unesco
Global Education Monitoring Report

ED/GEMR/MRT/2023/P1/x

Background paper prepared for
the Global Education Monitoring Report

Technology and education

Technology and education in light of human rights

RIGHT TO EDUCATION INITIATIVE (RTE)

2023

ABSTRACT

In her 2022 Report on the impact of the digitalisation of education on the right to education, the United Nations Special Rapporteur on the right to education clarified that any introduction of digital technologies in education must be framed around the right of every person to public, free, quality education and the commitments of states in this regard both under international human rights law and Sustainable Development Goal 4. This paper affirms that state obligations under the human rights framework must be the starting point for assessing and responding to discussions related to the monitoring of children's activities and the collection and use of their data in the field of education. Part 2 outlines the international and regional human rights legal framework that governs the relationship between technology and education, providing a baseline upon which states can verify compliance with international human rights law and useful guidance for anyone seeking to understand the impacts of existing and emerging educational products and services. Part 3 then provides a comparative analysis of the regulation of technology and education in ten countries, through an examination of current data protection, education and related legislation, for the purpose of understanding how different countries are paying attention to and addressing key human rights issues with regards to technology in education in practice.

1.Introduction

The use of technology in the education context (EdTech)[1] has increased rapidly in recent years, ranging from laptops, video, interactive whiteboards and associated equipment, to websites, online learning platforms, programs or applications, and more. This trend was further accelerated by the COVID-19 pandemic, which led to an estimated 90 per cent of the world's student population affected by school closures and a corresponding shift to temporary online education.[2]

Depending on its form, EdTech has the potential to facilitate learning and connection across time and distance, as well as respond to individual circumstances such as disability and contribute to the longer-term evolution of teaching methods. At the same time, significant challenges exist in relation to corporate profit motivations, government or school censorship of online materials, and the broader impacts of technology on personal and societal development and cohesion.

In this paper, we look specifically at concerns arising in connection with the collection and use of learners' data through the use of EdTech.[3] Such issues include the lack of choice regarding the use of EdTech (when mandated by schools or governments); insufficient, and a lack of age-appropriate, information regarding the terms of such use; the surveillance and collection of significant amounts of data from learners (extending to their physical locations, personal details, product and program usage, academic performance, among other information); and the storage, use or sale of such data for purposes unrelated to education, particularly as led by financial motives or political interests. Also considered is the lack of any, or appropriately updated, government assessment, oversight or regulation related to a rapidly developing sector, as well as the challenges associated with ensuring accountability or access to justice in connection with EdTech-related harms.

This paper affirms that State obligations under the human rights framework must be the starting point for assessing and responding to such concerns. Part 2 outlines the international and regional human rights legal framework that governs the relationship between technology and education, providing a starting point and useful guidance for anyone seeking to understand the impacts, particularly on children, of existing and emerging EdTech products and services. Part 3 then provides a comparative analysis of the regulation of EdTech in ten countries, through an examination of current data protection, education and related legislation, for the purpose of understanding how different countries are paying attention to and addressing key human rights issues in practice.

2.The international and regional human rights legal framework as it relates to the relationship between children, technology and education

This part outlines the application of the international and regional human rights legal framework to EdTech. It begins with a brief introduction to the human rights framework, including with reference to State obligations, corporate

[1] Technology in education and EdTech are hereby used interchangeably. For the purposes of this paper, technology in education means 'any technology — including hardware, software and digital content—designed or appropriated for (any) educational purpose' as well as 'any companies that produce products for the educational sector — hardware (equipment) and software (applications, programs and systems). (Hennessy, S., Jordan, K., Wagner, D. and Ed Tech Hub Team. 2021. Problem analysis and focus of EdTech Hub's Work: technology in education in low- and middle-income countries. EdTech Hub. (Working Paper 7.), p.8; and Fernanda Campagnucci, Following the pandemic: The dilemma around digital rights in education. In Campanha Latinoamericana por el Derecho a la Education (CLADE), Human right to education: horizons and meanings in the post pandemic, p. 2-32)

[2] See, for example: UNESCO, *Supporting learning recovery one year into COVID-19: the Global Education Coalition in action* (2021), p.7.

[3] Other issues relevant to the enjoyment of children's human rights in relation to EdTech but beyond the scope of this paper include but are not limited to equal accessibility to EdTech for all children; the quality and age-appropriate nature of EdTech materials; the impacts of EdTech on children's physical, cognitive and social development; and the safeguarding of children from cyberbullying, exploitation, abuse, harmful content arising through the use of EdTech.

activities, key principles related to children's human rights, followed by discussion of the human rights of most relevance to this topic, namely the right to education and right to privacy. It then provides an overview of more specific guidance, released by UN treaty bodies and UN experts in recent years, in relation to children, technology and education.

2.1.The human rights framework

2.1.1.States' human rights obligations

The human rights framework sets out the long-standing, global recognition of the basic rights and freedoms enjoyed by every person in the world, throughout their lives. All human rights are universal, inalienable, indivisible, and interdependent. They encompass civil, cultural, economic, political, and social rights, to be enjoyed without discrimination, and are inherent to all people, regardless of nationality, sex, national or ethnic origin, colour, religion, language, or any other status.

Under international law, states have obligations and duties to respect, protect and fulfil human rights, so that they: refrain from interfering with or curtailing the enjoyment of human rights; protect individuals and groups against human rights abuses by third parties; and take positive action to facilitate the enjoyment of basic human rights in practice. Where human rights violations or abuses by non-state actors occur, governments have an obligation to ensure effective remedies are available. Such remedies, including as experienced by children in relation to EdTech contexts, must be widely known; readily available; ensure prompt, thorough and impartial investigation of alleged abuses; and be capable of ending ongoing harm.[4]

2.1.2.Key principles in children's rights

Children's rights are human rights, and all children everywhere are entitled to the full range of human rights under the international human rights framework. Their rights are further enshrined in the Convention on the Rights of the Child, the most ratified human rights treaty in the world, which also affirms the special status of, and safeguards afforded to, children. These include the following four principles, through which the implementation of all other rights in the Convention should be viewed: the right to non-discrimination (article 2); best interests of the child (article 3(1));

[4] ICCPR, Article 2(3); UN HRC, *The right to privacy in the digital age. Report of the United Nations High Commissioner for Human Rights*, UN Doc. A/HRC/39/29 (3 August 2018), paras. 50-57; CRC, *General Comment No. 16 on State obligations regarding the impact of the business sector on children's rights*, UN Doc. CRC/C/GC/16 (17 April 2013), para. 4; CRC, *General Comment No. 25 on Children's rights in relation to the digital environment*, UN Doc. CRC/C/GC/25 (2 March 2021), para.

the right to life, survival and development (article 6); and the right of the child to be heard (article 12).[5] Children also have special protections against violence, and economic, sexual and other forms of exploitation.[6]

2.1.3.Human rights and corporate activities

The UN Guiding Principles on Business and Human Rights (UNGPs) represent the authoritative global standard for preventing and addressing human rights harms connected to business activity, setting out the distinct but complementary role of states and companies in preventing and addressing business-related human rights harms.[7]

The UNGPs are comprised of three separate but mutually reinforcing pillars, namely: the *State duty to protect* against human rights abuses by third parties, including businesses, through appropriate policies, regulation and adjudication (Pillar I); the *corporate responsibility to respect* human rights, by not infringing on the rights of others, and to address adverse impacts on human rights related to their activities (Pillar II); and *access to remedy* for victims of corporate-related human rights abuse through judicial or non-judicial mechanisms (Pillar III).

In order to meet their responsibility to respect human rights, companies should have in place policies and processes including a human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights, and processes to remedy rights abuses which they caused or to which they contributed.[8] [UNGP principles 15, 22]

Further, the UN Committee on the Rights of the Child has emphasised that while voluntary actions of corporate responsibility by companies can advance children's rights, these 'are not a substitute for State action and regulation of businesses in line with obligations under the Convention and its protocols or for businesses to comply with their responsibilities to respect children's rights.'[9]

2.2.International human rights framework relating to technology and education

Across different contexts, the specific human rights impacted by EdTech will vary. However, there are certain human rights which are likely to be particularly relevant as ones vulnerable to violation or abuse, and also important as a lens through which to assess laws, policies or practices. These include: the right to education; the right to privacy; the right to freedom of thought, conscience and religion; the right to freedom of opinion and expression, including

[5]CRC, General Comment No. 5 on General measures of implementation of the Convention on the Rights of the Child, UN Doc. CRC/GC/2003/5 (27 November 2003), para. 12; CRC, General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration, UN Doc. CRC/C/GC/14 (29 May 2013); CRC, General Comment No. 16 on State obligations regarding the impact of the business sector on children's rights, UN Doc. CRC/C/GC/16 (17 April 2013), paras. 13-23.

[6] The CRC provides that States shall encourage the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being (Article 17(e)) and ensure the protection of the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse (Article 19). Further, two of the Optional Protocols cover the protection of children in specific contexts, namely armed conflict (OPAC) and as related to the sale of children, child prostitution and child pornography (OPSC).

[7] UN HRC, *Human rights and transnational corporations and other business enterprises*, UN Doc. A/HRC/RES/17/4 (6 July 2011); UN HRC, *Guiding Principles on Business and Human Rights*, available at: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf (UNGPs).

[8] UNGPs, Principles 15 and 22.

[9] CRC, General Comment No. 16 on State obligations regarding the impact of the business sector on children's rights, UN Doc. CRC/C/GC/16 (17 April 2013), para. 9.

the right to seek, receive and impart information and ideas of all kinds, regardless of frontiers;[10] the right to freedom of association and peaceful assembly; the right to health (particularly regarding access to information and support related to health and well-being); and the right to culture, leisure and play. Further, all human rights legal provisions must be read in conjunction with the principles of non-discrimination and equality.

2.2.1.The right to education

Of obvious relevance to EdTech, the right to education has been widely recognised by governments around the world through a number of international instruments, including the Universal Declaration on Human Rights,[11] International Covenant on Economic, Social and Cultural Rights,[12] (1966, CESCR), the Convention on the Rights of the Child,[13] the Convention on the Elimination of All Forms of Racial Discrimination,[14] and the UNESCO Convention against Discrimination in Education, as well as through specific provisions in other treaties covering specific groups (for example, women and girls,[15] persons with disabilities,[16] migrants,[17] refugees[18] and Indigenous peoples[19]) and contexts (for example, education during armed conflicts[20]).

It has also been incorporated into various regional treaties and enshrined as a right in the vast majority of national constitutions.[21]

The UN Committee on Economic, Social and Cultural Rights has provided guidance on State obligations under the International Covenant on Economic, Social and Cultural Rights, stating that education in all its forms and at all levels shall exhibit these interrelated and essential features: [22]

- *availability* (i.e. education is free and there is adequate infrastructure and trained teachers able to support the delivery of education);
- *accessibility* (i.e. the education system is non-discriminatory and accessible to all, and positive steps are taken to include the most marginalised);
- *acceptability* (i.e. the content of education is relevant, non-discriminatory and culturally appropriate, and of quality; schools are safe and teachers are professional);

[10] As expressed in ICCPR, Article 19 and CRC, Article 13. Article 17 of the CRC further affirms that children must have access to information and material from a diversity of national and international sources. See also, UNGA, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/73/348 (29 August 2018), which outlines a human rights-based approach to artificial intelligence.
[11] Article 26: 'everyone has the right to education'
[12] Articles 13 and 14.
[13] Articles 28 and 29.
[14] Articles 5 and 7.
[15] Convention on the Elimination of All Forms of Discrimination against Women, 1979, Article 10.
[16] Convention on the Rights of Persons with Disabilities, 2006, Article 24.
[17] Convention on the Protection of the Rights of All Migrant Workers and Members of their families, 1990, Article 30, 43(1) and 45(1).
[18] Convention Relating to the Status of Refugees, 1951, Article 22.
[19] Declaration on the Rights of Indigenous Peoples, 2007, Articles 14, 15, 17 and 21.
[20] See https://www.right-to-education.org/node/69.
[21] See https://www.right-to-education.org/sites/right-to-education.org/files/resource-attachments/RTE_International_Instruments_Right_to_Education_2014.pdf for the full text of the international right to education provisions, regional human rights framework on the right to education, and UN treaty body general comments and general recommendations which offer more specific guidance as to the right to education.
[22] CESCR, *General Comment No. 13 on the right to education*, UN Doc. E/C.12/1999 (8 December 1999), para. 6.

- *adaptability* (education evolves with the changing needs of society and challenges inequalities, such as gender discrimination; education adapts to suit locally specific needs and contexts).

Regarding the purpose of education, the human rights framework guides that education shall be directed to the full development of the human personality and to the strengthening of respect for human rights and fundamental freedoms, and that education shall enable all persons to participate effectively in a free society, promote understanding, tolerance and friendship among all nations and all racial, ethnic or religious groups.[23] The CRC further outlines that:[24]

> **States parties agree that the education of the child shall be directed to:**
>
> **(a) The development of the child's personality, talents and mental and physical abilities to their fullest potential;**
>
> **(b) The development of respect for human rights and fundamental freedoms, and for the principles enshrined in the Charter of the United Nations;**
>
> **(c) The development of respect for the child's parents, his or her own cultural identity, language and values, for the national values of the country in which the child is living, the country from which he or she may originate, and for civilizations different from his or her own;**
>
> **(d) The preparation of the child for responsible life in a free society, in the spirit of understanding, peace, tolerance, equality of sexes, and friendship among all peoples, ethnic, national and religious groups and persons of indigenous origin;**
>
> **(e) The development of respect for the natural environment.**

State responsibility for the resourcing of education is also covered in the international human rights framework, which makes clear that primary education shall be compulsory and available free to all, and secondary and higher education shall be both supported in particular by the progressive introduction of free education.[25] The Committee on Economic, Social and Cultural Rights has provided guidance to states as to what progressive realisation of rights means in practice, regarding the use of maximum available resources (referring to both the resources existing within a State as well as those available from the international community through international cooperation and assistance), the immediate obligation to guarantee rights without discrimination of any kind, the obligation to take timely steps which

[23] UDHR, Article 26(2) and CESCR, Article 13(1).
[24] CRC, Article 29(1).
[25] CRC, Article 28(1) and CESCR, Article 13(2). See also CESCR, *General Comment No. 11 on plans of action for primary education*, UN Doc. E/C.12/1999/4 (11 May 1999).

are deliberate, concrete and targeted, and the requirement for states to take into account the precarious situation of disadvantaged and marginalised individuals and prioritise grave situations or situations of risk.[26]

The right to education has been recognised as a 'gateway' or foundational right to the enjoyment of many other human rights across a person's life, such as related to work and livelihood opportunities, political participation and engagement in communities and societies more broadly, the enjoyment of gender and other forms of equality,[27] and as increasingly important to people's abilities to address escalating climate and ecological crises, in supporting environmental literacy and engagement.[28]

2.2.2. The right to privacy

The international human rights framework does not recognise personal data protection as a fundamental right. However, the right to privacy – generally framed as protection of the law from arbitrary or unlawful interference with privacy, family, home or correspondence, and from unlawful attacks on honour and reputation – is recognised and protected a human right through a series of international legal instruments, notably the Universal Declaration of Human Rights,[29] and the International Covenant on Civil and Political Rights.[30] A specific right to privacy for children is enshrined in the Convention on the Rights of the Child.[31]

The right to privacy is also reiterated in regional contexts, often with more specificity than many of the international agreements which were drafted prior to the development and widespread use of the internet and other relevant developments.[32]

2.3.Specific guidance by UN treaty bodies and experts relevant to children, education, and technology

[26] CESCR, *Statement by the Committee: An evaluation of the obligation to take steps to the "Maximum of available resources" under an optional protocol to the Covenant*, UN Doc. E/C.12/2007/1 (21 September 2007). See also: A/HRC/50/32, para. 9.

[27] See, for example: CEDAW Committee, *General recommendation No. 36 on the right of girls and women to education*, UN Doc. CEDAW/C/GC/36 (16 November 2017) which sets out a tripartite framework which provides guidance through a substantive equality lens in relation to the right of access to education; rights within education; and rights through education.

[28] See, for example: Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (Aarhus, Denmark, 25 June 1998); Regional Agreement on Access to Information, Public Participation and Justice in Environmental Matters in Latin America and the Caribbean (Escazú, Costa Rica, 4 March 2018)

[29] Article 12. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

[30] Article 17. 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.

[31] Article 16. 1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.
2. The child has the right to the protection of the law against such interference or attacks.

[32] This includes regional legal instruments in: Africa, including the African Union Convention on Cyber Security and Protection of Personal Data 2014, which contains specific provisions on personal data protection (see Chapter 3), the Supplementary Act A/SA.1/01/10 on personal data protection within ECOWAS 2010, and the African Charter on the Rights and Welfare of the Child (Article 10); in Europe, including the European Convention on Human Rights 1950 (Article 8), the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – Convention 108, 1981 (Articles 5-8), the Charter of Fundamental Rights of the European Union 2000 (Articles 7 and 8), the Treaty on the Functioning of the European Union (Article 16(1)), and EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of data); and in the Americas, including the American Convention on Human Rights 1969 (Article 11).

Additional authoritative guidance on the applicability of the international and regional human rights framework to specific geographical and thematic contexts, as well as to ongoing technological developments, can be found in a variety of sources. These include the concluding observations, general comments/recommendations, statements and views of UN human rights treaty bodies (i.e. the bodies of independent experts tasked with monitoring implementation by State parties of specific treaties) and the reports issued by UN special procedure mandate holders (i.e. the independent human rights experts – rapporteurs, independent experts or working groups – appointed by the Human Rights Council to report and advise on human rights from a thematic or country-specific perspective). National human rights institutions, case law, academic commentary provide other sources of the interpretation of human rights in practice.

Set out below are key points from guidance of particular relevance to EdTech, as released in recent years, in relation to children's right to privacy and to the digitalisation of education.

2.3.1. Children's right to privacy

In January 2011, the UN Special Rapporteur on the right to privacy released a report addressing two separate challenges; artificial intelligence and privacy, and children's privacy.[33] In relation to data and artificial intelligence generally, he highlighted the necessity of a privacy analysis given that:

> **…most data are held by private corporations that leverage their commercial value, combining diverse data sets to maximize their analytical capacity. A response is required to growing public concern about the intrusiveness and potential impact of data gathering, the risk of surveillance and the increasing use of algorithms using such data sets to automate decisions that affect individuals' lives.[34]**

In considering principles and recommendations on the right to privacy of children, the Special Rapporteur affirmed that the Convention on the Rights of the Child, which guarantees a right to privacy for children, must be interpreted broadly to fully accommodate their privacy experiences.[35]

Regarding education and schooling in particular, the report reiterated the purpose of education as set out in the human rights framework and noted the large role played by schools in how children experience privacy on a day-to-day basis. With the COVID-19 pandemic – which saw approximately 90 per cent of the global school population affected by school closures in 193 countries by 1 April 2020[36] – education shifted online rapidly and to a significant degree, with downloads of education applications increasing 90 per cent compared to the weekly average in late

[33] UNGA, *Special Rapporteur on the right to privacy's report on 'Artificial intelligence and privacy, and children's privacy'*, UN Doc. A/HRC/46/37 (25 January 2021).
[34] A/HRC/46/37, para. 6.
[35] A/HRC/46/37, para. 70.
[36] A/HRC/46/37, para. 105.

2019.[37] Among other impacts noted by the Special Rapporteur, the shift to online education amplified existing power imbalances between EdTech companies and children, and between governments and children and parents. The report reflected information received that indicated, variously, a lack of protection for children's right to privacy in national legal frameworks or a waiving of such protection, no capacity on the part of children or their parents to challenge EdTech company privacy arrangements or refuse to provide data, and that the selection of EdTech by schools was driven by curriculum and financial considerations rather than privacy concerns.[38]

The report noted that EdTech companies 'routinely control children's digital educational records' and that schools themselves 'hold significant amounts of children's information and increasingly track children by monitoring students' online activities and surveillance cameras', with such data extending to thinking characteristics, learning trajectory, engagement score, response times, pages read, videos viewed, device identification, location data, and being shared with third parties such as advertising partners.[39]

The Special Rapporteur noted that use of EdTech requires accountability, meaningful consent, purpose limitation, data minimisation, transparency and security safeguards, and that educational processes need not and should not undermine the enjoyment of privacy and other rights, wherever or however education occurs, nor intensify existing inequalities.[40]

In light of these findings, the report set out specific conclusions and recommendations to states. These included direction to states to incorporate children's views, children's strategies for privacy, findings of child-focused research and/or child privacy impact assessments in public policy settings; develop comprehensive online educational plans of action based on Article 29(1) of the CRC and the Council of Europe guidelines on children's data protection in an education setting[41]; ensure that appropriate legal frameworks are established and maintained for online education; create public infrastructure for non-commercial educational and social spaces; ensure that information is available to children on exercising their rights on, for example, the websites of data protection authorities, and ensure the provision of counselling, complaint mechanisms and remedies specifically for children, including for cyberbullying; and implement the UNGPs and its associated gender guidance.[42]

2.3.2.The digitalisation of education

In March 2021, the Committee on the Rights of the Child released its general comment no. 25 on children's rights in relation to the digital economy. The aim of the guidance was to explain how States parties should implement the Convention in relation to the digital environment and adopt approaches to relevant legislative, policy and other

[37] A/HRC/46/37, para. 106, referencing a submission from Human Rights Watch.

[38] A/HRC/46/37, paras. 106 and 108.

[39] A/HRC/46/37, paras. 106-109.

[40] A/HRC/46/37, paras. 109-110.

[41] Council of Europe, Children's data protection in an education setting - Guidelines (2021). Available at: https://edoc.coe.int/en/children-and-the-internet/9620-childrens-data-protection-in-an-education-setting-guidelines.html

[42] A/HRC/46/37, paras. 126(a)(iii) and 127(g), (h), (i), (s), (u) and (x).

measures to ensure full compliance with their obligations, in the light of the opportunities, risks and challenges in promoting, respecting, protecting and fulfilling all children's rights in the digital environment.[43]

The CRC noted that innovations in digital technologies affect children's lives and their rights in ways that are wide-ranging and interdependent, even where children do not themselves access the internet,[44] and affirmed that the rights of every child must be respected, protected and fulfilled in the digital environment using the following four principles as a guide for determining the measures to guarantee such rights: non-discrimination; best interests of the child; right to life, survival and development; respect for the views of the child.[45]

Regarding the best interests of the child, the Committee advised that States parties should ensure that this is a primary consideration in all actions regarding the provision, regulation, design, management and use of the digital environment, and that this should involve regard for all children's rights, including their rights to seek, receive and impart information, to be protected from harm and to have their views given due weight, with transparency in the assessment of the best interests of the child and the criteria that have been applied.[46]

With respect to the right to life, survival and development:

> **States parties should pay specific attention to the effects of technology in the earliest years of life, when brain plasticity is maximal and the social environment, in particular relationships with parents and caregivers, is crucial to shaping children's cognitive, emotional and social development. In the early years, precautions may be required, depending on the design, purpose and uses of technologies. Training and advice on the appropriate use of digital devices should be given to parents, caregivers, educators and other relevant actors, taking into account the research on the effects of digital technologies on children's development, especially during the critical neurological growth spurts of early childhood and adolescence.[47]**

Considering the implementation of children's rights in practice, the Committee stated that the realisation of children's rights and their protection in the digital environment will require a broad range of legislative, administrative, and other measures, including precautionary ones.[48] With regard to the legislative environment, it stated that:

> **States parties should review, adopt and update national legislation in line with international human rights standards, to ensure that the digital environment is compatible with the rights set out in the Convention and the Optional Protocols thereto.**

[43] CRC/C/GC/25, para. 7.
[44] CRC/C/GC/25, para. 4.
[45] CRC/C/GC/25, para. 8.
[46] CRC/C/GC/25, paras. 12-13.
[47] CRC/C/GC/25, para. 15
[48] CRC/C/GC/25, para. 22

> **Legislation should remain relevant, in the context of technological advances and emerging practices. They should mandate the use of child rights impact assessments to embed children's rights into legislation, budgetary allocations and other administrative decisions relating to the digital environment and promote their use among public bodies and businesses relating to the digital environment.**[49]

The Committee further outlined specific measures in relation to comprehensive policy and strategy (paras. 24-26), coordination (para. 27), allocation of resources (paras. 28-29), data collection and research (para. 30), independent monitoring (para. 31), dissemination of information, awareness raising and training (paras. 32-33), cooperation with civil society (para. 34), children's rights and the business sector (paras. 35-39), commercial advertising and marketing (paras. 40-42) and access to justice and remedies (paras. 43-49). In Sections IV and XI of the general comment, the Committee provides further detail in relation to specific rights relevant to children's experiences in the digital environment, including access to information, freedom of expression, freedom of thought, conscience and religion, freedom of association and peaceful assembly, right to privacy, birth registration and right to identity, right to education, and right to culture, leisure and play.

Recognising the importance of privacy for children's agency, dignity, and safety and for the exercise of their rights, the Committee noted ways in which threats to children's privacy may arise, including through data collection and processing by public institutions, businesses and other organisations, from criminal activities such as identity theft, and through their own activities or the activities of family members, peers or others.[50] It reiterated that under the human rights framework:

> **Interference with a child's privacy is only permissible if it is neither arbitrary nor unlawful. Any such interference should therefore be provided for by law, intended to serve a legitimate purpose, uphold the principle of data minimization, be proportionate and designed to observe the best interests of the child and must not conflict with the provisions, aims or objectives of the Convention.**[51]

In relation to children's privacy rights, the CRC Committee further detailed: the legislative, administrative and other measures States parties should take to ensure that children's privacy is respected and protected by all organisations and in all environments that process their data; guidance on consent to process a child's data and the access/rectification/deletion of data; the accessibility of data; the relationship between privacy and data protection legislation and measures with children's other rights; digital surveillance of children together with any associated

[49] CRC/C/GC/25, para. 23 (footnotes omitted), citing the CRC's general comment No. 5 (2003), para. 45; general comment No. 14 (2013), para. 99; and general comment No. 16 (2013), paras. 78–81.
[50] CRC/C/GC/25, para. 67.
[51] CRC/C/GC/25, para. 69.

automated processing of personal data; safeguarding and so on.[52] In relation to ensuring the right to education in the context of digitalisation, the general comment provided guidance on equitable investment in technological infrastructure, the enabling of remote learning, the importance of digital literacy, and also advised that:

> **States parties should develop evidence-based policies, standards and guidelines for schools and other relevant bodies responsible for procuring and using educational technologies and materials to enhance the provision of valuable educational benefits. Standards for digital educational technologies should ensure that the use of those technologies is ethical and appropriate for educational purposes and does not expose children to violence, discrimination, misuse of their personal data, commercial exploitation or other infringements of their rights, such as the use of digital technologies to document a child's activity and share it with parents or caregivers without the child's knowledge or consent.[53]**

> **It is of increasing importance that children gain an understanding of the digital environment, including its infrastructure, business practices, persuasive strategies and the uses of automated processing and personal data and surveillance, and of the possible negative effects of digitalization on societies. Teachers, in particular those who undertake digital literacy education and sexual and reproductive health education, should be trained on safeguards relating to the digital environment.[54]**

A year following the CRC Committee's general comment, the UN Special Rapporteur on the right to education released a report also examining the digitalisation of education, with a specific focus of the risks and opportunities of such digitalisation for enjoyment of the right to education.[55] The overarching message of the report was the reminder to governments that discussion relating to the introduction of digital technologies in education must be framed around the right of every person to public, free, quality education and the commitments of states in this regard both under international human rights law and Sustainable Development Goal 4.[56]

Guidance is given as to the traditional right to education framework of availability, accessibility, acceptability and adaptability in such contexts,[57] and the report then presents an overview of the most important elements in identifying and enhancing the benefits of digital technology for the right to education, considering: digital citizenship

[52] See Annex A.

[53] CRC/C/GC/25, para. 103.

[54] CRC/C/GC/25, para. 105.

[55] UNGA, *Impact of the digitalization of education on the right to education. Report of the Special Rapporteur on the right to education, Koumbou Boly Barry,* UN Doc. A/HRC/50/32 (19 April 2022). As acknowledged in para. 1, the 2022 report builds on the work undertaken by the previous mandate holder, in particular a 2016 report on the right to education in the digital age, focusing on higher education (UN Doc. A/HRC/32/37).

[56] A/HRC/50/32, para. 6. SDG 4 calls for States to ensure inclusive and equitable quality education and promote lifelong learning opportunities for all.

[57] A/HRC/50/32, Section II.B.

(participation and autonomy in a digital world); personalised teaching and learning; digital solutions for crises (conflicts, epidemics and natural disasters); and the gathering of data to enhance the implementation of the right to education.[58]

However, returning to the purpose of education under international human rights law, the Special Rapporteur reiterates that "the digitalization of education should further not only skills, abilities and competencies, but also the development of the human personality, effective participation in a free society and societies' capacities to decide on their own development."[59] While noting that digitalisation brings potential opportunities and introduces novel approaches, these only arise under certain conditions.[60] In particular, the report states:

> **As debates around the digitalization of education tend to focus on the effectiveness of methods, tools and strategies – often in search of evidence-based solutions of "what works" – it is important to emphasize the lack of evidence and contextualized evaluation supporting the claimed added value of digital technologies in many respects. Decision makers at all levels must understand the profit-driven agenda of digital technology lobbyists and companies, who push them into introducing digital technologies rapidly in schools, and how this can negatively affect education systems for the benefit of a few.[61]**

The Special Rapporteur raises concerns regarding serious risks to human rights associated with the digitalisation of education, noting that:

> **Some risks are the exact opposite of potential benefits: heightened exclusion instead of improved access, standardization instead of personalized teaching, enhanced stereotypes instead of diversity, reduced autonomy and freedom instead of creativity and participation, and data mining for the benefits of a few at odds with the public interest. Attacks on freedom of opinion and expression and on the right to privacy, advertising and marketing in schools, and an even greater commercialization of education also constitute great dangers for the right to quality education for all.[62]**

In supporting governments to avoid such risks, the report provides specific guidance in relation to a number of issues. Regarding the growing involvement of commercial actors in education, the Special Rapporteur notes that public policies have been unable to keep up with the changes in digital education, and that there is a lack of appropriate international and national regulation to govern, for example, the marketisation of education as linked to profit motives

[58] A/HRC/50/32, Section III.
[59] A/HRC/50/32, para. 10.
[60] A/HRC/50/32, para. 6.
[61] A/HRC/50/32, para. 5.
[62] A/HRC/50/32, para. 50.

of EdTech companies, increasing pressure and influence by corporations on public institutions and decision-making spaces, and harmful dependency of governments on private services often provided at low or no cost, which leads to a lack of control over data, decisions, privacy and autonomy with particular implications for countries in the global South in connection with predominantly global North located EdTech corporations and the exacerbation of existing international inequalities.[63]

Another challenge raised in the report is that of datafication and surveillance, with a recognised "massive imbalance in power, awareness and knowledge between those who decide on the technologies and the users".[64] Issues highlighted include the lack of transparency related to data collection and use, unclear lines of accountability for data-based decision-making, an inability to opt-out of EdTech use or to challenge privacy arrangements in the face of legitimate concerns, impacts on children's right to privacy, and the potential for digital record of students' education to adversely impact their employment options.[65]

The report concludes with an extensive list of recommendations, including that privatisation risks should be addressed via full abidance with the Abidjan Principles[66] and the UNGPs, and that coordinated efforts should be made to ensure adequate financing for education.[67] In relation to risks of increased surveillance and data mining, the Special Rapporteur recommended:

> **(a) Child-specific privacy and data protection laws that protect the best interests of children in complex online environments should be adopted and/or implemented at all times. Privacy and data protection laws should also protect adults in any educational setting, including online;**
>
> **(b) Child rights impact assessments and data privacy audits should be conducted before adopting digital technologies in education. Categories of sensitive personal data that should never be collected in educational settings, in particular from children, should be defined. Any services procured to deliver online education must be safe for children;**
>
> **(c) States should perform due diligence to ensure that the technology they recommend for online learning protects children's privacy and data protection rights; and provide guidance to educational institutions to ensure that data privacy clauses are included in contracts signed with private providers;**

[63] A/HRC/50/32, paras. 56-61.

[64] A/HRC/50/32, para. 62.

[65] A/HRC/50/32, paras. 62-74.

[66] The Abidjan Principles on the human rights obligations of States to provide public education and to regulate private involvement in education. 2019. Available at: https://www.abidjanprinciples.org

[67] A/HRC/50/32, para. 99.

(d) Commercial advertising to students should be banned in all educational settings at all levels, whether private or public, including through digital content and programmes. No data collected within the education system should be used for marketing purposes, and commercial interests should not be considered legitimate grounds for data processing that override the right to education or other human rights;

(e) States should invest in free and public digital platforms and infrastructure for education, grant adequate funding to public institutions to develop alternative free digital solutions and tools that do not involve the private personal data market, and support the development of non-proprietary data tools, platforms and services that are based around values of openness, transparency and common stewardship (rather than individual ownership) of data. They should prioritize the production and use of content in the form of open educational resources and provide a professional, systematic and personal guiding service to individual users;

(f) States and other stakeholders should not allow the surveillance of students, families and communities through digital programmes.

2.4.Further useful guidance

Further relevant guidance, depending on the circumstances being considered, may include:

2.4.1.Additional UN treaty body general comments or recommendations

Other UN treaty body general comments may be relevant to data collection and use and the monitoring of children's activities, depending on the particular context. These include but are not limited to:

- The CRC Committee's general comment on state obligations regarding the impact of the business sector on children's rights,[68] which provides detailed guidance to states as to the application of the CRC, including key principles in children's rights, in the context of business activities and the provision of services.
- The CRC Committee's general comment on public budgeting for the realisation of children's rights,[69] which provides detailed guidance to states on their legal obligation to invest in children, recommends open, inclusive and accountable resource mobilisation, budget allocation and spending, and discusses non-discrimination and children's participation in budget decisions.

[68] CRC, General Comment No. 16 on State obligations regarding the impact of the business sector on children's rights, UN Doc. CRC/C/GC/16 (17 April 2013).

[69] CRC, General Comment No. 19 on public budgeting for the realisation of children's rights (art. 4), UN Doc. CRC/C/GC/19 (20 July 2016).

- The CEDAW Committee's general recommendation on State obligations regarding girls' access to education,[70] including with reference to access to the internet and measures to overcome the digital divide between women and men in the use of new technologies.

2.4.2. UN treaty body concluding observations

As part of the process of constructive dialogue with UN treaty bodies as to compliance with their obligations under relevant treaties, all States parties are obliged to submit regular reports, which the UN treaty bodies examine and then address any concerns and provide recommendations to the State party in the form of "concluding observations".

As education has been impacted by the COVID-19 pandemic and as the guidance from UN treaty bodies and experts relevant to children, education and technology has become more specific in recent years, as outlined above, so too have the concluding observations issued to states. For example, the CRC, CESCR, the Committee on the Elimination of Discrimination against Women and the Committee on the Rights of Persons with Disabilities have each issued guidance to states relating to topics including, variously: equal access to education, as affected by location (education for remote, island or rural locations), lived experiences (children with disabilities, girls, Indigenous girls, Roma children) and disruption (COVID-19 pandemic); educational infrastructure; internet affordability; quality of education; protection against cyberbullying and violence against children in digital settings.

Of particular relevance to this paper, the CRC committee has made specific reference in concluding observations to various states to their compliance with the right to privacy in relation to children, education and digitalisation. Such recommendations include ensuring that laws on the digital environment respect children's right to privacy;[71] developing regulations in the digital environment to protect the privacy of children;[72] expediting work on a national policy to ensure the right to privacy of children in the digital environment;[73] and strengthening mechanisms for monitoring and prosecuting information and communications technology-related violations of children's rights.[74]

2.4.3. Other UN guidance

Although not focused on education, in April 2022, the Office of the High Commissioner for Human Rights (OHCHR) released a report on the practical application of the UNGPs to the activities of technology companies. The findings

[70] CEDAW Committee, *General recommendation No. 36 on the right of girls and women to education*, UN Doc. CEDAW/C/GC/36 (16 November 2017), para. 61.

[71] CRC, *Concluding observations on the combined fifth and sixth periodic reports of the Kingdom of the Netherlands*, UN Doc. CRC/C/NLD/CO/5-6 (9 March 2022), para. 42.

[72] CRC, *Concluding observations on the combined fourth to sixth periodic reports of Tunisia*, UN Doc. CRC/C/TUN/CO/4-6 (2 September 2021), para. 21(a); CRC, *Concluding observations on the combined fifth and sixth periodic reports of Portugal*, UN Doc. CRC/C/PRT/CO/5-6 (9 December 2019), para. 22(a).

[73] CRC, *Concluding observations on the initial report of the State of Palestine*, UN Doc. CRC/C/PSE/CO/1 (6 March 2020), para. 33.

[74] CRC, *Concluding observations on the combined fifth and sixth periodic reports of Portugal*, UN Doc. CRC/C/PRT/CO/5-6 (9 December 2019), para. 22(c); CRC, Concluding observations on the combined fourth and fifth periodic reports of Singapore, UN Doc. CRC/C/SGP/CO/4-5 (28 June 2019), para. 25(c).

were informed by deliberations from a two-day expert consultation, as well as by submissions received from States and other stakeholders, and other relevant processes and initiatives, in particular the OHCHR B-Tech Project.[75]

3. Safeguarding children's rights at the domestic level with regards to the use of technology in education

While the international legal framework still needs to be developed and strengthened as regards the protection of students' rights in the context of the use of technologies in education,[76] the current existing framework must be implemented at national level and the states should follow the recommendations made by various human rights bodies as described in part 2. This part provides an illustration of how states have implemented the international legal framework and developed law and policies aimed to ensure children's rights protection in the context of the increased use of technologies in education, particularly children's data protection and their privacy.

We have done a comparative analysis based on review of laws and policies in ten countries covering all regions and including countries with different income levels. This analysis is not comprehensive and does not aim to reflect the global situation. It is a starting point for further research and analysis. For the review of law and policies, we received pro bono support from lawyers across the world who provided information for the following countries[77]: Australia, China, Ireland, Japan, Singapore, South Africa, and the United Kingdom. In addition, to complete geographical representativity, we conducted our own research for the following countries: Brazil, France, and India. Some countries have been picked based on lawyers' expertise, others because we knew some laws and policies had been developed as regards the use of technology in education.

It is important to mention here that the adoption of law and policies are not always implemented in practice, and we recommend reading them in light of the specific country context.

3.1. Overview of national laws safeguarding data protection

The UN Committee on the Rights of the Child (CRC) has recommended states to take legislative measures to ensure that children's privacy is respected and protected by all organisations and in all environments that process their data. The recommendation suggests a legal framework with strong safeguards to protect children from the risks and

[75] Human Rights Council, The practical application of the Guiding Principles on Business and Human Rights to the activities of technology companies. Report of the Office of the United Nations High Commissioner for Human Rights, UN Doc. A/HRC/50/56 (April 2022).

[76] See The Right to Education Initiative's contribution to the global conversation on the right to education: Reviewing and extending the understanding of the right to education in the 21st Century. 2021. Available at: https://www.right-to-education.org/resource/right-education-initiative-s-contribution-global-conversation-right-education-reviewing-and

[77] The Right to Education Initiative has required assistance with regards (i) to the extent to which learners and/or children are referenced or otherwise protected in national laws relating to data protection and (ii) to the implementation and enforcement of such laws, specifically the existence of relevant case law related to learners and/or children. For this purpose, RTE addressed a query to human rights lawyers across the world with nine guiding questions tailored to the analyses. RTE specifically acknowledges the contribution of the following law firms: Anglo American, Dechert LLP, DLA Piper UK LLP, Morrison Foerster.

consequences of the processing of their personal data[78]. Nevertheless, most of the existing legislative frameworks protecting data privacy and security do not specifically protect children nor are specifically tailored to learners' protection in an educational context.

Our analysis of national legislations concluded that most of the general data protection instruments under review make no distinction between adults and children with respect to the treatment of their personal data (Australia, Japan, Singapore, India, and South Africa). Some General Data Protection Laws – such as the EU GDPR that was incorporated into national legislation in the three European countries reviewed – recognise that children 'merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned' as well as of 'their rights in relation to the processing of personal data'[79]. But despite recognising the need for enhanced protection regarding children's data, most of the general data protection laws do not grant further protection to those under 18, leaving regulation to the authorities. Some countries, like Brazil, have integrated a specific chapter on children's data within their General Data Protection Law safeguarding on and offline processing of personal data of those under 18 years old[80]. Although not focused specifically on the use of technology in education, Japan[81] and China[82] have separate laws regulating children's rights to privacy and security in a digital environment. Some of the countries we reviewed have issued non-binding instruments providing interpretation to general data protection laws and guiding organisations on its application with regards to the processing of minor's data (France[83], UK[84], Singapore[85], Ireland[86], Australia[87]). Although general in scope and not specifically tailored to the protection of learners' data, those laws and guidelines may apply to educational settings.

There are indeed very few laws and/or regulations within the national legal frameworks analysed in this paper that offer specific protection to learners' data in educational contexts. The EU has issued two relevant guidelines regarding the protection of children's data rights in digital and on educational environments: Guidelines to respect, protect and fulfil the rights of the child in the digital environment[88]and the Guidelines on Children's data protection on education setting[89]. But to this day, China is the sole country reviewed having binding instruments regulating

[78] CRC/C/GC/25, para 22, 23, 70.
[79] EU/GDPR/Recital 38
[80] Brazil, Lei Geral de Proteção de Dados (or LGPD), Lei nº 13.709/2018.
[81] Japanese Act on Establishment of Enhanced Environment for Youth's Safe and Secure Internet Use provides for educating youths regarding the internet and promoting internet literacy and use of filtering software on PCs and smartphones. Japan, Act No. 79, 2008.
[82] China has two laws dedicated to the protection of children's digital rights, namely the law of the People's Republic of China on the Protection of Minors, and the Provisions on Cyber Protection of Children's Personal Information.
[83] France's regulatory authority CNIL has issued eight recommendations dedicated to the protection of children's rights.
[84] The English Information Commissioner's Office (ICO) has issued two guides providing for special protection of children with regards to data processing: Guidance on children and the UK GDPR, The Age-Appropriate Design Code. The first one provides guidance related to the rights of the child under the UK GDPR, consent, targeted marketing, profiling, and automatic decision making, and data-sharing. The second one sets 15 standards and explains how the General Data Protection Regulation should be applied to the use of digital services by children.
[85] The Singapore Personal Data Protection Commission (PDPC) has issued guidelines advising organisations to implement 'relevant precautions' if they are collecting, using, or disclosing personal data about minors. See Personal Data Protection Commission, "Advisory Guidelines on the PDPA for Selected Topics", revised 17 May 2022.
[86] The Data Protection Commission of Ireland (DPC) has published three short guides addressed to children regarding their rights under the GDPR. It has also edited the Fundamentals for a Child-Oriented Approach to Data Processing (2021), which set out the standards that all organisations should follow when collecting and processing children's personal information as, for example, putting the best interests of the child at the forefront of their considerations.
[87] The Office of the Australian Information Commission has issued the Australian Privacy Principles Guidelines – APP Guidelines providing guidance to the implementation of the Australian data protection law.
[88] EU, Committee of Ministers, Recommendation CM/Rec(2018)7, Guidelines to respect, protect and fulfil the rights of the child in the digital environment
[89] EU, Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, Children's data protection in an education setting - Guidelines (2021)

child protection in the use of digital devices in education, namely, the Provisions on the Protection of Minors by Schools[90].

People's Republic of China, Provisions on the Protection of Minors by Schools (2021)

Article 10 stipulates that:

- Schools should notify students and their parents when collecting personal information of students. Schools are obligated to manage and keep confidential such information, and should not destroy, abandon, illegally delete, disclose, publicise or trade such information.
- Schools should not divulge personal privacy of students and privacy of their families during the rewards, grants, poverty assistance application. It should facilitate the students and their parents in gaining information such as examination results, rankings and other academic information, but it should not disclose these to the public. Except for reasons provided by the law, it should not access the correspondence, diaries, e-mails, or other online communications of students.

Article 34 stipulates that:

- Schools should conduct cybersecurity and cyber-courtesy education. It should also prevent and intervene in its students' excessive use of the network.
- Schools should install online protection software to prevent students from accessing information not suitable for minors. It should take immediate measures and report to relevant competent authorities when it discovers that network products, services, or information contain any content harmful to the physical and mental health of students, or that a student uses the network to conduct illegal activities.
- **Article 38 forbids a school** and its staff from disclosing students' information and from using information in their possession to seek benefits. Under Article 60, teachers and staff violating this provision will be ordered to return any fee charged or benefit received, pay compensation in accordance with the law, if economic loss is caused to any student. They may also be subjected to discipline according to the circumstances, and if the violation is legally or criminally punishable, a transfer should be made to the relevant department for holding the staff member liable.
- **Article 52 provides that** an external contractor providing services for schools should also be subjected to confidentiality agreements so as to protect the privacy of students and their families.

Other countries under review have shown political will to regulate child protection in the use of digital devices in education but for different reasons those regulations are not yet in force (Ireland) or have limited application (Singapore and Australia). For instance, The Irish Education (Digital Devices in Schools) Bill 201 – which aimed,

[90] The Provisions on the Protection of Minors by Schools was adopted on 25 May 2021 and came into effect as of September 1, 2021. An English version is available at: https://www.pkulaw.com/en_law/65e0f07394eecfb6bdfb.html

amongst other things, to regulate the use of digital devices in primary and secondary schools – was proposed and debated by the Oireachtas (the Irish Government) but the bill lapsed in 2020 and has not made into effective law. In Singapore, the Personal Data Protection Commission (PDPC) issued specific guidelines for the education sector (The Advisory Guidelines for the Education Sector`) but exempted government and other specified statutory bodies of its application[91]. Similarly, whether the Australian Privacy Act covers a child's childcare centre, school or tertiary education depends on whether it is a private or public entity. Indeed, the Australian Privacy Act applies to how personal information is handled by private institutions under certain conditions: when they have an annual turnover of more than $3 million; when they are connected to a larger organisation (with an annual turnover of $3 million); or when they supply a health service and hold health information, although this is not their primary activity. For local government-run childcare centres and schools, the Privacy Act generally does not cover the entity as it does not apply to state or territory agencies, including local government agencies, unless they are an incorporated company, society or association. While in those cases, state or territory privacy laws may apply, public primary and secondary schools would not fall under the general data protection law.

The next section provides an overview of the above-mentioned laws and regulations, focusing on the extent to which they implement the human rights international legal framework presented in part 2 at a national level.

3.2.Lawful processing in educational contexts

One's personal information cannot be collected, processed, disclosed and/or retained unless authorised by law. Whilst the lawful conditions that authorise the processing of personal data vary from country to country, it is possible to identify a few situations that are common to many national legislations, such as, for example, when processing is necessary to ensure compliance with the law or to protect the vital interest of the data subject; when processing is necessary for the performance of a contract to which the data subject is party; when processing is necessary for the performance of a task carried out in the public interest and when processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party; or, when the data subject consents to the processing of their personal data. In any case, the legality of the processing is also subject to compliance with all applicable laws, including general principles, such as data minimisation, purpose, adequacy, fairness, and transparency, amongst others.

This section focuses on the grounds on which learners' – especially children's – data can be lawfully collected and processed with regards to the educational environment. It focuses on three categories of lawful processing that are

[91] Part 1 (1.3) of the The Advisory Guidelines for the Education Sector states that: 'Section 4(1)(c) of the PDPA provides that, among others, the Data Protection Provisions shall not impose any obligation on any public agency. Public agencies include the Government and specified statutory bodies, including the CPE. The examples in these Guidelines on the Data Protection Provisions are relevant to education institutions that do not fall within the definition of a public agency, such as government-aided schools, specialised independent schools, specialised schools, independent schools, autonomous universities, SIM University, Nanyang Academy of Fine Arts, LASALLE College of the Arts, and private education institutions ("PEIs"), e.g., Foreign System Schools'.

specifically relevant to educational contexts: public interest, legitimate interest of the controller or a third party, and consent.

3.2.1. Lawful processing on the grounds of public interest or legitimate interest of the controller or a third party

When processing is based on public interest, on the legitimate interest of the controller or a third party, there is no need to obtain consent from the data subject (even if they are a child). In practice, this means that, in general, schools or universities can lawfully process data from their students without requiring their previous consent if the processing is justified on one of the above-mentioned grounds and if they respect the principles of purpose limitation, data minimisation, adequacy and fairness. In any case, data collection, processing, and retention should not override the interests or fundamental rights and freedoms of the data subject. Additionally, if the data subject is a child, the principle of the best interest of the child as stated in the Convention on the Rights of the Child should always prevail.

Where the law establishes lawful processing without consent on the grounds of public interest or on the grounds of the legitimate interests of the controller or a third party, it supposes a weighting exercise whereby the public interest and the interests of the controller or third party must not override the interests or fundamental rights and freedoms of the data subject. The purpose of this balancing exercise should always be to safeguard the learners' rights and avoid exposing them to unnecessary and disproportionate risks, especially when public interest or what is understood as legitimate interest of the controller, or third party is not aligned with the best interests of the child.

This general safeguarding rule can be illustrated by the Irish regulation. The Irish General Data Protection Law establishes that processing on the grounds of legitimate interest is lawful where it 'is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child' (emphasis added)[92]. In the same line, the Irish Data Protection Commission's Guidelines - 'Fundamentals for a Child-Oriented Approach to Data Processing' - provides interest guidance on how this balancing exercise should be conducted, spelling out the following useful steps:

- identify the public interest at stake/the legitimate interests of the controller which are sought to be achieved,
- demonstrate why/ how processing is a necessary and proportionate means to achieving the legitimate interests, and
- balance those legitimate interests against the child's interests or fundamental rights and freedoms.
- Moreover, the Irish 'Fundamentals' establish the principle of zero interference with the best interest of a child.

[92] See also, for other European countries, Article 6(1)(f) of the European Union General Data Protection Regulation (GDPR).

Principle of zero interference with the best interests of a child

'Online service providers processing children's data should ensure that the pursuit of legitimate interests do not interfere with, conflict with or negatively impact, at any level, the best interests of the child'.

Ireland Data Protection Commission (DPC), Fundamentals for a Child-Oriented Approach to Data Processing, Section 2.4, 'Legal bases for processing children's data'.

It is worth noting that even when processing children's data on the grounds of public interest, when engaging in contracts with third parties – such as EdTech companies, for example – for the processing of learners' data, schools need to be sure that the roles and responsibilities of the controller and the processor are clearly defined in their agreement with such third parties. This is relevant for accountability purposes, as the level of compliance to the law is not the same if one is a controller or a processor. Indeed, educational institutions' (public or private) compliance to general data protection laws will usually depend on whether the school/university is a controller, a joint controller, or a processor[93]. The controller has the highest level of compliance responsibility while the processor acts on behalf of and following instructions of the controller. If an EdTech provider is able to influence how children's data is used, for example, it should be considered a joint controller. But most of the contacts between schools and EdTech companies do not clearly state the responsibilities of each party, blurring accountability lines.

A report of the Digital Futures Commission and the 5Rights Foundation, titled 'Problems with data governance in UK schools: the cases of Google Classroom and ClassDojo' sheds light on how this issue can affect the privacy of learners. It concludes, amongst other things, that it is near impossible to discover exactly what data is being collected by EdTech companies and whether and how this data is interpreted by third party organisations who may have been given access to it[94]. The report points out that the contracts between the schools and both Google Classroom and Class Dojo contained provisions asserting that each EdTech provider was a processor, despite many aspects of their processing revealing that they were in fact acting as controller, which entitles different levels of responsibility according to the UK Data Protection Act. The report concludes that these contracts often lack clarity, making it difficult to determine who is responsible for complying with the relevant laws, thus undermining children's rights to privacy.

To this matter, the EU Guidelines on Children Data Protection in Education have recommended that 'all parties involved in data processing in educational settings should clarify the responsibilities and accountability between

[93] The UK Information commissioner's office (ICO) clarifies that 'controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data'. But 'if two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes'. ICO, Guide to the General Data Protection Regulation (GDPR)

[94] Hooper, L., Livingstone, S., and Pothong, K. Problems with data governance in UK schools: the cases of Google Classroom and ClassDojo. Digital Futures Commission, 5Rights Foundation. (2022)

roles to establish legal authority and their duties as regards data processing, and when contracting with providers and third-party data processors (recommendation 7.1.2)[95].

3.2.2. Lawful processing on the grounds of consent

UNESCO has warned about 'a disproportionate and paradoxical reliance on notice-and-consent regimes for the processing of learners' data', highlighting the challenges of obtaining consent in learning environments in situations such as those observed during the covid pandemic[96]. Indeed, opting out of the processing of their data through digital devices that were chosen by the educational authorities to provide online classes during Covid-19 school closures would have meant, for most students, not being able to exercise their right to education.

This example illustrates a typical situation in school settings, where the imbalance between the data subject (the learner) and the controller (school authority) may challenge the possibility of learners opting out of the processing without undermining other rights. Indeed, the Digital Futures Commission and 5Rights Foundation report mentioned above has concluded that consent is an inappropriate basis for lawful processing by EdTech companies. This is because in a school setting it is too difficult for a child to refuse consent due to the power imbalance between child/parent and teacher, especially when the data subject is not able to understand to what they are consenting, as was the case with Google Classroom and ClassDojo[97]. Consent is also challenging because of gaps in most national legal frameworks regarding who should consent and how consent should be obtained with regards to the processing of children's data, but also because privacy and security policies are usually long, complex, and difficult to understand.

Recognising the risks involved in the processing of children's data on the grounds of consent, the UN Committee on the Rights of the Child has issued recommendations stating that where consent is sought to process children's data, State parties need to ensure that consent[98]

- is given by the person having legal capacity to consent (either the child or, depending on the child's age, a parent or legal guardian)
- is acquired prior to the processing of the data
- is free, informed, and meaningful

[95] EU, Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, Children's data protection in an education setting - Guidelines (2021)
[96] UNESCO, Minding the Data. Protecting Learners' privacy and security, 2022.
[97] Hooper, L., Livingstone, S., and Pothong, K. (2022). *Problems with data governance in UK schools: the cases of Google Classroom and ClassDojo*. Digital Futures Commission, 5Rights Foundation.
[98] CRC/C/GC/25, para. 71.

That means that the child - or their legal guardians, when applicable - need to understand exactly what it is they are consenting to (what kind of data will be collected, used, and stored and for what purposes) and what are the risks of not consenting. Only then they will be able to freely decide, without any constraints, if they want to give or withdraw consent.

This is particularly relevant in educational contexts because even if schools and universities can lawfully collect, retain, and process data from learners without their consent (for example, on the grounds of public interest, as specified in previous section), whenever the collection, processing and retention is not relevant nor strictly related to the purpose of education they will require consent (data minimisation). According to all general data protection laws reviewed, consent will also be required to collect and process special category data. Indeed, according to the purpose of data minimisation the collection, processing and retention of personal data should be adequate – sufficient to properly fulfil the stated purpose; relevant – linked to that purpose; and limited to what is necessary. That means that consent would be necessary, for example, for marketing or advertising purposes, sharing students' personal data with third parties, and collecting biometric data.

As we will see in the next subsections, while some of the States under review have taken steps to protect children's rights when their personal information is processed on the grounds of consent, not all countries have stepped up to the issue and the CRC recommendations have yet to be fully implemented. The issue is relevant in educational contexts because even if schools have the right to lawfully process students' data on the grounds of public interest, this processing must be strictly related to the educational purposes. Thus, when wishing to share personal data with a museum or a zoo when organising a field trip for third graders, or when wishing to share pictures of students taken in the last school science fair on the schools' webpage, schools must obtain previous and specific consent from learners – or, depending on their age, from their parents or legal guardians.

The next sections focus on a few examples of challenging issues regarding consent – capability to consent, age verification, informed and meaningful consent – and look at how they are reflected on some countries' legislation or regulations.

3.2.3. Digital age of consent

While most of the countries under review require prior, free, and informed consent for the lawful processing of personal data on the grounds of consent, not all countries have binding laws establishing when a child is considered capable of giving consent (digital age of consent) and when children must be represented or assisted by their parents or legal guardians in the act of consenting to online processing of their personal data.

This is relevant because while individuals aged 18 years old or younger are considered children under international human rights law, most domestic regulations establish a different threshold for online consent with regards to the processing of children's personal data. Amongst the countries under review, the lowest digital age of consent is 13 years old and the highest 16 years old. That means that in Ireland, for example, when processing data from a child

who is under 16 years old one needs to obtain parental consent, while in the UK parental consent would only be needed for children under 13 years old. In the example mentioned above regarding a third-grade field trip to the museum, assuming that third grade students usually are 8-9 years old, parental consent would be needed both in Ireland and in the UK. This means that in both countries schools would not be able to disclose any of the students' personal information required by the museum unless they obtain specific parental consent to do so. On the other hand, we would have a different situation regarding the need for parental consent if schools in Ireland and in the UK would like to share pictures of a ninth-grade science fair on their website. Assuming that ninth graders are usually around 14 years old, parental consent would be needed to process and publish children's pictures in the UK, but not in Ireland.

More importantly, some legal texts are not straightforward regarding the digital age of consent, making it difficult for controllers and processors to apply the law, and for authorities to enforce it. Australia, UK and France provide good examples, as described hereafter.

Under the Australian Data protection Act (The Privacy Act, 1988), for example, the age after which an individual can make their own privacy decision is not specified. The Office of the Australian Information Commissioner (OAIC) has stated that as a general rule, an individual under the age of 18 has the capacity to consent if they have the maturity to understand what's being proposed, but if they lack maturity, it may be appropriate for a parent or guardian to consent on their behalf[99]. Therefore, an organisation or agency handling the personal information of an individual under the age of 18 must decide on a case-by-case basis if the individual has the capacity to consent. This can be difficult to operationalise, and the OAIC has suggested that if it's not practical for an organisation or agency to assess the capacity of individuals on a case-by-case basis, they may assume, as a general rule, that an individual over the age of 15 has capacity.

Similarly, under the UK Data Protection Act there are no global rules on children's age of consent. Nevertheless, there is a specific provision in Article 8 regarding the lawful processing of children' data on the grounds of consent regarding 'information society services' (ISS)[100]: it establishes that when information society services are offered directly to a child who is at least 13 years old there is no need to get parental consent. Attention should be paid to the fact that if an ISS is offered through an intermediary, for example a school, then the ISS has not been offered 'directly' to the child for the purposes of Article 8. This is relevant in the context of EdTech companies providing services to students, including for the purposes of the application of the Information Commissioners' Office's (ICO) guidelines, 'The Age-Appropriate Design Code'[101]. The latter was issued by the UK regulatory authority acknowledging that the UK data protection regime previously 'failed to create a safe space for children to learn,

[99] See particularly https://www.oaic.gov.au/privacy/your-privacy-rights/children-and-young-people#:~:text=The%20Privacy%20Act%201988%20protects,must%20have%20capacity%20to%20consent.

[100] UK GDPR relies on the definition of ISS as provided in the Technical Standards Regulations Directive (EU) 2015/1535, which defines an ISS as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'.

[101] UK, ICO, Age-Appropriate Design code (2020)

explore and play'. The Code seeks to redress this through a series of standards with which organizations must comply when processing children's data. In doing so, the Code also sheds light on how the UK data protection regime applies to children specifically. But in accordance with the above mentioned Art. 8 of the UK GDPR, the Age-Appropriate Design Code applies to EdTech companies only where the EdTech service is provided to children on a direct-to-consumer basis (e.g., through an app store), or where the EdTech provider influences the nature and purpose of children's data processing (e.g. where EdTech providers process children's personal data for: product development or research and marketing and advertising purposes, for their own commercial endeavours). The Code will thus not apply provided in an educational environment if: (i) the EdTech service is provided to children via an intermediary (i.e., a school); (ii) the service only processes children's data to fulfil the school's public tasks and educational functions; and (iii) the EdTech provider acts solely on the instructions of the school and does not process children's data in any form beyond these instructions[102]. The rationale behind this distinction is that EdTech providers who do meet the three above criteria are providing a service that is merely an extension of the school's offline activities. That means that the Age-Appropriate Design Code – which would afford better protection to children – does not necessarily apply to EdTech Companies owing to the confusion between when an ISS is and is not bound to comply.

The French Data Protection Act, for instance, allows children at the age of 15 years or older to solely grant or withhold consent to some sensitive features (such as, accepting cookies, activating geolocalisation, setting the public/private status of a social network profile)[103] while at the same time establishing their incapacity to sign up for a contract. The imbalance of the protection afforded to children according to those provisions was highlighted by the French Regulatory authority CNIL: children aged 15 or more are 'both incapable of signing up to a social network (insofar as this involves a contract), but at the same time capable of granting or withholding consent to some of the more sensitive additional features such as geolocation and the use of cookies'[104]. In light of this observation, the CNIL has issued guidance, subject to the discretionary assessment of the French courts, stating that children above the age of 15 could to be considered capable of entering into contracts that involve the processing of their data for the purposes of online services if certain conditions are respected: the services are suitable for a child audience; the processing strictly complies with data protection rules as set out in the GDPR and the French Data Protection Act (e.g. minimisation of data collected, for a clearly-stated purpose, for a limited period of time and in a secure manner); the child is given clear and appropriate information about how their data will be used and of their data protection and privacy rights; parents are ensured the legal right to request deletion of their child's account if they consider it necessary to protect their child's best interests[105]. To our knowledge, the courts have not yet pronounced on this matter.

[102] UK, ICO, FAQs for education technologies (EdTech) and schools, available at https://ico.org.uk/for-organisations/childrens-code-hub/faqs-for-education-technologies-edtech-and-schools/

[103] France, CNIL, Recommendation 4: Seek parental consent for children under 15, 2021

[104] France, CNIL, Recommendation 1: Regulate the capacity of children to act online, 2021

[105] France, CNIL, Recommendation 1: Regulate the capacity of children to act online, 2021

These examples show the importance of clear, straightforward, and enforceable (binding) regulations with regards to consent for processing children's personal data. Furthermore, it is worth noting that while some countries encourage children's digital autonomy (e.g. France) and require that parents take into consideration their children's point of view regarding the processing of their personal data, it is difficult to know to what extent parents are really listening to their children's opinions. In cases of conflict of interest, the principle of the child's best interest should apply, but it would be subject to appreciation from a third party (external to the parent-child relationship).

Age verification

In cases where consent is needed for lawful processing of learners' data, some legislations determine that if the data subject is a child the processor must verify, 'taking into consideration available technology', that consent is given or authorized by the person having the capacity to do so (Brazil, France, UK, and Ireland).

While many solutions have been developed to ensure the verification processes – offline verification systems; analysis of identity documentation; inferential age verification systems (browsing history, maturity surveys), age verification through payment card validation; biometrical/facial analysis; verification through an entrusted third party – age verification mechanisms and parental consent tools are still in many cases considered ineffective, usually relying exclusively on users declarations (e.g. entering a birth date or ticking a box)[106]. Moreover, most technological solutions do not adequately safeguard both the verification process and the data being transmitted for verification, exposing the subject to risks of data leakage, phishing, privacy violation, etc.[107] Technological solutions for online age verification must ensure sufficiently reliable verification, non-discrimination, and respect for the protection of individuals' data and privacy and their security, especially if they are children.

Current examples of regulations to age verification amongst the countries we reviewed can be found in France and in the UK. France's regulatory authority CNIL has issued a recommendation calling for age verification systems to be structured around six pillars: minimisation, proportionality, robustness, simplicity, standardisation, and third-party intervention[108]. By doing so, the French regulatory authority reinforces that verification systems should be designed to limit the collection of personal data to what is strictly necessary for the verification, and that the information collected should not be used for other purposes - including commercial uses - nor retained by the processor once the verification has been completed.

The UK regulatory authority's Age-Appropriate Design Code establishes that information service societies (ISS[109]) should 'take a risk-based approach to recognising the age of individual users and ensure they effectively apply the standards set in the code for child users'[110]. In practice it means that information service societies (ISS) should assess

[106] European Commission, New European strategy for a Better Internet for Kids – Questions and Answers, May 2022.
[107] France, CNIL, Online age verification: balancing privacy and the protection of minors, September 2022.
[108] France, CNIL, Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy.
[109] UK GDPR relies on the definition of ISS as provided in the Technical Standards Regulations Directive (EU) 2015/1535, which defines an ISS as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'.
[110] UK, Information Commissioners' Office (ICO), Age appropriate design: a code of practice for online services, Chapter 3, 'Age appropriate application'.

the level of risk to which they are exposing children and apply age verification methods that are consistent with this assessment to ensure the level of certainty of age verification before processing occurs. For example, if an online service is low risk, a self-declaration method alone could ensure age verification (for example, ticking a box confirming age or entering a birth date). But if the risks related to the exposure of the children are high, other methods of age verification should be put in place. The Information Commissioner's Office suggests that risk assessment should take into account factors such as the types of data collected; the volume of data; the intrusiveness of any profiling; whether decision making, or other actions follow from profiling; and whether the data is being shared with third parties.

Due to the complexity of the verification process and the imperative to safeguard children's rights when collecting and processing their personal data, the implementation of age verification systems deserve further and continuous research to keep up with technological progress while ensuring the maximum protection to children[111].

Informed and meaningful consent

General Comment 25 of the Committee on the Rights of the Child provides that when processing children's data on the grounds of consent, State parties must ensure that consent is freely given by the child or his/her parents prior to the processing, and after being fully informed of the purposes of the data collection and use as well as the risks of not consenting to the processing of the child's data[112]. The CRC also encourages States to use child friendly language and accessible formats to inform children and parents of their rights regarding the processing of children's data[113].

Following the CRC recommendation and recognising that 'the obligation to provide appropriate information is the cornerstone of online child protection'[114], some countries have issued specific norms regulating how children - and their parents or legal guardians - should be informed of their privacy and security rights in order to ensure their very ability to give informed and meaningful consent.

The Singapore Personal Data Protection Commission, for example, has advised the use of child-friendly language or pictures and other visual material when stating terms and conditions under which data is being collected, processed, and stored[115]. The Brazilian General Data Protection law also establishes that information on the processing of children and adolescents' data shall be provided in a 'simple, clear and accessible manner, taking into account the physical-motor, perceptive, sensorial, intellectual and mental characteristics of the user, using audio-visual resources when appropriate, in order to provide the necessary information to the parents or the legal representative and that is appropriate for the children's understanding'[116].

---

[111] It is worth noting that in the United States, while The COPPA Rule does not mandate the method a company must use to get parental consent, the Federal Trade Commission (FTC)'s has determined that a number of consent methods meet the standard of verifiable parental consent.

[112] CRC/C/GC/25, para. 71

[113] CRC/C/GC/25, para. 72.

[114] France, CNIL, Recommendation 6: Strengthen the information and rights of children by design.

[115] Singapore, Personal Data Protection Commission (PDPC), Advisory Guidelines on the PDPA for Selected Topics, revised 17 May 2022.

[116] Brazil, Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019), Art. 14, para 6.

Brazilian General Data Protection Law (Law nº 13.709/2018)

Section III - Processing of Children and Adolescents' Personal Data

- Art. 14. The processing of personal data belonging to children and adolescents shall be done in their best interest, pursuant to this article and specific legislation.
- §2 When processing data as mentioned in §1 of this article, controllers shall make public the information about the types of data collected, the way it is used and the procedures for exercising the rights of data subjects referred to in Art. 18 of this Law.
- §6 Information on the processing of data referred to in this article shall be provided in a simple, clear and accessible manner, taking into account the physical-motor, perceptive, sensorial, intellectual and mental characteristics of the user, using audio-visual resources when appropriate, in order to provide the necessary information to the parents or the legal representative and that is appropriate for the children's understanding.

European countries reviewed in this paper (UK, Ireland, and France) require that information relating to processing to the data subject should be disclosed in a 'concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular if they are addressed to children'[117]. The information that must be provided usually includes the identity and contact details of the organization that is collecting or using the personal data; the purposes and legal basis for collecting or using the personal data; who the personal data is being shared with; how long it will be kept for; and what the individual's data protection rights are. Regulation authorities in UK, Ireland, and France have also issued guidelines and recommended standards regarding transparency of consent when information society services (ISS) are offered directed to a child[118]. One example is the UK Information Commissioner's Office's Age-Appropriate Design Code: when setting standards to which information service societies (ISS) should comply, the Code stablishes that the privacy information provided to users must be prominent, in clear child friendly language, and tailored to the age of the data subject. It suggests 'using diagrams, cartoons, graphics, video and audio content, and gamified or interactive content that will attract and interest children, rather than relying solely on written communications'[119]. Likewise, child-oriented transparency is also one of the 14 principles contained in the Irish Data Protection Commission guidelines (The Fundamentals for a Child-Oriented Approach to Data Processing), that state that 'when a child has given consent for their data to be processed, that

[117] Art. 12 of the EU GDPR

[118] Irish Data Protection Commission (DPC), The Fundamentals for a Child-Oriented Approach to Data Processing, UK Information Commissioners' Office (ICO), Age appropriate design: a code of practice for online services, France's CNIL, Recommendations to enhance the protection of children online.

[119] UK, Information Commissioners' Office (ICO), Age appropriate design: a code of practice for online services, 2020.

consent must be freely given, specific, informed and unambiguous, made by way of a clear statement or affirmative action'[120].

Informed and meaningful consent is a means to ensuring that individuals have control over their own data. This is particularly relevant because of the imbalance of the power relations between learners and public authorities deciding on the use of technology in education. To this matter, Recital 43 of the European Union GDPR states that 'in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation". The EU Guidelines on Children's data protection in an education setting specifically provides that 'when a school requires the use of e-learning tools, a consent basis for processing personal data either by the school or by the third-party processor will not be valid, because consent must be unambiguously freely given and be able to be refused without prejudice'[121]. It also states that when Educational institutions use a service that constitutes a contractual agreement, for example 'in the use of videoconferencing software in order to be able to implement distance-learning programmes and in which staff may agree to the terms and conditions of a service that include the processing and recording of content including children's images and voice data', consent cannot be assumed by the educational institution nor granted by it on behalf of the child[122].

3.2.4. Best interest of the child

Article 3 of the Convention on the Rights of the Child establishes that 'in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration'. As stated previously in this paper, the Committee on the Rights of the Child has advised that states parties should ensure the primacy of this principle in all actions regarding the provision, regulation, design, management, and use of the digital environment. But only Brazil[123] and China[124] have established the principle of the best interests of the child in their legislative frameworks.

Regulation authorities in other countries under review have issued guidelines advising that the best interest of the child should be the primary consideration of all parties when processing children's data, but those guidelines are, once again, not binding. It is for example the case for the Irish Fundamentals for a Child-Oriented Approach to Data processing, stating that 'any organisation interacting with children's data must put the best interests of the child at

[120] Ireland, Data Protection Commission (DPC), The Fundamentals for a Child-Oriented Approach to Data Processing, 2021. See particularly Section 2.4: "Legal bases for processing children's data".

[121] EU, Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, Children's data protection in an education setting - Guidelines (2021)

[122] EU, Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, Children's data protection in an education setting - Guidelines (2021)

[123] Article 14 of the Brazilian General Data protection law states that 'the processing of personal data belonging to children and adolescents shall be done in their best interest, pursuant to this article and specific legislation'.

[124] According to Art. 4.3 of China's Law on the Protection of Minors, the 'principle of the best interest of minors' should be followed while handling matters related to minors, notably in case of the protection of the privacy of and personal information of minors. Art. 72 of the same law also requires information processors to follow the principles of legitimacy, fairness and necessity when processing the personal information of minors through the internet.

the forefront of their considerations' and respect the principle of Zero Interference with the Best interest of the Child[125]. The UK Age-Appropriate Design Code includes the best interest of the child as one of the standards that information society services should comply with. It states that considering the best interests of child users in all aspects of the design of online services would be a step to ensure compliance with the lawfulness, fairness and transparency principles established in Article 5(1)(a) of the UK GDPR and to take proper account of Recital 38 of the European Union, which states that children merit specific protection with regard to their personal data[126]. The UK Information Commissioners' Office (ICO) has also issued a self-assessment tool to help organisations evaluate if they are taking the best interest of the child in account when designing their services[127]. It is worth noting that even when the ICO Age-Appropriate design code does not apply to schools, as previously mentioned, the UK regulatory authority has encouraged service providers and particularly schools to guide their data collection, processing, and retention practices by the standards therein[128].

Like South Africa and India, Australia does not refer to the principle of the best interest of the child when regulating the processing of children's personal data – indeed, Australian law treats children and adults alike with regards to their personal information. But the Australian government is in the process of reviewing the Australian General Data Protection Law (Australian Privacy Act) and is considering integrating the principle of the best interest of the child in the proposed Online Policy Code with regards to social media services offered to children. The Privacy Discussion Paper states that the Online Policy Code will require social media services to ensure that the collection, use or disclosure of a child's personal information is fair and reasonable in the circumstances. In determining whether the collection, use or disclosure is fair and reasonable in the circumstances, the best interests of the child must be the primary consideration. Because of the limited scope of the discussion paper, there is no guarantee that if the law passes it will be applied to the use of technology in education.

3.3.Challenging issues regarding data processing in educational environments

As stated in part 2, some issues are particularly challenging when considering data processing in educational environments: cyberbullying and online abuse; profiling, marketing, and advertising; automatic decision making; surveillance; data sharing; data breaches; etc. While this section does not cover all these challenging issues and does not pretend to be exhaustive, it sheds some light on how some of them are dealt with within the national legislations of the countries we reviewed.

As we will demonstrate, if some countries have sought to enhance the protection of children regarding geolocalisation, profiling, advertising and automated decision making, most legislations fall short on ensuring special

[125] Ireland, Data Protection Commission (DPC), The Fundamentals for a Child-Oriented Approach to Data Processing, 2021.
[126] UK, Information Commissioners' Office (ICO), Age appropriate design: a code of practice for online services, 2020.
[127] UK, Information Commissioners' Office (ICO), Best interests of the child self-assessment.
[128] UK, Information Commissioners' Office (ICO), FAQs for education technologies (EdTech) and schools, available at https://ico.org.uk/for-organisations/childrens-code-hub/faqs-for-education-technologies-edtech-and-schools/

protection to children with regards to those issues. Furthermore, they have not yet followed the recommendations issued by the Committee on the Rights of the Child[129], the UN Special Rapporteur on the right to privacy[130] and the UN Special Rapporteur on the right to education[131] calling for the prohibition of profiling or targeting of children of any age for commercial purposes. Indeed, a Human Rights Watch global investigation of the education technology endorsed by governments for children's education during the pandemic concluded that 'the majority of these online learning platforms put at risk or directly violated children's privacy and other children's rights, for purposes unrelated to their education'[132]. It demonstrated that most online learning platforms tracked students' geolocalisation, browsing history, contacts details, and sent or granted access to children's data to advertising technology (AdTech) companies, sometimes in ways that made it impossible for them or their parents to know what data was being collected and how it was being used.

While some solutions to minimise such risks have been advanced by regulatory authorities, binding laws banning profiling, targeted advertising and automatic decision making in educational contexts are yet to be considered by national parliaments. Similarly, children's exposure to cyberbullying and online abuse in educational contexts have not yet been given enough attention; while there is much progress in awareness raising, not all countries have specific laws enhancing the protection of children with regards to online abuse, despite the growing use of technology in education. As we will demonstrate, the principles of the best interest of the child as well as measures such as privacy by design and by default may help prevent children's exposure to risks and threats related to their life, integrity, dignity and privacy. Nevertheless, if some solutions have been put forward by national regulatory authorities, there is still much to be done not only to develop and/or enhance national legal frameworks regulating the use of technology in education, but also in holding state and non-state actors accountable for violations of students' rights when technology is used for learning purposes, especially with regards to children.

3.3.1. Cyberbullying and online abuse

Under Article 19 of the Convention on the Rights of the Child, states are responsible for the protection of children from all forms of physical or mental violence, injury or abuse, maltreatment or exploitation. Children can be exposed to cyberbullying and online abuse when their data is processed in educational contexts when, for example, a breach of data leads to their personal information landing in abusers' hands.

While most countries do not expressly define cyberbullying and online abuse as a distinct offence, those behaviours may fall under other existing domestic laws. In Australia, for instance, the Criminal code Act 1995 (Cth), the Crimes (Domestic and Personal Violence) Act 2007 (NSW) and other similar state and territory laws establish regulations

[129] CRC/C/GC/25.
[130] UNGA, *Special Rapporteur on the right to privacy's report on 'Artificial intelligence and privacy, and children's privacy'*, UN Doc. A/HRC/46/37 (25 January 2021).
[131] UNGA, *Impact of the digitalization of education on the right to education. Report of the Special Rapporteur on the right to education, Koumbou Boly Barry,* UN Doc. A/HRC/50/32 (19 April 2022).
[132] Human Rights Watch, *'How Dare They Peep into My Private Life?' Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic*, 2022.

criminalising stalking[133], intimidating or threatening conduct[134], encouraging suicide[135], defamation[136], accessing online accounts without authorisation[137], etc. According to Australian law, these conducts can be punished with penalties ranging from 2 years to 10 years of imprisonment. At present, there is no civil or criminal penalty for cyberbullying under UK law. It has, however, been a matter of concern and the Education and Inspection Act 2006 specifically requires schools in England and Wales to have a policy in place to address/mitigate cyber bullying and online offences in school, regardless of whether the victim and perpetrator are on the school premises. Likewise, the Independent School Standards (England) (Amendment) Regulations 2012 requires such schools to implement anti-bullying strategies. Cyberbullying in the UK can fall under the Protection from Harassment Act 1997 (PHA), which establishes both civil and criminal protection to individuals subjected to harassment [138]. Cyberbullying may also fall under the UK's Equality Act 2010 when configurating discrimination based on disability, race, religion or belief, gender identity or sexuality. In summary, the Act protects individuals from discrimination on account of possessing any of the protected characteristics listed in the legislation and determines that schools and public sector bodies are obliged to take steps to eliminate any such conduct that may be prohibited by the Act. Other existing UK legislation may also relate to cyber bullying, even if it doesn't specifically mention it. The Communications Act 2003, for example, provides grounds for criminalising cyberbullying when it establishes that sending a message via electronic equipment which is false, grossly offensive, or of an indecent, obscene, or menacing character will be punishable by either an unlimited fine and/or imprisonment of a term not exceeding six months[139]. The Communications Act 2003 also criminalises sending a message through a public network intended to annoy, inconvenience, or cause needless anxiety to the recipient. In either case, there is no need for the message to have actually been received by the recipient, or for anyone to have been offended by it; what matters is that the sender intended for it to have an unpleasant effect.

Likewise, protection against cyberbullying and online abuse in Singapore would fall under The Protection from Harassment act 2014 (POHA) and The Protection from Online Falsehoods and Manipulation Act 2019 (POFMA)[140]. In South Africa, the law also does not directly refer to cyberbullying but the Cybercrimes Act (2020) stipulates that it constitutes an offence to engage in acts (including using data messages or electronic means) with the intentions to incite the causing of any damage to property belonging to, or violence against, a person or a group of persons, to threaten a person or group of persons with violence or damage to property and to disclose an intimate image[141]. In India, there is also no specific law regarding cyberbullying, but the Indian Information Technology Act may be used as a legal basis. It prescribes punishment for sending annoying, offensive, and insulting communication through

[133] Australia, The Crimes (Domestic and Personal Violence) Act, 2007, Section 13.
[134] Australia, The Criminal Code Act, 1995, Section 474.15.
[135] Australia, The Crimes Act, 1990, Section 31C.
[136] Australia, The Crimes Act, 1990, Section 529.
[137] Australia (NSW), The Crimes Act, 1900, Section 308H, the Criminal Code Act, 1995, Section 478.1.
[138] UK, Protection from Harassment Act (PHA), 1997, Section 1 (civil offence) and 2 (criminal offence).
[139] UK, Communications Act (CA), 2003, Section 127.
[140] Online abuse against children in Singapore can also be addressed referring to the provisions in the Penal Code, Films Act, undesirable Publications Act, Broadcasting Act and Children and Young Person Act.
[141] South Africa, Cybercrimes Act, 2020, Sections 14, 15, 16.

digital and information communication technology (Section 66A). Cyberbullying could also fall under the Indian Penal Code if it configures offenses such as defamation (Section 499), printing intended to blackmail (Section 292A), sexual harassment (Section 354A), stalking (Section 354D), or word, gesture, or act intended to insult the modesty of a woman (Section 509). However, no special protection is granted to children under these laws.

In absence of specific legislation in relation to cyberbullying, the Irish courts have relied on the Non-Fatal Offences Against the Person Act 1997 (the 'NFOAP Act') to decide on a case of online abuse[142].

As illustrated above, in most of the countries under review cyberbullying is not considered a particular offence and no special protection is granted to children in this regard. But a few countries (Japan, Australia, and China) have sought to enhance child protection against Cyberbullying with bidding legislations that sometimes impose obligations on schools. In Japan, for instance, the Act for the Promotion of Measures to Prevent Bullying, which does not separate online and offline bullying, states the obligations of national and local governments, schools, teachers and parents regarding the prevention, early detection, and response to bullying. In Australia, the Online Safety Act 2021 (the Act) defines cyberbullying material [143] and grants the Australian Office of the eSafety Commissioner the power to require online service providers to remove cyberbullying content and to manage complaints for Australians under 18 who experience cyberbullying. China has specific provisions regarding cyberbullying. The Law of PRC on the Protection of Minors (2020) provides that 'no organisation or individual should insult, slander, or threaten minors, maliciously damage the image of minors, or conduct other cyber bullying acts against minors through the Internet in the form of text, picture, audio and video, among others' (Art. 77). It also establishes the obligation of network service providers to act in a timely manner after receiving notification from the cyberbullying victim in order to stop the cyberbullying acts and prevent the spread of information, including by deleting, blocking and disconnecting links, as well as the obligation to keep relevant records and report to relevant authorities (Art. 77 and Art. 80).

The Irish government is also in the process of drafting legislation in relation to cyberbullying. The proposed Online Safety and Media Regulation Bill 2022 has been passed by the Irish Seanad (senate) as of 11 July 2022 and is currently being debated by the Irish Dáil (parliament) and should come into effect in mid-late 2023. The bill proposes to create a regulatory framework for online safety, providing oversight over how online services deliver and moderate user-generated content. This will be overseen by a duly appointed Online Safety Commissioner, who will set out binding online safety codes for how online services will address the spread and amplification of certain defined categories of harmful online content, such as: content which it is a criminal offence to share, serious cyberbullying material, material promoting eating disorders, and material promoting self-harm and suicide. Of note is Section 7(2) of the draft bill, which provides that the Online Safety Commissioner shall have all powers as are

[142] Harry Browne, *A Rare Conviction for Cyberbullying Shows it Can be Done*, 24 April 2019, the Dublin Enquirer. See also the Irish Harassment, Harmful Communications and Related Offences Act 2020 that has specific provisions with regards to the distribution or publication of intimate images without consent.

[143] According to the eSafety Commissioners cyberbullying material is 'anything posted on a social media service, relevant electronic service or designated internet service which is intended to target an Australian child, and which has the effect of seriously humiliating, harassing, intimidating, or threatening the child'.

necessary and in the performance of its functions, shall ensure 'that the interests of the public, including the interests of children, are protected, with particular commitment to the safety of children'.

Under Article 19 of the Convention on the Rights of the Child states are responsible to protect children from all forms of physical or mental violence, injury or abuse, maltreatment or exploitation. A poll conducted by UNICEF and the UN Special Representative of the Secretary-General (SRSG) on Violence against Children in 2019 demonstrated that one in three young people in 30 countries said they have been a victim of online bullying, with one in five reporting having skipped school due to cyberbullying and violence[144]. Following this poll, UNICEF has called for urgent action and the Implementation of policies to protect children and young people from cyberbullying and bullying. But as this analysis shows, much more needs to be done by states to ensure that children are protected against cyberbullying and that schools are safe places for children to learn, play and grow.

3.3.2. Profiling, automatic decision making, and direct or targeted marketing

Profiling aims to assess a person's behaviour and predict their reactions and preferences[145]. It can be used for a wide range of purposes, including to suggest or serve content to users, to determine where, when, and how frequently that content should be served, to encourage users towards particular behaviours, or to identify users as belonging to particular groups[146]. Profiling usually draws on cookies[147] or automated decision making, which are decisions made solely by a machine, without human interference. Art. 22(1) of the European Union GDPR ensures the 'right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects him or her'. It does, however, establish exceptions to this rule[148] while at the same time emphasising that automated decision-making based on profiling should not apply to children[149].

Following the European Union GDPR, France, Ireland, and the UK have sought to restrict the profiling of children to cases where it might effectively be in the best interests of the child. But it is worth noting that this is not reflected in their general protection law, and rather in guidelines or recommendations issued by the countries' data protection regulatory authority. For instance, the Irish Data Protection Act 2018 contains a section specifically dedicated to micro-targeting and profiling of children, but this section is not yet into force. It establishes that: 'It shall be an offence under this Act for any company or corporate body to process the personal data of a child [...] for the

144 UNICEF, UNICEF poll: More than a third of young people in 30 countries report being a victim of online bullying, September 2019.

145 Art. 4(4) of the European Union GDPR defines profiling as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.

146 UK, Information Commissioners' Office (ICO), Age appropriate design: a code of practice for online services, 2020, Standard 12 (Profiling).

147 According to the UK Information Officers Commission 'A cookie is a small text file that is downloaded onto 'terminal equipment' (e.g. a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions.' ICO, Age appropriate design: a code of practice for online services, 2020, Principle 12 (Profiling).

148 EU, GDPR, Art. 22(1), para. 2.

149 EU, GDPR, Recital 38 and Recital 71

purposes of direct marketing, profiling or micro-targeting. Such an offence shall be punishable by an administrative fine [...]'[150]. The Irish Data Protection Commission (DPC) has nevertheless established the principle of a 'precautionary approach' to profiling and automated decision making in relation to children, stating that 'online service providers should not profile children and/or carry out automated decision making in relation to children, or otherwise use their personal data, for marketing/ advertising purposes due to their particular vulnerability and susceptibility to behavioural advertising, unless they can clearly demonstrate how and why it is in the best interests of the child to do so[151]. Similarly, the UK Age-Appropriate Design code advises information society services to 'switch options which use profiling 'off' by default (unless they can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child)'. It also sets as a standard that organisations should 'only allow profiling if they have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing)'.

Both the Irish Data Protection Commission (DPC) and the UK Information Commissioners' Office (ICO) advise information society services (ISS) to take a Data Protection Impact Assessment (DPIA) to assess the risk posed to children by processing their personal data in case of profiling, automated decision making and marketing[152]. Both regulatory authorities also recommend organisations not to exploit children's vulnerabilities and susceptibilities, whilst also recommending that industry-specific guidance is taken into account when undertaking marketing activities. The UK government is discussing the Online Safety Bill (OSB) which introduces a new obligation to online services providers to prevent children's exposure to 'fraudulent adverts'. But the Bill, which is expected to be passed in 2023, fails to ban the use of children's data for direct marketing.

It is worth noting that in July 2022, the EU adopted the Digital Services Act (DSA), which will apply in the EU from 2024[153] and will probably affect EU countries' legislations (France and Ireland) and influence others. The DSA prohibits online intermediaries (such as online platforms) from subjecting minors to targeted advertising, along with profiling users for advertising purposes by using special category data. The Act also imposes a ban on "nudging" and "dark patterns" (i.e. on any techniques that seek to influence or manipulate user decision-making).

It is also important to highlight that while general data protection laws fail to ban advertising and marketing techniques to children, other laws may apply regardless of whether data processing is taking place. In Brazil, for example, following the provisions of the Consumer's Defense Code regarding abusive marketing and advertising[154], the National Council of the Rights of the Child and the Adolescent (CONANDA) issued a Resolution banning abusive ads targeting children under 12[155]. The Resolution considers abusive all types of advertising and marketing

[150] Ireland, Data Protection Act 2018, Section 30.

[151] Ireland, Data Protection Commission (DPC), The Fundamentals for a Child-Oriented Approach to Data Processing, 2021. Section 6.

[152] UK, Information Commissioners' Office (ICO), Age appropriate design: a code of practice for online services, 2020, Standard 12 (Profiling).

[153] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)

[154] Brazil, Law 8.078/90, Consumers Defense Code, Art. 37, para. 2.

[155] Brazil, CONANDA, Resolution No. 163, Art. 2, para. 2.

communications designed to target children and adolescents (including the advertising of products, services, brands, and companies, regardless of the form, media, or means) with the intention of persuading the children to consume. The resolution also establishes that marketing communications within day care centres and educational institutions, from kindergarten to elementary education, is also considered abusive.

It is nevertheless clear that those regulations do not sufficiently protect children in educational environments against profiling, direct or targeted marketing, and automatic decision making. The Human Rights Watch report 'How Dare They Peep into My Private Life?' Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic' has indeed demonstrated that children's data extracted from educational settings were used to target them with personalised content and advertisements that followed them across the internet, including outside the educational platforms or products[156].

3.3.3.Sharing with third parties

Most of the current legislations pertaining to the countries we reviewed do not specifically regulate how and when the sharing of children's personal information is considered to be lawful. Children are generally submitted to the same provisions applied to adults and specific and previous consent is usually required whenever data collected is to be shared with third parties. But the Human Rights Watch report mentioned previously has shown that despite those general regulations, children's data collected in educational environments in countries like India, Brazil, or France during the Covid pandemic were shared with Ad Tech (advertising technology) companies without awareness of the data subjects nor their legal guardians[157].

Some countries have pushed forward guidance that intends to offer enhanced protection to children with regards to the privacy of their data, restricting cases where sharing children's data with third parties would be considered lawful. For example, a recommendation from France's regulatory authority (CNIL) advises that data of children should not be re-used or passed on to third parties for commercial or advertising purposes, unless they can demonstrate that they are acting for overriding reasons in the best interests of the child[158]. The UK Age-Appropriate Design Code established that children's data should not be disclosed unless the ISS can demonstrate a compelling reason to do so, taking into account the best interest of the child[159]. It also establishes that children's personal data should not be used in ways that have been shown to be detrimental to their wellbeing, or that would go against industry codes of practice, other regulatory provisions, or Government advice[160]. But as mentioned previously,

[156] Human Rights Watch, *'How Dare They Peep into My Private Life?' Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic*, 2022.

[157] Human Rights Watch, *'How Dare They Peep into My Private Life?' Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic*, 2022.

[158] France, CNIL, Recommendation 8: Provide specific safeguards to protect the interests of the child.

[159] UK, Information Commissioners' Office (ICO), Age appropriate design: a code of practice for online services, 2020, Standard 9 (Data sharing).

[160] UK, Information Commissioners' Office (ICO), Age appropriate design: a code of practice for online services, 2020, Standard 5 (Detrimental use of data).

whether the Age-Appropriate Design Code applies to educational settings will depend on if ISS are offering services directly to learners – and not through the intermediary of a school[161].

Despite those regulations, no specific legislation banning sharing students' data with third parties without their consent has been implemented, except the Chinese Provisions on the Protection of Minors by Schools. Indeed, China has extensive regulations regarding sharing children's data: Chinese Provisions on the Cyber Protection of Children's Personal Information, for example, establish that if a network operator wishes to transfer children's personal information to a third-party, it should establish the scope and purpose of the handling and conduct security assessment of the entrusted party or authorise a third-party agency to do so[162]. The law also requires network operators to grant minimum authorisation access to data of minors for their staff so as to prevent illegal copying or downloading of such information[163]. Similarly, but providing specific protection in educational environments, the Chinese Provisions on the Protection of Minors by Schools stipulate that schools collecting personal information of students are mandated to manage and keep this information confidential, and cannot disclose, publicise, or trade such information[164]. Furthermore, it forbids schools and educational staff from disclosing students' information and from using it to seek benefits, establishing penalties to teachers and staff that violate this provision[165]. The Cyberspace Administration of China has released a Draft of Regulations on Cyber Protection of Minors which is, to date, under public consultation. The regulation should reinforce the above provisions regarding sharing children's personal information. If the law passes in its current form, it will require that personal information processors do not provide minors personal information they handle to any other person (Article 38). However, it establishes that if it is truly necessary to provide it to others, processors should conduct a personal information protection impact assessment in advance and inform the minors or their guardians of the recipient's name, contact information, purpose of the processing, method of processing, and types of personal information, and obtain separate consents[166]. Articles 42 and 45 will also enforce existing provisions demanding processors to strictly set access rights for their staff based on the principle of minimum authorization and requiring cyberspace authorities, other relevant competent authority as well as their employees, to safeguard the confidentiality of the personal information of minors. It will specifically determine that any child personal data that cyberspace authorities or relevant competent authorities come to know in the course of performing their duties should not be disclosed to third parties[167]. If those provisions will improve child safety and security, they still need to be transformed into law and implemented in practice. Despite these existing Chinese laws, this review did not find any decisions on its implementation.

[161] UK, Information Commissioners' Office (ICO), FAQs for education technologies (EdTech) and schools, available at https://ico.org.uk/for-organisations/childrens-code-hub/faqs-for-education-technologies-edtech-and-schools/

[162] China, Provisions on the Cyber Protection of Children's Personal Information, Art. 16 and 17.

[163] China, Provisions on the Cyber Protection of Children's Personal Information, Art. 15.

[164] China, Provisions on the Protection of Minors by Schools, Art. 10

[165] China, Provisions on the Protection of Minors by Schools, Art. 38.

[166] China, Cyberspace Administration, Draft of Regulations on Cyber Protection of Minors.

[167] China, Cyberspace Administration, Draft of Regulations on Cyber Protection of Minors.

3.3.4.Geolocalisation

The Human Rights Watch analysis mentioned previously showed that 89 per cent of the EdTech products analysed could put children's privacy at risk[168]. It showed that EdTech products endorsed by governments collected and shared information on children's locations, putting not only their privacy and well-being but also their physical and mental integrity at risk. Geolocalisation can allow tracking of where students live, where they go to school, places they frequently go (such as sports clubs, for example), thus putting them at risk of abduction, physical and sexual abuse, and trafficking.

According to the above-mentioned report, 'of the 73 apps examined by Human Rights Watch, 21 apps (29 percent) granted themselves the ability to collect precise location data, or GPS coordinates that can identify a child's exact location to within 4.9 metres. These 21 apps also had the ability to collect the time of the device's current location, as well as the last known location of the device — revealing exactly where a child is, where they were before that, and how long they stayed at each place'[169]. Furthermore, the report demonstrated that 'four apps are built and owned by the education ministries of India, Indonesia, Iran, and Turkey, giving these governments the ability to track an estimated 29.5 million children and pinpoint where they are, at any given moment, until the app is closed by the user'[170]. Even more worryingly, the report concluded that the Indian EdTech App owned and operated by the Indian's Ministry of education collected children's precise location without the government disclosing it to users, thus misleading both students and their parents.

India is amongst the countries analysed in this review and up to the moment of this paper writing there are no current binding laws banning or restricting geolocalisation in educational environments. Amongst the countries reviewed in this paper only a few provided recommendations and standards referring to geolocalisation, and none had binding laws banning schools to track or allow others to track their students' location. France's regulatory agency CNIL, for example, has recommended that geolocalisation should be disabled by default[171]. Similarly, the UK Age-Appropriate Design Code provides that ISS 'should switch geolocation options off by default (unless they can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child), and provide an obvious sign for children when location tracking is active'[172].

Indeed, privacy by default has been one of the solutions pushed by many regulatory agencies to enhance children's rights in the digital world.

---

[168] Human Rights Watch, *'How Dare They Peep into My Private Life?' Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic*, 2022.

[169] Human Rights Watch, *'How Dare They Peep into My Private Life?' Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic*, 2022.

[170] Human Rights Watch, *'How Dare They Peep into My Private Life?' Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic*, 2022.

[171] France, CNIL, Recommendation 6 : Strengthen the information and rights of children by design (2021)

[172] UK, Information Commissioners' Office (ICO), Age appropriate design: a code of practice for online services, 2020, Standard 10 (Geolocalisation).

3.3.5.Privacy by default

Technology can contribute to better privacy and security – including that of students – by the way it is designed and incorporates control and restriction options in the operations performed on data as it is being collected and processed[173]. Although not specific to children nor to a learning environment, Article 25 of the EU GDPR provides that protection measures should be built into the architecture and functioning of a product or service from the very start of the design process, stating that 'controllers must … implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects'. Specifically applying to the educational context, recommendation 8.1.1 of the EU Guidelines on Children Data Protection in Education states that 'since children merit special protection, the expected standards for the processing of children's data in the education sector should set a high bar by design, to meet appropriate standards of quality and the rule of law, and data protection by design and by default [174]. Accordingly, Section 76 of the Irish Data Protection Act regulates data protection by design and by default. It is complemented by guidelines issued by the Data Protection Commission (DPC) – 'The Fundamentals' – stating that online service providers that routinely process children's personal data should, by design and by default, have a consistently high level of data protection which is "baked in" across their services and provide child-friendly privacy information with regards to proactive consent to cookies[175].

Since most users do not change their default settings, encouraging service providers to ensure that additional features that are not part of the core service are disabled by default, as recommended by France's regulatory authority CNIL[176], could indeed enhance the protection of children whenever their data is being processed. But it is relevant to highlight that even where privacy settings by design are ensured, transparency remains the key to ensuring that children's rights are protected, respected, and fulfilled: children who choose to change their default settings should be able to get the complete information, guidance and advice on what it means to change de default settings before they do so. Information must be transparent, clear, and use child-friendly language in order to make sure children fully understand the consequences of changing the default settings. Moreover, when requiring consent to change default settings, the parties involved must assure that consent is given by the person having the capacity to do so[177].

The UK Age-Appropriate design code has a very illustrative example on how this could be done:

---

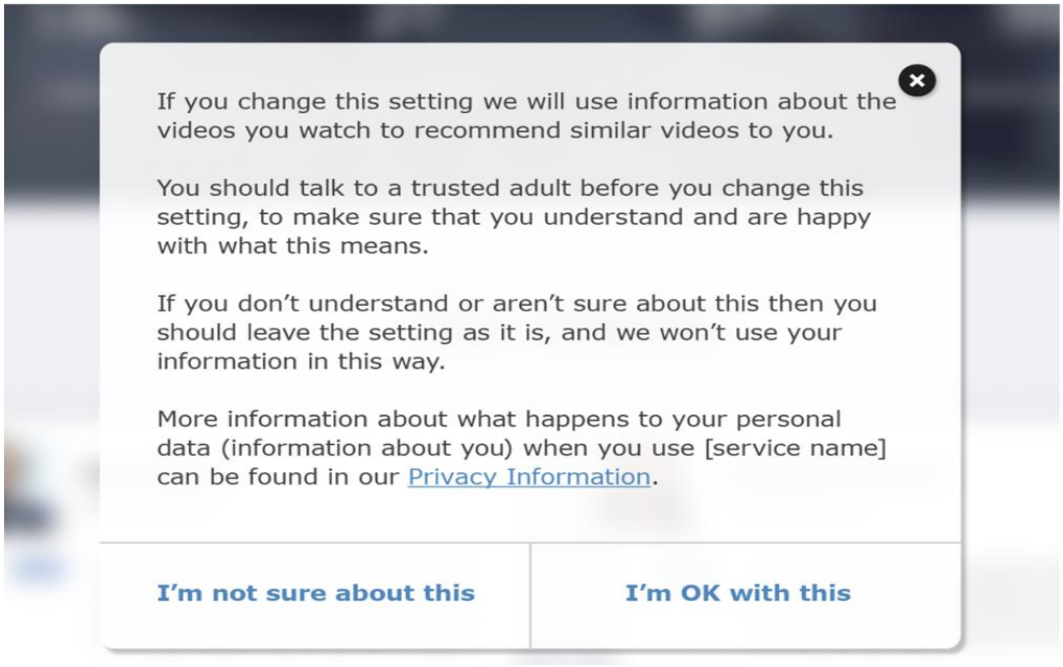
[173] UNESCO, Minding the Data. Protecting Learners' privacy and security, 2022.

[174] EU, Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, Children's data protection in an education setting - Guidelines (2021)

[175] Ireland, Data Protection Commission (DPC) , Fundamentals for a Child-Oriented Approach to Data Processing,2021

[176] France, CNIL, Recommendation 8: Provide specific safeguards to protect the interests of the child (2021)

[177] For further information, see the section on this paper on consent.



3.3.6.Sensitive Data

Lawful processing of children's data should also respect the rules regarding the collection, retention, use and disclosure of sensitive data. Sensitive data usually refers to data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, sex life or sexual orientation, as well as genetic and biometric data and data concerning one's health.

The Special Rapporteur on the Right to Education has recommended that states determine what categories of sensitive personal data that should never be collected in educational settings, in particular from children. But almost all the legislations analysed in this paper treat children and adults alike when legislating about special category data. China is the only country amongst those reviewed that considers personal information of minors under the age of 14 as sensitive personal information[178].

3.3.7.Accountability

Accountability is crucial for human rights enforcement. It is only by holding states accountable for not protecting, enforcing, and/or not implementing human rights at a national level that we ensure positive and sustainable changes in the educational environment. This section briefly analyses accountability from three perspectives: due diligence, administrative and judicial remedies. It shows that very little has been done to hold both state and non-

[178] The Chinese Personal Information Protection Law (2021) provides that personal information of minors under the age of 14 are to be treated as sensitive personal information and can only be processed when there are specific purposes, sufficient necessity, and after protective measures have been adopted and parental consent has been obtained.

state actors (specifically EdTech companies) accountable for violations of student's rights in the use of technology in education.

Human rights and/or child rights due diligence processes

In most of the countries we reviewed there is no provision requiring governments or companies to conduct and publish human rights and/or child rights due diligence processes to verify compliance with human rights and/or child rights.

Under the European Union GDPR, a Data Protection Impact Assessment (DPIA) is required as a part of the protection by design principle when collecting and processing is likely to involve 'a high risk' to the rights and freedoms of natural persons[179]. The Article 29 Working Party, consisting of representatives from each data protection authority in the EU, has adopted guidelines on DPIAs and whether processing is likely to result in a high risk for the purposes of the GDPR[180]. The guidelines follow Recital 75 of the RU GDPR[181], and shed light on what would be considered a high risk for the purposes of conducting a DPIA. Amongst others, it enunciates a few criteria, including automatic decision making; evaluation or scoring, including profiling and predicting; systematic monitoring; processing special category data; data transfer across borders; use or applying of innovative technological or organisational solutions; and data concerning vulnerable data subjects. Those regulations have been incorporated by France, UK and Ireland, but they do not refer specifically to children nor to educational contexts. Nevertheless, the UK Information Commissioner's Office and the Irish Data Protection Commission have advised information society services to undertake a Data Protection Impact Assessment (DPIA) to assess and mitigate risks to the rights and freedoms of children who are likely to access their service. Both the UK Age Appropriate Design Code and the Irish Fundamentals for a Child-Oriented Approach to Data Processing specifically refer to the use of the personal data of children for marketing purposes, profiling or other automated decision-making, as well as online services offered directly to children, stressing that the principle of the best interests of the child should be the criteria that prevails when balancing risks to children's fundamental rights and commercial interests in the DPIA.

Similarly, Brazilian General Data Protection law establishes that the Data Protection Regulatory Authority (ANDP) can request the government and controllers to publish a Data Protection Impact Report (DPIR) assessing risks to civil liberties and fundamental rights, as well as measures, safeguards and risk mitigation mechanisms[182]. Pending regulations from the regulatory authority regarding the impact report, the Brazilian Digital Government Secretariat issued guidelines addressed to the public sector to instruct public entities on the interpretation of the General Data

[179] EU, GDPR, Art. 35

[180] EU, Article 29, Data protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (2017)

[181] Recital 75 of the EU GDPR details harms and risks that organisations need to safeguard individual against, including processing that could give rise to: discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage. EU, GDPR, Recital 75.

[182] Brazil. Law No. 13.709/2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019), Art. 5 (XVII), Art. 10 para. 3, Art. 32.

Protection Law. The guidelines advise public entities to issue a Data Protection Impact Report when children and adolescents data are processed, as well as in cases of geolocalisation, profiling and automated decision-making that may have legal effects, including decisions designed to define a data subject's personal, professional, consumer and credit profile or aspects of their personality[183].

The Australian Government Agencies Privacy Code (the Code) is a binding instrument that sets out specific requirements that government agencies must take as part of complying with Australian Privacy Principle 1.2 and applies to all Australian Government agencies subject to the Privacy Act 1988 (except for Ministers). It requires, amongst others, that government agencies (i) undertake a written Privacy Impact Assessment (PIA) for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information; (ii) keep a register of all PIAs conducted and publish this register, or a version of the register, on their websites; and (iii) take steps to enhance internal privacy capability, including by providing appropriate privacy education or training in staff induction programs, and annually to all staff who have access to personal information. Following the Code, the Office of the Australian Information Commissioner (OAIC) organises courses on PIA and has published a Guide to undertaking privacy impact assessments[184].

While the above provisions are a step forward in protecting children from the risks associated with online processing of their personal information, they do not provide the same assurances as human rights and/or child rights due diligence processes, in particular because they are grounded in a risks rather than rights-based approach. Therefore, they do not fully comply with the recommendations made by the Special Rapporteur on the Right to Education, specifically regarding the recommendations that child rights impact assessments and data privacy audits should be conducted before adopting digital technologies in education.

Administrative and judicial remedies

All countries under review have entrusted a regulatory authority with the power to bring administrative actions against parties who have committed a breach of data laws. The extent to which they can investigate, impose civil liability, issue fines against those violating the data protection laws, and apply the courts varies according to the country. Where more than one regulatory authority exists, they have been entrusted with different mandates. In Australia, for example, the Office of the Australian Information Commissioner (OAIC) has the power to investigate practices that have the potential to breach the Australian Privacy Act (after a complaint or on its own initiative). It can also apply the courts to seek a civil penalty order against offenders or to require an injunction to restrain a person from engaging in conduct that would constitute a breach of relevant the privacy law. The Office of the eSafety Commissioner, on the other hand, is entrusted to manage complaints for Australians under 18 who

[183] Guidelines can be found here (in Portuguese).

[184] Australia, OAIC, Guide to undertaking privacy impact assessments (2021)

experience cyberbullying or seriously threatening, intimidating, harassing or humiliating online behaviour, having the power to require that service providers remove abusive material.

With regards to children, while some countries recommend that information on how to exercise their rights should be available and accessible in a child-friendly manner, the analysis did not find any complaint mechanisms or administrative or judicial remedies specifically tailored for them. While not specifically directed to children, it is with noting that Article 69 of the Chinese Personal Information Protection Law reversed the burden of proof by holding personal information handlers liable to the extent that they 'cannot prove they are not at fault'. But unfortunately, the mechanism of holding relevant entities or individuals to be liable for any violation of data protection laws and regulations in China is very complicated. The regulatory authorities involved may include cyberspace administrations, public security authorities, national security authorities, industry and information technology authorities, market regulation authorities, and other governmental authorities, both at the national and local level. The entities in question involved in such mechanisms may also include various governmental authorities, public institutions, a wide range of enterprises and companies, social organisations, self-governing mass organisations and other entities and individuals. Therefore, it can be very difficult to specifically address violations of students' rights, despite the inversion of the burden of proof.

At the time of the drafting of this paper, this analysis did not encounter any court jurisprudence on violations of children's data privacy specifically related to the use of technology in educational settings in the countries reviewed in this research. Nevertheless, it is worth noting that pressure from civil society has resulted in advances in the protection of students with regards to the use of technology as a learning too in a few countries. After the publication of the Human Rights Watch Report (HRW) denouncing how EdTech companies endorsed by states collected and shared students' data in violation of international human rights treaties, some states have taken actions to minimise the risks encountered by children when using digital products that are owned and/or approved by states as learning tools.

The Indian government, for example, has announced a third-party security audit of its educational app Diksha, that provide online education to students from 1st to 12th grade. According to Human Rights Watch, the app exposed the personal data of millions of students and teachers - including children's names, schools, test scores, districts, and precise information on their location data, as well as partially redacted phone numbers and email addresses. HRW also documented that the Indian app shared data with third-party companies using a tracker designed for advertising and called attention to the fact that the Indian proposed data protection law would not prevent such violations from happening again, showing that the government still has a lot to do to ensure and enforce that students learn in a safe environment where their human rights are respected, protected and fulfilled.

The Human Rights Watch report has also engendered a few changes in the use of technology in education in Brazil. HRW reported that several Brazilian learning websites and apps - including two owned and/or approved by the Brazilian states of São Paulo and Minas Gerais and used in public schools during Covid-19 - violated students' rights,

including with data surveillance techniques. 'These websites not only watched children in their online classrooms, but followed them across the internet, outside school hours, and deep into their private lives'185. Moreover, the websites used profiling and targeting tools and then shared users information with a wide range of advertising companies. The HRW investigation has called the attention of Brazilian media and ultimately led to one website, DragonLearn, being taken down from the internet as well as to action from the education secretariat of Minas Gerais that ended up removing all ad tracking from its website. Despite these advances, we note Human Rights Watch's comment that neither the Minas Gerais nor the São Paulo education secretariat appear to have checked whether their online learning endorsements were safe for children to use. There is thus an urgent need to pass specific legislation that can prevent those situations from happening and that hold states accountable to their duties of ensuring children's rights to privacy, dignity, and education.

These examples highlight the important role of civil society (CSOs, parent-teacher associations, student unions, teacher unions and the media) on monitoring the use of technology in education, calling out private Ed Tech companies and States on their responsibility to protect children's rights to education and privacy, pushing for national implementation of students' international rights as it relates to the relationship between technology and education, and holding state and non-state actors accountable for any violation of international human rights law.

4.Conclusion and policy implications

Technology has fundamentally changed the way in which children exercise and realise their rights - including their right to education. While the use of technology in education can enhance children's right to education, it can also put their physical and mental integrity, privacy, and dignity at risk. The UN Human Rights Council (UNHRC) has noted that the violations and abuses of the right to privacy in the digital age may affect all individuals, but that such violations may have a particular effect on children[186].

This paper provides a circumspect overview of some domestic legislation with regards to the protection of child privacy and security in respect to the processing of their personal data in the use of education technology. Although limited in scope, the analysis of ten national legal frameworks (Australia, Brazil, China, France, Ireland, India, Japan, Singapore, South Africa and the United Kingdom) illustrates the variety of domestic protection ranging from some specific legal protections to no legally binding provisions addressing the particular risks faced by children with regards to education technologies. Indeed, our analysis of national legislations concluded that most of the general data protection instruments under review make no distinction between adults and children with respect to the

185 https://www.hrw.org/news/2023/04/03/brazil-online-learning-tools-harvest-childrens-data

186 UNHRC 'The right to privacy in the digital age' A/HRC/34/L.7/Rev.1 (2017)

treatment of their personal data (Australia, Japan, Singapore, India, and South Africa). Following the EU GDPR and its recognition that children deserve 'special protection', European Countries have issued a number of guidelines and standards enforcing the protection of children's privacy rights but whether they apply to educational settings or not may depend on if the services are provided directly to children or through an intermediary, such as a school (as is the case for the Irish Fundamentals and the UK Age-Appropriate Design Code). While some general protection laws specifically grant children special protection, such as the Brazilian GDPR, China is the country having extensive protection regarding children's online privacy and safety - but as described above, those provisions are very difficult to enforce, entailing complex procedures regarding multiple public actors.

The EU has recently issued the Guidelines on Children's data protection on education settings[187], and one could expect it to have police and legislative implications not only in Europe, but also across the world. Nevertheless, we can conclude that there is an urgent need to push states to ensure legislative measures regulating technology in education, following the recommendations of the UN CRC and of the UN Special Representatives. Moreover, the existing legal framework and policies should be enforced by states in order to ensure that schools are a safe place for children to learn, play, develop and thrive.

[187] EU, Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, Children's data protection in an education setting - Guidelines (2021)

ACKNOWLEDGEMENTS

Written by the Right to Education Initiative (RTE) - a global human rights organisation focusing on the right to education. RTE promotes education as a human right, making international and national law accessible to everybody. We conduct research and legal analysis, and we develop tools and guides to help understand and effectively use human rights mechanisms to claim and enforce the right to education. We build bridges between disciplines (human rights, education, and development), actors (CSOs, international organisations, academics), and language communities, linking international, national and local advocacy with practical engagements leading to positive changes on the ground. For more information, see RTE website: www.right-to-education.org.

This report was written by Juliana Lima and Susie Talbot under the supervision of Delphine Dorsi.

Special thanks to Advocates for International Development and the following law firms for their generous pro bono work in providing information about the implementation of the right to education at national level: Anglo American, Dechert LLP, DLA Piper UK LLP, Morrison Foerster.

REFERENCES

International Human Rights Treaties

Convention on the Elimination of All forms of Racial Discrimination

Convention on the Elimination of All Forms of Discrimination against Women, 1979

Convention on the Rights of the Child, 1989

Convention on the Rights of Persons with Disabilities, 2006

Convention on the Protection of the Rights of All Migrant Workers and Members of their families, 1990, Article 30, 43(1) and 45(1).

Convention Relating to the Status of Refugees, 1951

Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters, 1998

Declaration on the Rights of Indigenous Peoples, 2007

International Covenant on Economic, Social and Cultural Rights (CESCR) 1966

International Covenant on Civil and Political Rights (ICCP)

UNESCO Convention against Discrimination in Education, 1960

Universal Declaration on Human Rights

UN Treaty Bodies

Committee on the Elimination of Discrimination against Women (CEDAW), General recommendation No. 36 on the right of girls and women to education, UN Doc. CEDAW/C/GC/36 (16 November 2017)

Committee on Economic, Social and Cultural Rights (CESCR), General Comment No. 11 on plans of action for primary education, UN Doc. E/C.12/1999/4 (11 May 1999)

Committee on Economic, Social and Cultural Rights (CESCR), General Comment No. 13 on the right to education, UN Doc. E/C.12/1998 (8 December 1999)

Committee on Economic, Social and Cultural Rights (CESCR), Statement by the Committee: An evaluation of the obligation to take steps to the "Maximum of available resources" under an optional protocol to the Covenant, UN Doc. E/C.12/2007/1 (21 September 2007).

Committee on the Rights of the Child (CRC), Concluding observations on the combined fifth and sixth periodic reports of the Kingdom of the Netherlands, UN Doc. CRC/C/NLD/CO/5-6 (9 March 2022)

Committee on the Rights of the Child (CRC), Concluding observations on the combined fourth to sixth periodic reports of Tunisia, UN Doc. CRC/C/TUN/CO/4-6 (2 September 2021)

Committee on the Rights of the Child (CRC), Concluding observations on the combined fifth and sixth periodic reports of Portugal, UN Doc. CRC/C/PRT/CO/5-6 (9 December 2019)

Committee on the Rights of the Child (CRC), Concluding observations on the initial report of the State of Palestine, UN Doc. CRC/C/PSE/CO/1 (6 March 2020)

Committee on the Rights of the Child (CRC), Concluding observations on the combined fourth and fifth periodic reports of Singapore, UN Doc. CRC/C/SGP/CO/4-5 (28 June 2019)

Committee on the Rights of the Child (CRC), General Comment No. 5 on General measures of implementation of the Convention on the Rights of the Child, UN Doc. CRC/GC/2003/5 (27 November 2003)

Committee on the Rights of the Child (CRC), General comment No. 14 on the right of the child to have his or her best interests taken as a primary consideration, UN Doc. CRC/C/GC/14 (29 May 2013)

Committee on the Rights of the Child (CRC), General Comment No. 16 on State obligations regarding the impact of the business sector on children's rights, UN Doc. CRC/C/GC/16 (17 April 2013)

Committee on the Rights of the Child (CRC), General Comment No. 19 on public budgeting for the realisation of children's rights (art. 4), UN Doc. CRC/C/GC/19 (20 July 2016).

Committee on the Rights of the Child (CRC), General Comment No. 25 on Children's rights in relation to the digital environment, UN Doc. CRC/C/GC/25 (2 March 2021)

UN Human Rights Council (UN HRC), Guiding Principles on Business and Human Rights (UNGPs)

UN Human Rights Council (UN HRC), Human rights and transnational corporations and other business enterprises, UN Doc. A/HRC/RES/17/4 (6 July 2011)

UN Human Rights Council (UN HRC), Report on the Special Rapporteur on the right to education, 'Impact of the digitalization of education on the right to education', UN Doc. A/HRC/50/32 (19 April 2022)

UN Human Rights Council (UN HRC), Report of the Office of the United Nations High Commissioner for Human Rights, 'The practical application of the Guiding Principles on Business and Human Rights to the activities of technology companies', UN Doc. A/HRC/50/56 (April 2022)
UN Human Rights Council (UN HRC), Report of the United Nations High Commissioner for Human Rights, 'The right to privacy in the digital age', UN Doc. A/HRC/39/29 (3 August 2018)
UN Human Rights Council (UN HRC), Report of the Special Rapporteur on the right to education, 'Issues and challenges to the right to education in the digital age', UN Doc. A/HRC/32/37 (6 April 2016)
UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/73/348 (29 August 2018)
UN General Assembly, Report of the Special Rapporteur on the right to privacy, 'Artificial intelligence and privacy, and children's privacy', UN Doc. A/HRC/46/37 (25 January 2021)

Regional and National legislations

Australia

Australian Data protection Act (The Privacy Act), 1988
Australia, The Crimes Act, 1990
Australia, The Crimes (Domestic and Personal Violence) Act, 2007
Australia, The Criminal Code Act, 1995
Online Safety Act 2021 (the Act)
Office of the Australian Information Commissioner (OAIC), Australian Privacy Principles Guidelines – APP Guidelines
Office of the Australian Information Commissioner (OAIC), Guide to undertaking privacy impact assessments (2021)
Office of the Australian Information Commissioner (OAIC), Australian Government Agencies Privacy Code (the Code)
Australian states and territories relevant laws:

- Information Privacy Act 2014 (Australian Capital Territory)
- Information Act 2002 (Northern Territory)
- Privacy and Personal Information Protection Act 1998 (New South Wales)
- Information Privacy Act 2009 (Queensland)
- Personal Information Protection Act 2004 (Tasmania), and
- Privacy and Data Protection Act 2014 (Victoria)

Brazil

Law No. 13.709/2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019)
Law No. 8.078/90, Consumers Defense Code
CONANDA, Resolution No. 163

China

Cyberspace Administration, Draft of Regulations on Cyber Protection of Minors.
Cybersecurity Law (2016)
Data Security Law (2021)
Law of the People's Republic of China on the Protection of Minors (2020)
Personal Information Protection Law (2021)
Provisions on Cyber Protection of Children's Personal Information (2019).
Provisions on the Protection of Minors by Schools (2021)
Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services
Regulations on Cyber Protection of Minors (Draft for Comments) (2022)

European Union

Article 29, Data protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (2017)
Committee of Ministers, Recommendation CM/Rec (2018)7, Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018)
Council of Europe, Children's data protection in an education setting - Guidelines (2021).
Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, Children's data protection in an education setting - Guidelines (2021)
European Commission, New European strategy for a Better Internet for Kids – Questions and Answers, May 2022.
General Data Protection Regulation, UE 2016/679
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)
Technical Standards Regulations Directive (EU) 2015/1535

Ireland

Data Protection Act (2018)
Data Protection Commission of Ireland (DPC), the Fundamentals for a Child-Oriented Approach to Data Processing (2021)
Data Protection Commission of Ireland (DPC), Guidance for Children on their data protection rights
Education (Digital Devices in Schools) Bill (2018)
Harassment, Harmful Communications and Related Offences Act (2020)
Non-Fatal Offences Against the Person Act (1997) (the 'NFOAP Act')

India

Indian Information Technology Act
Indian Penal Code

Latin American and the Caribbean

Regional Agreement on Access to Information, Public Participation and Justice in Environmental Matters in Latin America and the Caribbean (Escazú, Costa Rica, 4 March 2018)

France

Act No. 78-17 of January 6, 1978 on Information Technology, Data Files and Civil Liberties.
Act No. 2018-493 of 20 June 2018, incorporating the EU GDPR in Act No. 78-17
Ordinance No. 2018-1125 of 12 December 2018
CNIL, Recommendations to enhance the protection of children online (2021)
CNIL, Recommendation 1: Regulate the capacity of children to act online (2021)
CNIL, Recommendation 4: Seek parental consent for children under 15 (2021)
CNIL, Recommendation 6: Strengthen the information and rights of children by design (2021)
CNIL, Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy (2021)
CNIL, Recommendation 8: Provide specific safeguards to protect the interests of the child (2021)

Japan

The Act on the Protection of Personal Information ("APPI"), Act No. 57 (2003).
Act on Establishment of Enhanced Environment for Youth's Safe and Secure Internet Use, Act No. 79 (2008).
Act for the Promotion of Measures to Prevent Bullying, Act Nà. 71 (2013)

Singapore

Personal Data Protection Commission, "Advisory Guidelines on the PDPA for Selected Topics", revised 17 May 2022.
the Personal Data Protection Commission (PDPC) issued specific guidelines for the education sector (The Advisory Guidelines for the Education Sector`
The Protection from Harassment act 2014 (POHA)
The Protection from Online Falsehoods and Manipulation Act 2019 (POFMA)

United Kingdom

Communications Act (CA), 2003
Data Protection Act 2018
Education and Inspection Act 2006
Independent School Standards (England) (Amendment) Regulations 2012
Information Commissioners' Office (ICO), Best interests of the child self-assessment
Information Commissioner's Office (ICO), FAQs for education technologies (EdTech) and schools
Information Commissioner's Office (ICO), Guidance on children and the UK GDPR
Information Commissioner's Office (ICO), Guide to the General Data Protection Regulation (GDPR)
Information Commissioner's Office (ICO),The Age-Appropriate Design Code
Malicious Communications Act 1998
Protection from Harassment Act (PHA), 1997
The Public Order Act 1986
The UK Code of Practice for Online Social Media Platforms.
UK General Data Protection Regulation (EU) 2016/679)

South Africa

Cybercrimes Act, 2020

USA

Children's Online Privacy Protection Act (COPPA), 1998

Other References

The Abidjan Principles on the human rights obligations of States to provide public education and to regulate private involvement in education. (2019)

Campagnucci, F., Following the pandemic: The dilemma around digital rights in education. In, Campanha Latinoamericana por el Derecho a la Education (CLADE), Human right to education: horizons and meanings in the post pandemic (2020)

Harry Browne, A Rare Conviction for Cyberbullying Shows it Can be Done (24 April 2019)

Hennessy, S., Jordan, K., Wagner, D. and Ed Tech Hub Team. Problem analysis and focus of EdTech Hub's Work: technology in education in low- and middle-income countries. EdTech Hub. (Working Paper 7), (2021)

Hooper, L., Livingstone, S., and Pothong, K. Problems with data governance in UK schools: the cases of Google Classroom and ClassDojo. Digital Futures Commission, 5Rights Foundation., (2022).

Human Rights Watch, 'How Dare They Peep into My Private Life?' Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic (2022)

Right To Education Initiative, The Right to Education Initiative's contribution to the global conversation on the right to education: Reviewing and extending the understanding of the right to education in the 21st Century (2021)

UNESCO, Minding the Data. Protecting Learners' privacy and security (2022)

UNESCO, Supporting learning recovery one year into COVID-19: the Global Education Coalition in action (2021).

UNICEF, UNICEF poll: More than a third of young people in 30 countries report being a victim of online bullying (September 2019)

APPENDICES

Appendix A: Selected extracts from CRC general comment no. 25

70. States parties should take legislative, administrative and other measures to ensure that children's privacy is respected and protected by all organizations and in all environments that process their data. Legislation should include strong safeguards, transparency, independent oversight, and access to remedy. States parties should require the integration of privacy-by design into digital products and services that affect children. They should regularly review privacy and data protection legislation and ensure that procedures and practices prevent deliberate infringements or accidental breaches of children's privacy. Where encryption is considered an appropriate means, States parties should consider appropriate measures enabling the detection and reporting of child sexual exploitation and abuse or child sexual abuse material. Such measures must be strictly limited according to the principles of legality, necessity and proportionality.

71. Where consent is sought to process a child's data, States parties should ensure that consent is informed and freely given by the child or, depending on the child's age and evolving capacity, by the parent or caregiver, and obtained prior to processing those data. Where a child's own consent is considered insufficient and parental consent is required to process a child's personal data, States parties should require that organizations processing such data verify that consent is informed, meaningful and given by the child's parent or caregiver.

72. States parties should ensure that children and their parents or caregivers can easily access stored data, rectify data that are inaccurate or outdated and delete data unlawfully or unnecessarily stored by public authorities, private individuals or other bodies, subject to reasonable and lawful limitations. 36 They should further ensure the right of children to withdraw their consent and object to personal data processing where the data controller does not demonstrate legitimate, overriding grounds for the processing. They should also provide information to children, parents, and caregivers on such matters, in child-friendly language and accessible formats.

73. Children's personal data should be accessible only to the authorities, organizations and individuals designated under the law to process them in compliance with such due process guarantees as regular audits and accountability measures.37 Children's data gathered for defined purposes, in any setting, including digitized criminal records, should be protected and exclusive to those purposes and should not be retained unlawfully or unnecessarily or used for other purposes. Where information is provided in one setting and could legitimately benefit the child through its use in another setting, for example, in the context of schooling and tertiary education, the use of such data should be transparent, accountable and subject to the consent of the child, parent or caregiver, as appropriate.

74. Privacy and data protection legislation and measures should not arbitrarily limit children's other rights, such as their right to freedom of expression or protection. States parties should ensure that data protection legislation respects children's privacy and personal data in relation to the digital environment. Through continual technological innovation, the scope of the digital environment is expanding to include ever more services and products, such as clothes and toys. As settings where children spend time become "connected", through the use of embedded sensors connected to automated systems, States parties should ensure that the products and services that contribute to such environments are subject to robust data protection and other privacy regulations and standards. That includes public settings, such as streets, schools, libraries, sports and entertainment venues and business premises, including shops and cinemas, and the home.

75. Any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge or, in the case of very young children, that of their parent or caregiver; nor should it take place without the right to object to such surveillance, in commercial settings and educational and care settings, and consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose.

76. The digital environment presents particular problems for parents and caregivers in respecting children's right to privacy. Technologies that monitor online activities for safety purposes, such as tracking devices and services, if not implemented carefully, may prevent a child from accessing a helpline or searching for sensitive information. States parties should advise children, parents and caregivers and the public on the importance of the child's right to privacy and on how their own practices may threaten that right. They should also be advised about the practices through which they can respect and protect children's privacy in relation to the digital environment, while keeping them safe. Parents' and caregivers' monitoring of a child's digital activity should be proportionate and in accordance with the child's evolving capacities.

77. Many children use online avatars or pseudonyms that protect their identity, and such practices can be important in protecting children's privacy. States parties should require an approach integrating safety-by-design and privacy-by-design to anonymity, while ensuring that anonymous practices are not routinely used to hide harmful or illegal behaviour, such as cyberaggression, hate speech or sexual exploitation and abuse. Protecting a child's privacy in the digital environment may be vital in circumstances where parents or caregivers themselves pose a threat to the child's safety or where they are in conflict over the child's care. Such cases may require further intervention, as well as family counselling or other services, to safeguard the child's right to privacy.

78. Providers of preventive or counselling services to children in the digital environment should be exempt from any requirement for a child user to obtain parental consent in order to access such services.38 Such services should be held to high standards of privacy and child protection.

Appendix B: Questions addressed by RTE to Human Rights lawyers

Project Title: Legal research on national legal frameworks, particularly data protection laws, protecting learners and/or children from the risks of technology in education

Q1 – Is there a data protection law?

If so, please provide the name of the law and its year of adoption, with the text if available.

Please also provide information about the regulatory authority tasked with implementation and enforcement of this law.[188]

Q2 – Where it exists, does this data protection law provide specific protections for children? What protections does it provide?

If so, please provide details and/or the name of the law and its year of adoption, with the text if available.

Are there any case laws that have implemented these protections?

Q3 – Are there other laws, for example, Education Acts or otherwise, that include provisions on data protection for learners and/or children?

If so, please quote the relevant provision(s) and provide the name of the law and its year of adoption, with the text if available.

Q4 - if you responded no to the previous question, are you aware of any proposed legislation or related policy relevant to children's data protection, including in education?

Within the relevant legislation identified in Q1-3:

[188] There's a number of countries that have an obscure 'cybersecurity' law (not a data protection one) that was delegated to an equally obscure body who has never implemented it; there are also new data protection laws emerging but no regulatory body to enforce it, for example.

Q5 – Are there specific provisions protecting against cyberbullying and online abuse?

If so, please quote the relevant provision(s) and laws.

Q6 – Are there specific provisions preventing the collection and processing of children's data by technology companies and governments for the purpose of profiling, behavioural advertising, or other uses unrelated to the purpose of providing education, including uses unnecessary, disproportionate, or unlawful to a child's best interest as defined by the UN Conventions on the Rights to the Child.

If so, please quote the relevant provision(s) and laws.

Q7 – Are there specific provisions ensuring that companies respect children's rights and are held accountable if they fail to do so?

Particularly, are there provisions requiring technologies companies:

- to process children's data only for necessary, proportionate, and lawful purposes that are in the best interest of the child?
- to obtain meaningful consent by children and their caregivers?
- to provide the highest level of privacy by design and by default to services that are directed towards, and likely to be accessed by, children?
- conduct and publish human rights and/or child rights due diligence processes?
- Provide full transparency in data supply chains, and publicly report on how children's data are collected and processed, where they are sent, to whom and for what purpose?
- Provide child-friendly, age-appropriate processes for remedy and redress for children who have experienced infringements on their rights?

If so, please quote the relevant provision(s) and laws.

Q8 - what mechanisms does the law provide the government to be able to monitor and hold actors to account, whether they are companies or government entities?

Q9 – Is there any court decision or ombudsman decision relevant to learners' and/or children's data protection?

If so, please reference the case, and provide a short summary of the decision and implementation (if known) and provide the text if available.