España, Red Iberoamericana de Protección de Datos, 2017.

Rymanowicz, Kylie, Keeping Kids Safe: How Child Sexual Predators Groom Children, by Kylie Rymanowicz, États-Unis, Michigan State University Extension (MSU), 2020.

The Sex Information and Education Council of Canada [SIECCAN], Sexting: Considerations for Canadian Youth, by The Sex Information and Education Council of Canada [SIECCAN], Sexualityandu.ca, 2011.

Thierer, Adam D, Kids, Privacy, Free Speech & the Internet: Finding the Right Balance, SSRN Scholarly Paper, by Adam D Thierer, papers.ssrn.com, SSRN Scholarly Paper ID 1909261, Rochester, NY, Social Science Research Network, 2011.

UNE JEUNESSE, Quelle est la situation au Canada? : L'indice canadien du bien-être chez les enfants et les jeunes, par UNE JEUNESSE, UNICEF Canada, 2019.

US Department of Justice, The national strategy for child explotation prevention and interdiction, by US Department of Justice, États-Unis, United States Congress, 2010.

Wezum, observatorio joven, Primer informe global sobre cyberbullying, by Wezum, observatorio joven, Fundación Pontificia Scholas Occurrentes, 2019.

Guides et directives

Canadian Marketing Association, Guidelines for Marketing to Children and Teenagers, 2007

Commissariat à la protection de la vie privée du Canada, « Guide sur la protection de la vie privée à l'intention des entreprises », (24 décembre 2015), en ligne: <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/guide_org/>.

———, Lignes directrices pour l'obtention d'un consentement valable, 2018.

———, Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne, 2015.

Ministerio de Industria, Energía y Turismo, Guía de actuación contra el ciberacoso, Instituto Nacional de tecnologías de la comunicación [INTECO], 2014.

Office de la protection du consommateur du Québec, Publicité destinée aux enfants - Guide d'application des articles 248 et 249 Loi sur la protection du consommateur, 2012.

Poupart, Lise, La cyberviolence dans les relations amoureuses des jeunes: Guide pour les parents, Association québécoise Plaidoyer-Victimes, 2019.

R-U, Information Commissioner's Office, Guide: Children and the UK GDPR, ICO, 2020.

UIT, Directives pour la protection de l'enfance en ligne, destinées aux enfants, UIT, 2009.

Autres documents

Advertising Education forum, Children's data protection and parental consent, Research & Publication, 2013.AEPD, Guía de protección de datos para la prevención de delitos, AEPD, 2018.

Agencia española de protección de datos, Ficha didáctica: Situaciones de riesgo en el entorno Web 2.0: Suplantación de identidad, Ciberbullying, Grooming, Sexting.

Alliance médias jeunesse, La trousse numérique, par Alliance médias jeunesse, Société de développement de l'industrie des médias de l'Ontario et le Fonds des médias du Canada, 2015.

CE, Communication de la Commission au Parlement européen et au Conseil : La protection des données: un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique - deux années d'application du règlement général sur la protection des données, [2020], JO, C 264/2020 final.

Centre canadien de protection de l'enfance [CCPE], Fiche de prévention sur la cyberintimidation, Centre canadien de protection de l'enfance inc, 2017.

Centre Canadien de Protection de L'enfance [CCPE], Fiche de prévention sur le leurre, Centre canadien de protection de l'enfance inc, 2017.

Centre for Information Policy Leadership, GDPR Implementation in Respect of Children's Data and Consent, 2018.

Chambre des communes du Canada, Réponse du gouvernement au rapport du Comité permanent de 1' accès à 1' information, de la protection des renseignements personnels et de 1' éthique intitulé Vers la protection de la vie privée : Examen de la Loi sur la protection des renseignements personnels et les documents électroniques, ETHI 8512-421-344, 2016.

Clement, J, Cyber bullying - Statistics & Facts, Statista, 2019.

Commission scolaire des Draveurs, Le sextage, 2015.

É-U, Federal Trade Commission, Statement of Basis and Purpose: Children's Online Privacy Protection Rule; Final Rule, 16 CFR §312, vol 64, No. 12, 1999.

———, Statement of basis and purpose: Children's Online Privacy Protection Rule; Final Rule, 16 CFR §312, vol 78, No. 12, 2013.

Federal Trade Commission, Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business, 2013.

———, « COPPA Safe Harbor Program », (7 janvier 2015), en ligne: Fed Trade Comm <https://www.ftc.gov/safe-harbor-program>.

———, « Privacy online: a report to Congress », (1998), en ligne: <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>.

———, Proposed Rule; Request for Comment on Proposal to Amend Rule to Respond to Changes in Online Technology: Children's Online Privacy Protection Rule, 16 CFR §312, vol 76, No. 187, 2013.

———, Federal Trade Comission, « Largest FTC COPPA settlement requires Musical.ly to change its tune », (27 février 2019), en ligne: Fed Trade Comm <https://www.ftc.gov/news-events/blogs/business-blog/2019/02/largest-ftc-coppa-settlement-requires-musically-change-its>.

Fédération des associations de parents de l'enseignement officiel, L'évolution de la place de l'enfant dans la société, FAPEO, 2008.

Habilo médias, Marketing en ligne destiné aux jeunes : stratégies et techniques, Habilo médias, 2012.

Hinduja, Sameer & Justin W Patchin, « Sexting Laws Across America », en ligne: Cyberbullying Res Cent <https://cyberbullying.org/sexting-laws>.

Hinduja, Sammer & Justin W Patchin, Cyberbullying Fact Sheet: Identification, Prevention, and Response, Cyberbullying Research Center, 2019.

INTECO & Pantallas Amigas, Guía sobre adolescencia y sexting: qué es y cómo prevenirlo, 2011.

Josso-Bouchard, Helene, COPPA versus RGPD, L'académie d'Aix-Marseille, 2020.

Kredens, Élodie & Barbara Fontar, Les jeunes et Internet : de quoi avons-nous peur? par Élodie Kredens & Barbara Fontar, France, Fréquence écoles org, 2010.

Préposé fédéral à la protection des données [PFPDT] & plateforme nationale de promotion des compétences [Jeunes et Médias], Protection des données: Dossier d'information.

Statista Research Department, « Canada: internet user penetration by age 2019 », (31 août 2015), en ligne: Statista.com <https://www.statista.com/statistics/373955/canada-online-penetration-age/>.

Statistique Canada, Tableau : 35-10-0001-01: Cybercrimes déclarés par la police, selon l'infraction reliée à la cybercriminalité (certains services de police), Canada, 2020.

Steeves, Valerie, Jacquelyn Burkell & Anca Micheti, Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand, 2007.

UIT, « Let's work together to build a safer Internet for children: Doreen Bogdan-Martin », (5 février 2019), en ligne: ITU News <https://news.itu.int/lets-work-together-to-build-a-safer-internet-for-children/>.

———, Measuring digital development: Facts and figures 2020, ITU Publications, 2020.

UNICEF Argentina, ¿Qué es el ciberbullying?, UNICEF Argentina.

UNICEF Argentina & Ministerio de justicia y derechos humanos, Grooming: Guía práctica para adultos: Información y consejos para entender y prevenir el acoso a través de Internet, 2014.

Union internationale des télécommunications (UIT), Manuel pour mesurer l'accès des ménages et des particuliers aux TIC et l'utilisation de ces technologies, Service de la production des publications (PUBL) de l'UIT, 2020.

Entrée de dictionnaire et encyclopédie

Académie française, Dictionnaire de l'Académie française, 9e éd, France, 2011.

« Facebook » dans Wikipédia Encycl Libre.

Groupe de travail interinstitutionnel sur l'exploitation sexuelle des enfants 2016, « Sexting » dans Guide Terminol Pour Prot Enfants Contre L'exploitation L'abus Sex, Luxembourg, ECPAT International et ECPAT Luxembourg, 2017 122.

« Instagram » dans Wikipédia Encycl Libre.

Office québécois de la langue française (OQLF), Le Grand dictionnaire terminologique (GDT), Québec, 2008.

« Snapchat » dans Wikipédia Encycl Libre.
« Suicide d'Amanda Todd » dans Wikipédia.
« YouTube » dans Wikipédia Encycl Libre.

En ligne

Center for Media Education, « Web of Deception: Threats to Children from Online Marketing », (1996), en ligne: Democraticmedia <https://www.democraticmedia.org/article/web-deception-landmark-1996-report-triggered-coppa>.

Centrale canadienne de signalement des cas d'exploitation sexuelle d'enfants sur Internet (Cyberaide), « Le conditionnement », en ligne: Cyberaide.ca <https://cyberaide.ca/app/fr/child_sexual_abuse-grooming>.

« Comment les spécialistes du marketing ciblent les enfants », (25 mai 2012), en ligne: HabiloMédias <https://habilomedias.ca/litt%C3%A9ratie-num%C3%A9rique-et-%C3%A9ducation-aux-m%C3%A9dias/enjeux-des-m%C3%A9dias/publicit%C3%A9-et-consommation/comment-les-sp%C3%A9cialistes-du-marketing-ciblent-les-enfants>.Global Kids Online Canada, « The Canadian Kids Online project will investigate young Canadian's experiences in online environments. », en ligne: Glob Kids Online <http://globalkidsonline.net/gko-launching-in-canada-with-a-focus-on-privacy/>.

Jeunesse, J´écoute, « Qu'est-ce que le sextage ? », en ligne: jeunessejecoute.ca <https://jeunessejecoute.ca/information/quest-ce-que-le-sextage/>.

———, « Sextage et consentement : Faits importants », en ligne: jeunessejecoute.ca <https://jeunessejecoute.ca/information/sextage-et-consentement-faits-importants/>.

Jeunesse, J'écoute, « Sextage : la vie privée et la loi », en ligne: jeunessejecoute.ca <https://jeunessejecoute.ca/information/sextage-la-vie-privee-et-la-loi/>.

Le Curateur public du Québec, « Les droits du mineur - Tutelle des biens du mineur », en ligne: <https://www.curateur.gouv.qc.ca/cura/fr/mineur/tutelle-biens/droits/index.html>.

Ministère de la Justice du Canada, « Sextage : qu'est-ce que la loi permet? », (1 août 2018), en ligne: Cliquez-Justice <https://www.cliquezjustice.ca/vos-droits/sextage-qu-est-ce-que-la-loi-permet>.

Ministère de la Sécurité publique du Québec (MSP), « La cyberintimidation et le cyberharcèlement », (décembre 2009), en ligne: <https://www.securitepublique.gouv.qc.ca/police/publications-et-statistiques/statistiques/cyberintimidation/en-ligne.html>.

Ministère de la Sécurité publique du Québec [MSP], « Sextos- Échanger des photos intimes n'est pas un jeu d'enfants! », en ligne: <https://www.securitepublique.gouv.qc.ca/police/prevention-criminalite/semaine-de-la-prevention-de-la-criminalite/sextos.html>.

Rescue digital media, « Politique de confidentialité », en ligne: <https://fr.rescuedigitalmedia.com/politique-de-confidentialite>.

Sécurité publique Canada, « Qu'est-ce que la cyberintimidation? », (21 décembre 2018), en ligne: <https://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/cbrbllng/prnts/cbrbllng-fr.aspx#ftn1>.

Gautrais, Vincent, Consultations particulières et auditions publiques sur le projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, Québec, 2020.

x-Rouge canadienne, « La cyberintimidation », en ligne: Croix-Rouge Can <http://www.croixrouge.ca/nos-champs-d-action/prevention-de-la-violence-et-de-l-intimidation/educateurs/prevention-de-l-intimidation-et-du-harcelement/la-cyberintimidation>.

« À propos de l'Union internationale des télécommunications (UIT) », en ligne: UIT <https://www.itu.int:443/fr/about/Pages/default.aspx>.

« Children's Online Privacy Protection Rule: Not Just for Kids' Sites », (2 avril 2013), en ligne: Fed Trade Comm <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites>.

« Complying with COPPA: Frequently Asked Questions », (20 juillet 2020), en ligne: Fed Trade Comm <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0>.

« Droit à l'effacement | Autorité de protection des données », en ligne: <https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/droits-des-citoyens/droit-a-l-effacement>.

« FTC Staff Sets Forth Principles for Online Information Collection from Children », (16 juillet 1997), en ligne: Fed Trade Comm <https://www.ftc.gov/news-events/press-releases/1997/07/ftc-staff-sets-forth-principles-online-information-collection>.

« U.S. states with state sexting laws 2019 », en ligne: Statista <https://www.statista.com/statistics/509314/us-states-with-state-sexting-laws-policy/>.