**ORIGINAL TEXT IN FRENCH – COURTESY TRANSLATION**

Commission d'accès à l'information du Québec

Summary of the report:

# Ensuring a better protection for young people's personal information in the digital age

August 2022

This document aims to provide an overview of the main reflections and proposals presented in the full version of this report, available (in French only) on the Commission's website:

http://www.cai.gouv.qc.ca

# 1. INTRODUCTION

The recent reform of privacy laws[1] (hereinafter referred to as Law 25) adds an explicit safeguard for young people to the *Act Respecting the Protection of Personal Information in the Private Sector*[2] : under the age of 14, the parent or tutor must consent to the collection of personal information from the minor or to its use or communication for other purposes. Between the ages of 14 and 17, the minor can consent on his or her own, but the parent or tutor can continue to do so.

In its report, *Ensuring a better protection for young people's personal information in the digital age*, the Commission d'accès à l'information (the Commission) considers the adequacy of this measure at the request of the Minister responsible for Access to Information and Protection of Personal Information. The Minister has mandated the Commission to examine and make recommendations on whether additional measures should be considered in the Private Sector Privacy Act to further protect minors under the age of 14 in the context of the collection or use of their personal information for commercial purposes or commercial profiling.

The Commission's work focused in particular on the digital environment, which offers many opportunities, but also poses significant risks for the fundamental rights of young people, including the right to privacy. Throughout the world, these risks are of growing concern. Initiatives calling for stronger protections for young people in the digital world, including with respect to privacy, are multiplying. Many jurisdictions are currently considering legislation or standards that include such provisions. In the preparation of this report, the Commission was inspired in particular by this international work, but also by studies conducted among young people and their parents.

At the end of its reflection, the Commission finds that the vulnerability of young people and the very significant asymmetry of power they have with businesses argues in favor of reinforced legal protection. It believes that additional measures are required in order to protect young people from commercial exploitation, among other things.

In line with the reform of the Private Sector Privacy Act and the spirit of the *Consumer Protection Act*[3], which prohibits commercial advertising directed at children, the Commission recommends prohibiting the collection, use and communication of personal information about minors for advertising or profiling purposes and for any other purpose that are known or reasonably believed to cause harm to minors. It also recommends strengthening the accountability of businesses that profit from personal information of

---

1 *An Act to modernize legislative provisions as regards the protection of personal information*, SQ 2021, c 25.

2 *Act respecting the protection of personal information in the private sector*, CQLR, c P-39.1, hereinafter referred to as Private Sector Privacy Act.

3 *Consumer Protection Act*, CQLR, c P-40.1, hereinafter referred to as CPA.

minors and clarifying certain aspects of the law, for the benefit of both minors and businesses, given the significance of the penalties that businesses may face as of 2023 in the event of a violation of the law. Lastly, it suggests increased efforts in education and awareness regarding the digital environment and the right to privacy. The Commission's full recommendations are presented in section 6 on page 15**Erreur ! Signet non défini.**.

# 2. PRINCIPLES AND CONCEPTS

In its report, the Commission draws on a number of principles and concepts, about which it first gives some details.

## Internationally recognized principles and rights

Like much international literature and research dealing with the protection of the personal information of minors, the Commission's report is based upon the principles and rights set out in the United Nations Convention on the Rights of the Child[4], which concerns all children under 18. The Commission also considers General Comment No. 25 of the UN Committee on the Rights of the Child[5], which clarifies the application of the Convention in the digital environment.

The Convention is based on the following principles:

- **Nondiscrimination**: The rights in the Convention apply to every child, without distinction. In the digital environment, discrimination can occur, for example, when unfairly obtained information is used in an automated decision-making process involving a child.
- **Best interests of the child**: Decisions made about the child, whether by the child's entourage or by external actors, including the State, must prioritize the respect of the child's rights and the satisfaction of his or her particular needs.
- **Right to life, survival and developement**: Every child has the right to live and to develop fully, mentally, emotionally, cognitively, socially and culturally. States must take the necessary measures to reduce the risks that minors face in the digital environment.
- **Participation**: The child's views must be considered when decisions are made about him or her.
- **Evolving capacities:** The child's need for protection gradually diminishes as he or she acquires knowledge and skills that give him or her greater autonomy in

[4] UNITED NATIONS, *Convention on the Rights of the Child*, (1989), treaty no. 27531, online : <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>, hereinafter referred to as the Convention.

[5] UN COMMITTEE ON THE RIGHTS OF THE CHILD, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, 2021, online: < https://daccess-ods.un.org/tmp/2996619.34375763.html>.

realizing his or her rights. States should ensure that digital services respect the developmental stage of the child, which affects the likelihood and severity of risks.

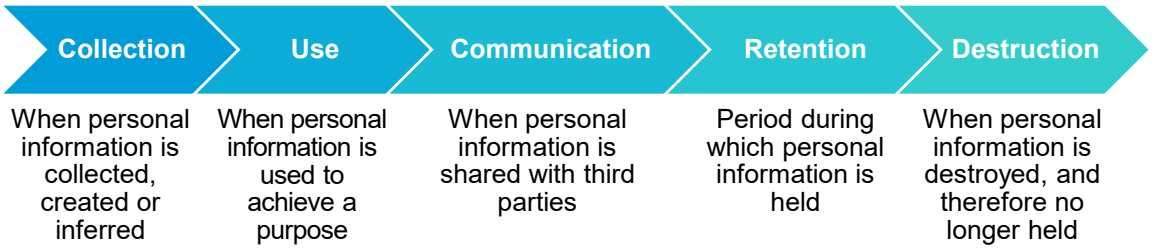
The Convention also recognizes many rights to children. Several of these are relevant when businesses collect, use, communicate or retain personal information about children:

- Right to freedom of expression and thought;
- Right to privacy;
- Right to information;
- Right to rest and leisure, to engage in play and to participate freely in cultural life and the arts;
- Right to be protected from economic exploitation or against all other forms of exploitation prejudicial to their welfare.

Many current digital practices pose risks to these rights.

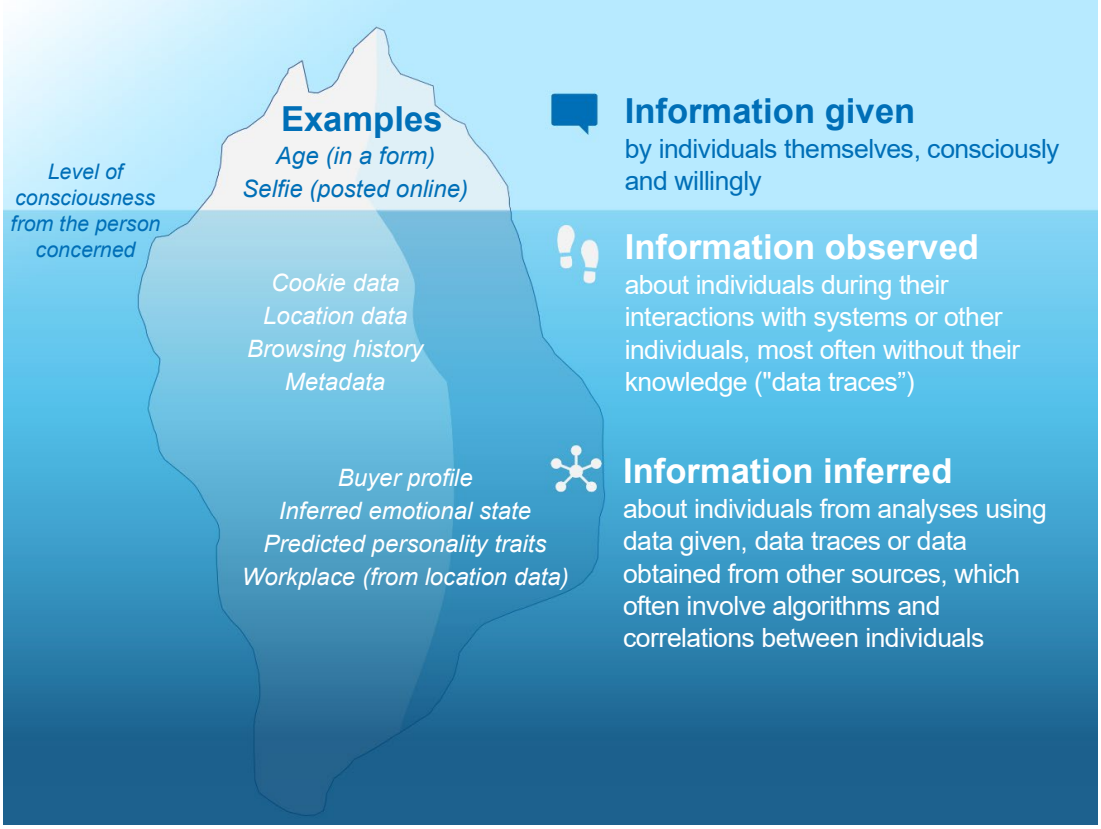
## Personal information lifecycle and typology

The Private Sector Privacy Act provides safeguards to protect personal information from their collection to their destruction. There are five stages in this lifecycle:




Moreover, in the digital age, classifying personal information according to the mechanism by which it is acquired helps to refine our understanding of the issues. Based on the work of legal scholar Simone van der Hof[6], the Commission distinguishes three categories of personal information, which refer to the way it is obtained by businesses. The iceberg metaphor is used to represent those categories:

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




## Dimensions of digital privacy

The Commission's report refers to three "dimensions of digital privacy" (interpersonal, institutional, commercial), which are taken from research on protecting youth in the digital environment.[7] These dimensions shed light on different privacy issues faced by minors.

- **Interpersonal privacy** relates to how personal information is managed through the minor's relationships with **other people**. It mainly involves information provided by the minor himself or herself.
- **Institutional privacy** relates to the collection and management of personal information about the minor by **public bodies**. The personal information it involves is either given by the minor or observed – records (such as medical or academic) are an example.
- **Commercial privacy** relates to the collection, use, communication or retention of a minor's personal information by **businesses.** Most commercial activities are based on observed data (for example, through metadata or cookies) or inferred data (for example, through profiling).

[7] Mariya STOILOVA, Sonia LIVINGSTONE and Rishita NANDAGIRI, *Children's data and privacy online*, The London School of Economics and Political Science, 2021, online : <https://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf>.

## Scope of the Commission's analysis

Based on the elements presented in this first part, the Commission clarifies the scope of the mandate that led to this report:

- The Commission's analysis considers **all young people under the age of 18, including 14- to 17-year-olds.** Unless ortherwise stated, the term "minor" refers to those under 18.
- Given that digital technology now plays a prominent role in young people's lives, the Commission focuses on the protection of personal information **in the digital environment**.
- In light of the Minister's request, commercial privacy is at the core of this report. On several occasions, however, the Commission makes links to **interpersonal privacy**.
- Since all stages of the personal information lifecycle involve specific risks, the Commission's analysis also considers the **communication and retention of personal information**, in addition to their collection and use.

# 3. CONTEXT

In order to inform its recommendations on measures to protect the personal information of minors, the Commission explores the characteristics of the digital environment in which they evolve, business practices, attitudes and knowledge of minors and their parents, and the risks to which minors are exposed in the digital environment. It concludes that their unique vulnerability warrants enhanced legal protection, like that provided by the CPA for commercial advertising directed at under-13s.

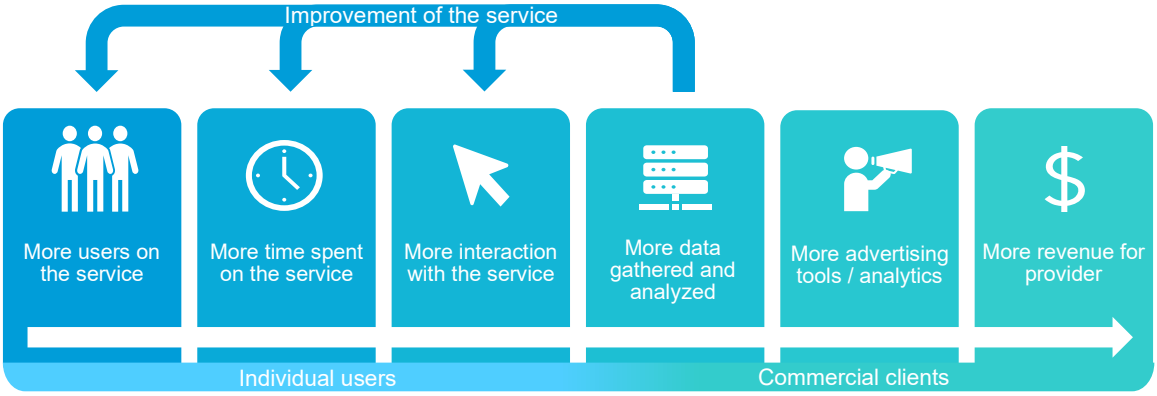
## Digital environment and business activities

The Commission first characterizes the digital environment, an essential part of young people's lives. It notes that this environment generates significant risks for minors. In fact, three major trends run through it and frame the interactions that take place in it:

- **Datafication:** Digital technology allows the collection of large amounts of data about individuals for exploitation, in an increasing number of contexts and at an increasing rate.
- **Hyperconnectivity:** Objects and places are now integrated into networks where people and organizations interact, which intensifies the use of data and blurs the boundaries between the physical and digital worlds.
- **Commercialization**: The digital environment is designed and operated primarily by businesses, which dictate its design and establish its features, usually following commercial imperatives.

The fast-paced nature of this environment is also a cross-cutting property. The combined effect of these forces on the privacy of minors and the realization of their rights is particularly important.

The Commission then looks at the current practices of businesses that provide digital products and services. It notes that the economic environment in which businesses operate today is driving them to collect more and more personal information. It has also led to business models that are problematic for the protection of personal information, such as behavioural advertising, which is a fundamental component of the so-called "attention economy", as illustrated in the following figure:




In this model, individuals are seen as both consumers and as resources that produce data. This data can be leveraged to attract more users to services and maximize the time they spend on them, but also used for advertising purposes by commercial clients. This value chain encourages the use of increasingly persuasive strategies based on design elements and algorithms that can be refined and made more powerful with the personal information collected.

There are also significant concerns about models that rely on the sale of personal information.

Since young people, who make up a third of Internet users, represent a particularly interesting customer base that can be retained in the long term, they are not left out of these practices and are sometimes specifically targeted. For example, connected toys and mobile applications designed for or popular with young people collect a lot of personal information, often without their knowledge, as some studies have shown.

## Characteristics of minors and their parents

The behaviors, attitudes, and knowledge of minors and their parents provide insight into how minors face and respond to digital risks. In particular, research indicates that both have limited digital literacy, which is further impacted by a lack of transparency in business practices, which puts them at a disadvantage.

Young people generally view privacy issues in terms of their interpersonal dimension (who can see what they post online) rather than in terms of what businesses collect about them

and how they use that information (commercial dimension). When presented with more details about the digital ecosystem in which they navigate, they express discomfort and describe certain practices related to algorithms, profiling, geolocation or targeted advertising as troubling and disturbing. Lastly, their perception of risk is also influenced by their interpersonal vision of this environment, which fits with the public discourse limited to online safety: cyberbullying, sexual predation, cyberstalking or hacking are thus at the heart of their concerns, since they have clearer consequences on their safety, reputation or dignity. Minors are also concerned about not always being followed by their parents.

Similar findings apply to parents. While they understand the basics, namely the trade-off that is often required between disclosure of personal information and provision of a digital service, parents also demonstrate a primarily interpersonal understanding of privacy. For example, they rely on audience restriction strategies when they want to protect the personal information about their children that they post on social networks. Similarly, they have little awareness of observed and inferred information. Their perception of risk also relates primarily to online safety.

## Digital risks for minors

For the purposes of its report, the Commission uses the CO:RE 4Cs classification. This classification distinguishes between content, contact, conduct and contract risks, which are articulated in three dimensions: aggression, sexuality and values. In addition, it identifies three cross-cutting risks: privacy, inequality and discrimination, and health risks.

All of these elements are summarized in the table below, which is adapted from the one proposed by researchers Sonia Livingstone and Mariya Stoilova[8]. The table also lists examples of risks that can be classified in each cell:

[8] Sonia LIVINGSTONE and Mariya STOILOVA, « The 4Cs: Classifying Online Risk to Children », *CO:RE Short Report Series on Key Topics* 2021, p. 12, DOI : 10.21241/SSOAR.71817. Table adapted according to the terms of the CC BY 4.0 FR license.

| | Content | Contact | Conduct | Contract |
|---|---|---|---|---|
| **Agressive** | Violent, gory, graphic, racist, hateful or extremist information and communication | Harassment, stalking, hateful behavior, unwanted or excessive surveillance | Bullying, hateful or hostile communication or peer activity e.g. trolling, exclusion, shaming | Identity theft, fraud, phishing, scams, hacking, blackmail, security risks |
| **Sexual** | Pornography (harmful or illegal), sexualization of culture, oppressive body image norms | Sexual harassment, sexual grooming, sextortion, the generation and sharing of child sexual abuse material | Sexual harassment, non-consensual sexual messaging, adverse sexual pressures | Trafficking for purposes of sexual exploitation, streaming (paid-for) child sexual abuse |
| **Values** | Mis/disinformation, age-inappropriate marketing or user-generated content | Ideological persuasion or manipulation, radicalization and extremist recruitement | Potentially harmful user communities, e.g. self-harm, anti-vaccine, adverse peer pressures | Gambling, filter bubbles, micro-targeting, dark patterns shaping persuasion or purchase |
| **Cross-cutting risks** | • **Privacy violations** (interpersonal, institutional, commercial; normalization of surveillance)<br>• **Physical and mental health risks** (e.g., sedentary lifestyle, excessive screen use, isolation, anxiety)<br>• **Inequalities and discrimination** (inclusion and exclusion, exploiting vulnerability, algorithmic bias/predictive analytics) | | | |

The CO:RE classification does not assume that each risk fits only in one cell of the table; indeed, risks are increasingly interrelated. In this regard, it is worth noting the important role of digital service providers in the emergence of the different risk types, due to their dominant position in all aspects of digital life. In addition to being able to directly drive contract risks, they manage, for example, the platforms where individuals interact, which can generate contact and conduct risks; they also host large amounts of digital content, whether created by users or organizations.

**Therefore, the choices made by businesses because of their commercial interests are not neutral**. They can significantly affect the likelihood and nature of risks of all kinds to which minors are exposed in the digital environment[9].

The Commission notes that personal information (given, observed and inferred) is central to the business models of online service providers. While not universal causes, its collection, use and communication can nonetheless open the door to the risks outlined in the table above. To illustrate this, section 3.3.2 of the report presents five fictional

[9] 5RIGHTS FOUNDATION, « Risky by design - Introduction », *Risky-By-Design* (2022), online : <https://www.riskyby.design/introduction> (consulté le 28 février 2022).

scenarios in which technical tools or design elements used by businesses generate risks to minors.

Also, the lack of certainty about the possible future uses of the information is important to consider, as is the social dimension of the potential harms – which may affect a *specific* minor, but also minors *as a group*.

### Reasons for action

Following this exploration of the contextual elements, the Commission concludes that privacy laws must provide for specific measures for minors. **These measures must maximize the opportunities available to them in the digital environment while minimizing the risks to which they are exposed.**

This is mainly due to the vulnerability of minors, who, among other things, navigate a digital environment designed primarily for adults, focus on the interpersonal management of the flow of their personal information, and are unable to be fully vigilant due to the complexity and opacity of commercial practices involving personal information. Other vulnerability factors often discussed in the field of consumer protection include: different reasoning abilities than adults, sensitivity to peer pressure and influence, and difficulty interpreting intentions. In short, minors are exposed to more potentially harmful situations and are also less equipped than adults to deal with them.

To the extent that many commercial practices exploit these vulnerabilities, there is a strong asymmetry of power between businesses and minors. For example, businesses control much of the design of the digital space and can mobilize innovative methods to influence young people's behaviors or intentions. These methods are often propelled by the large volume of data to which they have access.

The Commission notes that in other areas, Quebec society has put specific protections in place (e.g., sale of alcohol and tobacco, access to movies with restricted content, etc.). In particular, Quebec has chosen to prohibit commercial advertising directed at children under the age of 13. This prohibition, enshrined in the CPA, reflects a true societal choice to place the best interests of children above commercial interests. In section 3.4.2, the Commission draws several parallels between this prohibition and the issue examined in its report, recalling that the protection of minors from economic exploitation in a digital economy where their data is used for commercial purposes remains more important than ever.

# 4. MEASURES TO PROTECT MINORS

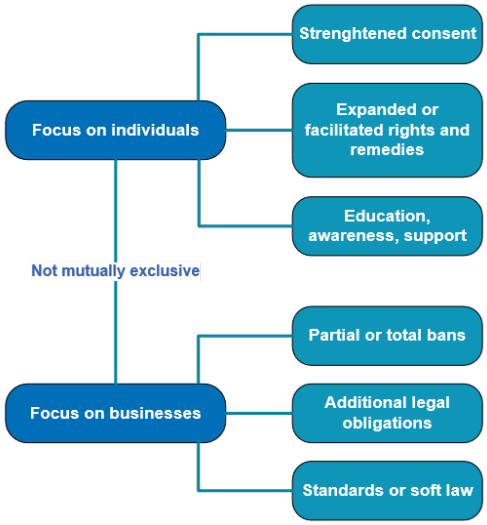
Having established the need for special protection for minors with respect to their personal information, the Commission assesses in this section the ways in which this can be achieved, based on its past recommendations and on the documentation prepared by several international or national organizations. Over the past decade or so, a growing body

of supra-governmental, governmental, and non-governmental work in various jurisdictions has provided policymakers with guidance on this issue.

There are many points of convergence. The Commission finds that in order to achieve the goal of maximizing the opportunities offered by the digital environment while minimizing the risks posed by it, there are essentially two approaches that can be taken – although they are not mutually exclusive:

- Focusing on **individuals** to improve their capacity to act and their knowledge (prevention) or so that they can act after the fact (remedies and rights). It should be noted that these measures may take the form of obligations incumbent on businesses; however, they place the main burden of protection on individuals.
- Focusing on **businesses** to reinforce their obligation of protection (prevention) in order to prevent harm to minors.

The following figure summarizes the broad categories of measures presented in section 4 of the report, which constitutes a benchmarking exercise prior to the Commission's recommendations. These categories are derived from analyses conducted by various organizations, laws, regulations and standards in Quebec and internationally.




For example, enshrining the principle of the best interests of the child into privacy legislation would not only clarify the weighing of interests in certain conflicting situations between individuals, but would also set the tone for organizations to make decisions that impact on the privacy of minors. In sections 4.1.1 to 4.1.3 of its report, the Commission provides more detail about each measure identified in the literature reviewed.

In section 4.2, it analyzes how the following 13 legislative frameworks[10] give effect to these measures:

[10] The full references of these frameworks are given at the beginning of section 4.2 of the report.

| # | Jurisdiction | Legislation or bill | Abbreviation |
|---|---|---|---|
| 1 | European Union | *General Data Protection Regulation* | GDPR |
| 2 | European Union | *Digital Services Act* | DSA |
| 3 | European Union | *Artifical Intelligence Act* | AIA |
| 4 | United Kingdom | *Data Protection Act 2018* | DPA18 |
| 5 | United States (federal) | *Children's Online Privacy Protection Act* | COPPA |
| 6 | United States (federal) | *Kids' Online Safety Act* | KOSA |
| 7 | California | *California Age-Appropriate Design Code Act* | CAADCA |
| 8 | Colorado | *Colorado Privacy Act* | CPA |
| 9 | Washington state | *Washington Privacy Act* | WPA |
| 10 | Canada (federal) | *Digital Charter Implementation Act, 2022* (bill C-27) | C-27 |
| 11 | Ontario | Government white paper on a potential future provincial private sector privacy act | OWP |
| 12 | India | *Personal Data Protection Bill 2019* | PDPB |
| 13 | Brazil | *Lei Geral de Proteção de Dados Pessoais* | LGPD |

The table on the next page is a summary of section 4.2. It is intended to facilitate the comparison of legal frameworks, but it is not exhaustive. The overview provided, which is the result of extensive research but not legal analysis, necessarily minimizes the nuances that apply in each jurisdiction, but does give an indication of the extent of the measures implemented or contemplated in each regime and the interaction between them.

| | Loi ou projet de loi | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | GDPR | DSA | AIA | DPA18 | COPPA | KOSA | CAADCA | CPA | WPA | C-27 | OWP | PDPB | LGPD |
| **Measures** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** |
| Parental consent up to a certain age threshold | 13-16 | GDPR | GDPR | 13 | 13 | COPPA | CERT<br>CCPA | 13 | 13 | PART | 13-16 | 18 | 18 |
| Information adapted to children's capacities | | | | | | | | | | | | | |
| Right to de-indexation | | | | | | | | | | | | | |
| Right to deletion | | | | | | | CCPA | | | | | CERT | |
| Prohibition (total or partial) on profiling / automated decisions | POT | | | CC | | | PART | | | | | | |
| Prohibition (total or partial) on targeted advertising | | | | | | | POT | | SENS | | | | |
| Prohibition (total or partial) on using children's PI in ways harmful to them | | | | CC | | IND | | | | | | | |
| Prohibition (total or partial) on dark patterns | | | | CC | | | | | CERT | | | | |
| Prohibition (total or partial) on communicating children's PI | | | | CC | | | | | | IND | | | |
| Children's PI explicitly identified as sensitive by law | | | | | | | | | | | | | |
| Automatic requirement for an impact assessment if children's PI are used | DPAs | | | CC | | IND | | | | | | | |
| Age assurance/verification by service providers | POT | | | CC | | | | | | | | | |
| "Highest privacy" settings by default | | | | | | | | | | | | | |
| Adoption of a code of practice | | PART | | | | | | | | | | | |
| Explicit reference to the best interests of the child | IND | | | CC | | | | | | | | | |

**Legend**

| | |
|---|---|
| | Included |
| | Potentially/partially |
| | Other document/law |
| CC | *Children's Code* (United Kingdom) |
| CCPA | *California Consumer Privacy Act* |
| DPA | National lists of processing operations subject to impact assessments (established by european data protection authorities) |
| POT | Potentially |
| CERT | Only in certain cases |
| SENS | Only on the basis of sensitive information |
| PI | Personal information |
| IND | Indirectly |
| PART | Partially |

Beyond these legal mechanisms, some European jurisdictions have developed standards for businesses to better protect the personal information of minors. In section 4.3 of the report, the Commission describes initiatives in Ireland, the Netherlands and France, which are essentially similar to the *Children's Code* developed by the Information Commissioner's Office in the United Kingdom[11], considered to be the first example of such a standard. These documents bring together principles for the collection, use and communication of personal information and design principles for businesses designing products and services likely to be accessed by minors.

# 5. Analysis of Law 25

In this section of its report, the Commission analyzes the relevant provisions of Law 25 in light of both the contextual elements presented earlier and the international legislations, standards and documents consulted, in order to assess whether the new obligations mitigate some of the identified risks. In the Commission's view, parental consent, which is the main element of specific protection for minors, is insufficient.

Among the substantial changes that Law 25 makes to the Private Sector Privacy Act, several can have a positive impact on the protection of minors. The Commission welcomes the progress in this area. The following table, which is based on the one on page 12, sets out some of the measures affecting minors in the Quebec legal framework as amended by Law 25.

| Measures | PSPA |
|---|---|
| Parental consent up to a certain age threshold | 14 |
| Information adapted to children's capacities | |
| Right to de-indexation | |
| Right to deletion | CERT |
| Explicit prohibition (total or partial) on profiling / automated decisions | PART |
| Explicit prohibition (total or partial) on targeted advertising | |
| Explicit prohibition (total or partial) on using children's PI in ways harmful to them | |
| Explicit prohibition (total or partial) on dark patterns | |
| Explicit prohibition (total or partial) on communicating children's PI | |
| Children's PI explicitly identified as sensitive by law | |
| Automatic requirement for an impact assessment if children's PI are used | |

**Legend**

| | |
|---|---|
| | Included |
| | Potentially/partially |
| CERT | Only in certain cases |
| PART | Partially |
| PI | Personal information |

[11] Information Commissioner's Office, *Age appropriate design: A code of practice for online services*, 2020, online: <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf>.

| Measures | PSPA |
|---|---|
| Age assurance/verification by service providers | |
| “Highest privacy” settings by default | PART |
| Adoption of a code of practice | |
| Explicit reference to the best interests of the child | |

Until the age of 14, the person having parental authority or the tutor of the minor is responsible for consenting to the collection of personal information from the minor or to its use or communication for purposes other than those for which it was collected[12]. From the age of 14 until majority, both the parent (or tutor) and the minor may consent. Consent will not be required in cases where the collection or use is clearly for the minor's benefit. This measure applies in both the physical and digital world.

The Quebec legislation as amended also provides for a right to de-indexation based on the fact that personal information relates to a minor, a right to deletion in certain circumstances, the disabling of profiling by default, and the requirement to set the settings of technology products and services to the highest level of privacy by default. In addition, other provisions related to transparency, sensitivity of information or privacy impact assessments reinforce accountability and are likely to have a protective effect for minors.

Although diverse, these measures may not be fully effective in preventing the risks for minors’ rights. In particular, the main provision that specifically targets minors – parental consent – suffers from significant limitations:

- The free and informed nature of consent may be challenged by certain parameters of the digital environment; for example:
  - Interfaces are not always neutral and can nudge choices;
  - Refusing the collection, use or communication of personal information often means giving up a digital product or service, which can have important consequences for the socialization of minors;
  - Business practices are opaque and complex;
  - Choices must be made instantaneously;
- Parental consent involves setting a threshold age above which it is no longer required and, potentially, verifying the minor’s age and relationship to the adult consenting on his or her behalf – those verifications present some real technical challenges;
- The parent’s and minor’s interests are not always aligned, and parental consent can in some cases be detrimental to the minor’s autonomy;
- Consent is an act of individual control, whereas many of the risks minors face in the digital environment are systemic in nature and are generated by businesses: placing the burden of protection on parents or teenagers is a form of imbalance.

[12] Private Sector Privacy Act, sect. 4.1 and 14.

Thus, in line with the objectives of the reform brought by Law 25 and considering the limits of consent, which are recognized by businesses themselves, the Commission believes that additional measures must be considered to limit certain purposes and increase businesses' accountability in order to protect minors.

# 6. RECOMMENDATIONS AND PERSPECTIVES

At the end of the analysis presented in the report, the Commission concludes that **the Private Sector Privacy Act should be improved in order to better protect minors in the context of the collection, use or communication of their personal information for commercial purposes or for commercial profiling.** It makes 12 recommendations regarding the measures that should be put in place, reviews the criteria for their application and offers some concluding remarks.

## Recommendations

**Recommendation 1:** The Commission recommends that the Private Sector Privacy Act include an explicit prohibition against collecting, using or communicating personal information about a minor (under the age of 18):

a) for the purpose of commercial advertising or commercial prospection, whether directed at the minor himself or herself, another person or a group sharing certain characteristics with the minor;

b) for the purpose of influencing the minor's behavior or decisions, or that of another person or group sharing certain characteristics with him or her, in a commercial setting;

c) for any other purpose that is known or reasonably believed to be likely to cause substantial harm to that minor or minors in general (e.g., discrimination, harm to physical or mental well-being, body image distortion, etc.).

**Recommendation 2:** The Commission recommends that the Private Sector Privacy Act include an explicit prohibition against the sale of personal information about a minor (under the age of 18) in any circumstances, even with consent.

**Recommendation 3:** The Commission recommends that the Private Sector Privacy Act be amended to make it explicit that inferred or created personal information is included within its scope and brings about the same obligations, rights and remedies as other personal information.

**Recommendation 4:** The Commission recommends enshrining, in the Private Sector Privacy Act:

a) the best interests of the child (noting that this principle must guide the interpretation of the law);

b) the right to express his or her opinion on matters of interest to him or her;

c) the right to be heard in all proceedings affecting him or her.

**Recommendation 5:** The Commission recommends that the Private Sector Privacy Act be amended so that businesses have a special duty of care to all minors, taking into account their age category; in particular, with respect to transparency, the law should require businesses to adapt the information they provide to the age and capacities of the minors concerned and to provide it just-in-time, using non-textual formats (e.g., images, videos, etc.) where appropriate.

**Recommendation 6:** The Commission recommends that the Private Sector Privacy Act be amended to give precedence to the opinion of a minor older than 14 over that of a parent or tutor for the purposes of consent, refusal to consent or withdrawal or consent.

**Recommendation 7:** The Commission recommends that the Private Sector Privacy Act be amended to clearly state that the functions that allow a person to be identified, located or profiled must be disabled by default.

**Recommendation 8:** The Commission recommends that the privacy settings of third-party cookies be covered by the first paragraph of section 9.1 of the Private Sector Privacy Act, at least in cases where such cookies are likely to concern a minor.

**Recommendation 9:** The Commission recommends requiring that the evaluation of projects involving personal information about minors also consider the potential impact on other fundamental rights of minors.

**Recommendation 10:** The Commission recommends that the Private Sector Privacy Act include an explicit prohibition against using dark patterns that affect the protection of personal information of minors.

**Recommendation 11:** The Commission recommends providing a framework for the design of digital products and services, for example by requiring simple mechanisms for minors or their parents to exercise their rights of access, rectification, de-indexation and portability or by stipulating that manufacturers of connected devices must provide full information on the packaging.

**Recommendation 12:** The Commission recommends allocating more resources to education and outreach about how the digital environment works, its benefits and risks, and personal information rights, including:

a) by incorporating these concepts into the general education curriculum and by giving them sufficient importance;

b) by increasing the Commission's budget so that it can fully fulfill its promotion and awareness-raising function with young people.

## Application criteria

The Commission has assessed the criteria that could be used to circumscribe the application of certain additional safeguards. While the Commission believes that many of its recommendations must apply broadly, it recognizes that it would not be proportionate to require all businesses, regardless of their sector, to adapt information to children or to change the design of their services, for example.

Based on existing international models, the Commission suggests that businesses offering products and services "likely to be accessed by minors" ("likely" meaning with a probability of more than 50%) should be subject to additional obligations.

## Perspectives

The Commission concludes its report by the following remarks:

1. If the Commission's recommendations are implemented, it will be important to hold discussions with groups of children and teenagers, respecting the right of minors to express their opinions on matters that concern them.
2. The Commission des droits de la personne et des droits de la jeunesse [Human Rights and Youth Rights Commission], with its expertise in fundamental rights, should be consulted when considering how to implement the recommendations put forward in the report. Similarly, input from other agencies, such as the Office de la protection du consommateur [Consumer Protection Office], could be helpful.
3. The interaction between the exercise of personal information rights, such as consent, and contract law should be further explored.
4. While the report addresses the issue of private sector activities on young people, it does not touch on issues related to the public sector. The collection, use and communication of personal information by public bodies would benefit from further examination, particularly as artificial intelligence is increasingly put forward in education and as the number of public-private partnerships is growing in schools (e.g., educational technologies, surveillance systems, etc.).
5. The Commission's report does not address in detail the issues of online age verification and verification of parental consent. They have received considerable international attention because of the technical and legal challenges involved and the data minimization and anonymity issues associated with them. Moreover, the introduction of parental consent into the Private Sector Privacy Act implicitly raises the possibility of the roll-out of verification mechanisms. The Commission will therefore continue to monitor these issues closely.