Regulatory initiatives on school children's data protection in Latin America

Revista Latinoamericana de Economía y Sociedad Digital

Issue 3, agosto 2022

Autores: Alexandra Contreras

DOI: 10.53857/RAKT3016

Publicado: 31 agosto, 2022

Recibido: 30 abril, 2022

Cita sugerida: Contreras, A. (2022). Regulatory initiatives on school children's data protection in Latin America. Revista Latinoamericana de Economía Y Sociedad Digital, 3. https://doi.org/10.53857/RAKT3016

Licencia: Creative Commons Atribución-NoComercial 4.0 Internacional (CC BY-NC 4.0)

Tipo: Estado del arte

Palabras clave: children, Data Protection, privacy, regulation

Resumen

El acceso gratuito e ilimitado a Internet y los dispositivos móviles aumentan las oportunidades de digitalización y conectividad, pero también los riesgos para los menores. La privacidad y la protección de datos son de suma importancia y deben ser abordados con urgencia por los legisladores y los gobiernos, los padres, las empresas y la sociedad, centrándose especialmente en el entorno educativo. Siguiendo la Convención de las Naciones Unidas sobre los Derechos del Niño (CDN), los niños son reconocidos como sujetos de derechos y como objetos de protección especial y el mal uso de los datos de los niños viola esos derechos. Este documento pretende crear conciencia sobre la importancia de la protección de datos de los niños y, en segundo lugar, alentar a los actores públicos y privados de la sociedad a establecer los derechos de los niños dentro de las regulaciones existentes y futuras. Para lograr estos objetivos, identificamos problemas clave de vulnerabilidad relacionados con los datos de niños y adolescentes que están relacionados con su comprensión de los riesgos, su edad y antecedentes. Además, presentamos una descripción general de los riesgos actuales en la protección de datos personales que se basa en las normas y directrices internacionales vigentes y detallamos cómo los reguladores en

América Latina están abordando estos problemas y riesgos, comparando las políticas nacionales y la legislación en la región. El artículo también describe algunos marcos regulatorios alrededor del mundo que pueden servir como guía a nivel regional y, finalmente, brindamos un resumen del kit de herramientas de protección de datos para escuelas que se ha implementado en el Reino Unido.

Abstract

Free and unlimited access to the Internet and mobile devices are increasing the opportunities for digitalisation and connectivity but also the risks for minors. Privacy and data protection are of utmost importance and need to be urgently addressed by policymakers and governments, parents, companies, and society, focusing especially on the educative setting. Following the UN Convention on the Rights of the Child (CRC), children are recognised as subjects of rights and as objects of special protection and misuse of children’s data violates those rights. This document intends to raise awareness of the importance of children’s data protection and second, to encourage public and private actors in the society to establish children’s rights within existing and future regulations. To accomplish these goals, we identify key vulnerability problems related to children’s and teenagers’ data which are related to their understanding of the risks, their age and background. In addition, we present an overview of the current risks in the protection of personal data which is based on current international regulations and guidelines and detail how regulators in Latin America are addressing these problems and risks, comparing national policies and legislation in the region. The article also describes some regulatory frameworks around the world that can serve as a guide at the regional level and finally, we provide a summary of the data protection toolkit for schools that has been implemented in the United Kingdom.

Resumo

O acesso gratuito e ilimitado à Internet e aos dispositivos móveis aumenta as oportunidades de digitalização e conectividade, mas também os riscos para os menores. A privacidade e a proteção de dados são de suma importância e precisam ser abordadas com urgência por legisladores e governos, pais, empresas e sociedade, com foco particular no ambiente educacional. De acordo com a Convenção das Nações Unidas sobre os Direitos da Criança (CDC), as crianças são reconhecidas como sujeitos de direitos e objetos de proteção especial e o uso indevido dos dados das crianças viola esses direitos. Este documento visa aumentar a conscientização sobre a importância da proteção de dados das crianças e, em segundo lugar, incentivar os atores públicos e privados da sociedade a estabelecer os direitos das crianças dentro das regulamentações existentes e futuras. Para atingir esses objetivos, identificamos os principais problemas de vulnerabilidade relacionados a dados de crianças e

adolescentes relacionados à sua compreensão dos riscos, sua idade e antecedentes. Além disso, apresentamos uma visão geral dos riscos atuais na proteção de dados pessoais com base nos padrões e diretrizes internacionais atuais e detalhamos como os reguladores da América Latina estão abordando esses problemas e riscos, comparando as políticas e legislações nacionais da região. O artigo também descreve algumas estruturas regulatórias em todo o mundo que podem servir como guia em nível regional e, finalmente, fornecemos uma visão geral do kit de ferramentas de proteção de dados para escolas que foi implementado no Reino Unido.

1. Introduction

Children of today are born digital-by-default. Even before birth, they may have a digital profile generated by their parents, a health record, and they may have attracted the interest of commercial actors (Valcke, Bonte, de Wever, and Rots; 2010). Unicef (2017) has estimated that one in three of all Internet users is below the age of 18[1], therefore contemporary children are called "digital natives" (Prensky, 2001) or "Millenials" (Howe and Strauss, 2000). A large extent of what children -or their parents- do is digitally recorded, shaping that profile, and potentially impacting their life opportunities. On the other hand, the development of technology has made possible an increasing interaction of kids and teenagers with digital devices which are also gathering information from children. The COVID-19 outbreak evidenced, on the one hand, the importance of connectivity and digitalization as key enablers of remote work, education, healthcare as well as entertainment. Most governments around the globe are working to foster network deployment, connectivity, and digital inclusion. Several initiatives have been put in place to allocate public and private resources to promote digital learning, especially for children. However, increasing connectivity is not the ultimate goal. Once internet access is guaranteed, the priority for parents, policymakers, and education systems is keeping children safe from digital risks, including cyberbullying and privacy violations. Developing robust and clear policies, providing teachers and parents with the support they need to protect children and enforcing the legal frameworks established at a national level is of utmost importance.

The responsible use of children's data plays a key role in promoting children's well-being especially when it comes to the management of children's personal data within the education system. Violation of information privacy can occur with the collection, storage or processing of minors' personal data, especially if this occurs without their consent (UNICEF, 2018; Stoilova et.al., 2020).

To understand the problem and risks associated to minor's data misuse in education, one must consider that schools need to gather information about their students, those attending classes in person and remotely. This data collected by schools -though is not usually processed (Stoilova, et. al, 2020), is usually sent to other public institutions such as the ministries of education. Besides, children provide their data to several businesses related

with their education (i.e. educative items stores or education resources' webpages or applications). The amount of data that is provided by children's parents in the education setting is enormous and concerns about children's data are growing. Parents worry about who has access to data about their children and for which purposes such data may be used. There is a widespread and accurate sense that a greater amount of personal information is being assembled in databases (so called "big data") and might be being sold to third actors without data owners' permission especially for marketing efforts (Desimpelaere et.al., 2021).

Attempts to recognise children's right to privacy and data protection are relatively new and most of the work is being done at regulatory level. Although policies and specific laws with child-specific provisions are being established in developed countries, developing countries such as the Latin American ones, are under construction. Policies are still in the stage of diagnosis, proposed or ongoing which leaves children still unprotected. This lack of clarity in regulation relates, for instance, to the age of consent for processing children's data, the technical requirements regarding parental consent, the interpretation of the extent to which profiling of children is allowed and the level of transparency which that may significantly affect children and their rights. In addition, regulatory frameworks in the region do not consider specific rules for the management of minor's data by education institutions.

The economics and technologies underlying use of children personal information are fundamentally changing. These changes, in turn, arise the need to change the institutional arrangements governing use of personal information.

In this context, this essay has three main objectives. First, raise awareness about the importance of minor's data protection and potential risks especially related to the educational environment. Second, to analyze to which extend regulatory frameworks in Latin America are considering and guaranteeing children's data protection and privacy and finally, to motivate public and private actors in the society to ensure children's data protection are expressly considered within existing and future data regulation.

To accomplish these goals, along with this document we will a) identify key vulnerability problems related to children's and teenagers' data and present an overview of the risks in the protection of personal data in the education system, b) detail how regulators in Latin America are addressing these problems and risks, comparing national policies and legislation in the region and c) summarising some of the challenges to be faced by the different social actors to ensure minor's data are protected. By way of conclusion, the article describes some best practices from European countries that can serve as a guide at the regional level.

This research project follows a qualitative approach, where we intend to analyse existing literature, build a benchmark with information related to the status of regulation and provide the reader with suggestions on possible approaches to undertake data protection regulation in the education sector.

This document has five sections: 1, the introduction where we define the main objectives of the essay, and the research approach; section 2, the conceptual and theoretical framework where we explain the importance of data protection and why it is necessary to propose specific regulation focused on children and teenagers; section 3, details the content of the regulations in several countries of Latin America; section 4, depicts some examples of regulation and toolkits set in countries outside our region and finally, section 5 presents some conclusions.

2. Why a specific children's data protection regime?

To lay the groundwork for this essay's approach to children's data protection regulation, it is necessary to identify why protecting minor's data is important, which are the risks and problems related to their privacy, as well as which are the key issues when it comes to regulate minor's data protection.

Whilst the CRC, adopted 30 years ago, is not a legally binding instrument, it recognises the responsibilities of public and private actors to respect children's rights. However, a lot has happened since that time and now and it has become imperative to raise awareness on children's data protection as part of their rights to be ensured safety and well-being.

On the one hand, the fast advancement of technology, the availability of new programs, applications and handsets and the endless possibilities of human interaction in the digital environment have fostered the use of the internet worldwide. On the other hand, changes in society, parenting and education systems throughout time have resulted in children and adolescents using mobile devices and the Internet at an earlier age than in former generations. As a result, technologies have transformed children's lives into data that is recorded, tracked, aggregated, analysed and monetised (Stoilova, et. al, 2020). The amount of information that children and their parents disclose to different actors has increased exponentially (Desimpelaere et.al., 2021).

Stoilova, et. al, 2020, building on the work of van der Hof (2016), distinguish three types of data in the digital environment: data given (knowingly contributed by individuals about themselves or others); data traces (left, mostly unintentionally through online activities and captured via data-tracking technologies); and inferred data (resulting from analysing data given and data traces, known as 'profiling'). Regarding children, the data meaningfully given are usually those provided to public institutions (i.e. school or medical records). However, in commercial contexts, children's data is mostly inferred, aggregated, and used to generate pro-files in order to target advertising or for other profitable purposes (Stoilova, Nandagiri, & Livingstone, 2019).

A specific children's data governance process is required because of the presumption that children cannot effectively advance and advocate on behalf of their interests given their age and capacity to discern their needs and rights. The UK General Data Protection Regulation (GDPR) states that children require *"specific protection regarding their data as they may be*

less aware of the risks, consequences and safeguards concerned and their rights about the processing of personal data".

2.1 Risks and problems related to children data privacy

In the report *Case for better governance of children's data: a manifesto* (2021), the UNICEF emphasises the short- and long-term risks related to youth data:

– Surveillance by corporations and governments threatens children's freedom and privacy, not only in their present but also in their future;
– Poor protection of children's sensitive data due to a lack of clear regulation, standards, and limits on children's data management, including its commercialisation;
– Predictive analytics could increase existing discrimination;
– Manipulation and influence of children's behaviour by using their data (i.e. microtargeting strategies deployed via social media platforms);
– Lack of exploration and adequate regulation on management of aggregated, non-personal children data;
– A paucity of information on verification, encryption and use of parental controls and no education on how these tools must be considered in connection with children's wishes, capacities and freedoms;
– Data governance does not account for children's evolving capacities and varied experiences or capabilities;
– Most data regimes do not adequately address consent, child protection and representation.

2.2 Fundamentals in children data protection regulation

Policies and rules in place around the world and existing literature point out several issues to be considered to establish a modern, flexible, and adequate regulatory framework that protects minor's data.

2.2.1 Best interests of the child

Although there is no standard definition of "best interests of the child," the term generally refers to the deliberation that courts undertake when deciding what type of services, actions, and orders will best serve a child as well as who is best suited to take care of a child. Article 3 of the United Nations CRC highlights *"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.*"

Therefore, when applied to data protection regulation, governments, business and other actors, including education systems, must consider the rights and freedoms of the child so that they can learn, develop, and explore, in their homes and schools and particularly, in an online context.

2.2.2 Consent

Consent is one of the lawful basis for processing a child's personal data. Article 4(11) of the UK GDPR defines consent as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*". This means people -including children or their parents or legal guardians- must be able to refuse consent without detriment and must be able to withdraw consent easily and costless at any time. It also means consent should be unbundled from other terms and conditions wherever possible.

Another key issue is whether parental consent is an adequate mechanism to protect children (Krivokapic and Adamovic, 2016; Van der Hof, 2017) and at which age children are allowed or prepared to give their consent to collect, process and/or use their data. Where the child is not competent then, in data protection terms, their consent is not "informed" and it therefore isn't valid. The Information Commissioners Office of the UK, set some guidelines based on regulation and points out that if someone wishes to "*rely upon consent, the consent of a person with parental authority over that child is required, unless it is evident that it would be against the best interests of the child to seek such parental consent*".Schermer et al, 2014 conclude that consent is completely ineffective in practice due to consent and information overload, complexity of data processing, and lack of actual choice. However, consent is still

It is also important to notice that children's awareness of their privacy is relevant. Young and children generally know they are entitled to their privacy online from their parents or peers however, they usually ignore how their privacy could also be infringed by any state or company (Livingstone, 2018, Desimpelaere et.al., 2021). Children's own definition of privacy could differ from the one adults have. Livingstone (2019) points out that "w*hile children, like anyone else, are influenced by social as well as digital environments, their privacy perceptions and practices might be different from how adults (parents, educators, policymakers) envision them or wish them to be*". In addition, depending on the social network, teenagers can consider they have different levels of privacy and disclose more -or- less information according to it. The author also emphasises the fact that understanding of privacy evolves with age and therefore the self-disclosure choices may vary. Even though children might have "control" over what they share online, they have zero control over what other people share about them or how their data is processed or managed.

2.3 Data protection in schools

When digital technologies are used for educational purposes, a variety of actors intervene in the processing of children and adolescents' data, including national governments, policymakers, public and private schools (staff and teachers), companies, providers of products or services, software developers and legal guardians, parents, and peers. All stakeholders in the education system should ensure children can access mechanisms for

enforcing their rights including data protection and privacy in the digital environment.

In relation to the education context, schools hold a large amount of minors' personal information— collected or provided by students and parents. Education records contain information on student background, photographs, attendance records, fingerprints, addresses, academic performance, grades, standardised test results, health information, psychological evaluations, disability reports, and anecdotal remarks from teachers or school authorities regarding academic performance or student's behaviour (FERPA, 1974, 20 U.S.C §1232g). This was rarely a cause for concern, since schools' and -in general- institutional data collection is necessary to ensure children's health, safety, learning or well-being, provided data use is limited to the original purpose: monitoring, supervision and surveillane (Stoilova et.al., 2020), however, increasing attention is driven to the management of these data and concerns are raised.

Based on that trust from minors and parents, the protection of that data on the school's side should be established as a requirement. The establishment of good practices can be useful and they should involve consultation with legal guardians and children -according to their capacity and keeping in mind the best interest of the child- about decisions to adopt new technology which might result in the processing of children's data.

In this sense, it is vital that public institutions (different authorities usually cooperate and share information), are mandated to apply a principle of data minimisation and comply with restrictions on storage and retention. In addition, governments must enforce regulation and monitor any breach of children's rights by companies within the education setting and digital environment. It is essential to acknowledge that it is not only the child's right to data protection that is affected when it comes to education and digital technologies but also that the right to privacy and data protection are enabling rights for the protection of further rights of the child.

Literature review

Children data privacy and protection regulatory regimes in education settings are of relatively recent concern, at academic level most researchers have focused on analysing the general implications of the contemporary digital environment in children's online safety.

Van der Hof and Lievens, 2017 propose that other data protection instruments, i.e. privacy by design and data protection impact assessments are better tools of protection and empowerment in the European GDPR in order to safeguard children's data. They analyse the law and claim that data protection seems illusory given the complexities of the digital world, which is largely dominated by commercial interests. These principles require that controllers implement data protection principles into the design of their data processing systems.

Stoilova et. al., 2020, conducted focus group interviews with 169 UK children aged 11–16 to explore their understanding of privacy in interpersonal, institutional, and commercial

contexts. They found that children primarily conceptualise privacy as something they control over as regards deciding when and with whom to share information with. This leads them to trust how personal data is collected, inferred and used by organisations, be these public institutions such as their schools or commercial businesses. The authors conclude that, since the complexity of the digital environment challenges teachers' capacity to address children's knowledge gaps, businesses, educators, parents and the state must exercise a shared responsibility to create a legible, transparent and privacy-respecting digital environment in which children can exercise genuine choice and agency.

Regarding the use of smart devices by children (which includes tablets which could be used for studying), Rafferty et al.(2017) consider that children do not understand the concept of privacy and the children do not know how to protect themselves online, especially in a social media and cloud environment. They also highlight that children may disclose private information to smart toys and not be aware of the possible consequences and liabilities.

Just a few studies focus on institutional or commercial privacy which concern (children's) data processing practices by governmental institutions and commercial organisations. A qualitative study by Desimpelaere, Hudders and Van de Sompel (2020) where the authors conducted in-depth interviews with ten parents and nine children (8-11 years), found that although children engaged in avoidance (e.g., leaving the website) and confrontation (e.g., seeking support) strategies, they mainly did this to protect their privacy from malicious individuals and not from commercial parties. The academics show a void in the responsibilities parents legally have over their children's online privacy and their actual skills regarding this topic. While parents expressed privacy concerns (mostly about their children), they do not sufficiently know how to protect their own or their kids' online privacy and find it too burdensome.

Livinstong et.al., (2019) emphasise that one raising concern amongst parents and public in general is that institutional administrative data (i.e. children education records), which are "*collected in circumstances in which one would expect confidentiality*" can be "*shared across intra- and inter- governmental, public and commercial institutions, for purposes described as for 'public benefit', such as fraud prevention, health and welfare or education*". They conduct empirical research of several studies with children, including both primary and secondary data analysis studies and perform a cross-analysis of child development and types of privacy and define resulting.

Bowyer et. al., 2018, using the "Family Design Games" applied a qualitative understanding of families' requirements for the handling of their data. Writers concluded that organisations must support a dynamic consent model of data handling, and plan for a new paradigm of co-operative, data-based relationships with families, one where meaningful, representative data is nurtured for mutual benefit and families remain involved throughout.

Sabourin, J., et. al, (2020), analyse student's reports data mining in education. Education data mining (EDM) offers to improve student learning and education systems, however,

these systems are often driven by the collection of large amounts of student data, which is a growing concern to many. Shifts in public opinion and policy have led to barriers to the adoption of EDM technologies in commercial applications. They conclude that trust, fear, and misunderstanding are inherent to technology and modern systems used in education. Companies and experts in the field must work hard to both gain the trust of the public and communicate what is being done with student data to gain trust.

Lievens and Verdoodt (2018), explore several key issues present in the European GDPR, for instance, the age of consent for processing children's data in relation to information society services, the technical requirements regarding parental consent in that regard, the interpretation of the extent to which profiling of children is allowed and the level of transparency that is required vis-à-vis children. The authors question whether those aspects are accurately defined and specified in the regulatory framework or are sources of uncertainty when it comes to guaranteeing children's rights.

3. Children's data protection regulation and best practices in other countries

To provide a complete overview of the need of a strong regulatory framework to protect children and teenagers' data and privacy, this research summarises three of the most relevant regulatory initiatives around the globe: the American, British, and European.

It is indeed of superlative importance to observe and analyse the measures that other countries have taken to protect children from the risks previously analysed. This would be valuable for policymakers in Latin America to propose a novel, flexible and more holistic regulatory framework. The basic idea is that enforcement of mandatory legal rules would deter people from abusing minor's privacy and misuse of their data.

3.1 The United States: FERPA and COPPA

In the U.S., the government has established privacy protections for children by asking for consent from parents or guardians and implementing policies which hold private and public organisations, accountable for obtaining consent when collecting, storing or disclosing data, and ensuring proper usage. Two federal acts address children's privacy directly: the Federal Education Rights and Privacy Act (FERPA), and the Children's Online Privacy Protection Act (COPPA).

FERPA regulates among other issues, minor's data protection in the education system. It states that schools that want to disclose information contained in students records must have written permission from a parent or eligible student, an individual who is 18 or attending post-secondary school. Education record information is only shared with a third party on the assurance that that third party will not allow further outside access to requested information without additional written parental consent (FERPA, 1974, 20 U.S.C § 1232g (b)(4)(B)).

While FERPA affects private interests, the Children's Online Privacy Protection Act

(COPPA), a US federal law adopted in 1998, is focussed in online service providers that have direct or actual knowledge of minors and collect information online. COPPA defines 'a child' as a person under 13 years of age and also defines 'personal information as individually identifiable information about a person collected online.

Interestingly, the definition of personal information includes the screen or username, a persistent identifier that can be used to recognise a user over time and across different websites or online services, a photograph, video, or an audio file if this file contains a child's image or voice (Federal Trade Commission, 2015).

COPPA regulation mandates operators of websites or online services "*directed to*" children (also applicable to operators of other online services that have "*actual knowledge*" that they are collecting personal information online from a child) to notify that they are collecting children's personal information, and to collect "verifiable" parental consent. The Federal Trade Commission (FTC), is the federal body which oversees the implementation of COPPA and must ensure verification methods are used (Federal Trade Commission, 2015).

This requirement impacted the development of terms and conditions of several digital companies such as Facebook, Google, Instagram, Snapchat, Twitter and other companies. That is the reason why many online services set 13 years as the minimum age for creating an account or profile.

Under COPPA, parents must have access to their child's personal information to review and have the information deleted and they can prevent the further use or online collection of a child's personal information.

3.2 Europe: the General Data Protection Regulation, the newest regulatory approach

The GDPR, which entered in force in 2018, explicitly recognises that children deserve specific protection of their data and introduces additional rights and safeguards for children. Children's rights under the European GDPR include to:

– correct their data;
– withdraw consent to the processing of personal data;
– obtain a copy of the personal data;
– have their data deleted;
– transfer their data to another controller;
– restrict the personal data processed;
– request processing of their data is stopped.

Differing to the US, the GDPR has set the age of consent at 16, meaning users 15 years and younger need parent consent where applicable. However, member states can choose a younger age down to 13. Data processors need to prove that consent is valid, that it is informed and that they have methods in place to allow parents to exercise their children's

(could be through the use of platforms for parents to allow for the management of consent and revocation).

3.3 The UK: A holistic approach and special interest in children's data protection in education

UK GDPR was born with the European GDPR, however, British are pioneers in regulating children's data protection and privacy in the United Kingdom.

One of the UK's pillars in data protection is "transparency" as a mean to raise children's and their parents' awareness of data protection risks, consequences, safeguards, and rights.

Transparency is considered as "telling users what it is being done with their data, being open about the risks and safeguards involved and letting them know the actions to be taken if they are unhappy with their data management". This approach is intended to also help individuals make informed decisions about what personal data they wish to share.

Regarding children in the education setting, in April 2018, the UK government published the Guidelines to support schools with data protection activity, including compliance with the GDPR. The guidance was developed by the Department for Education (DfE) working in collaboration with schools, multi-academy trusts (MATs), local authorities, system suppliers, GDPR support providers, the National Cyber Security Centre and the Information Commissioners Office (ICO). This instrument intends to "*help schools develop policies and processes for data management, from collecting and handling the data through to the ability to respond quickly and appropriately to data breaches*".

The document provides nine steps to guide schools to develop the culture, processes and documentation required to be compliant with the legislation in force and effectively manage the risks associated with data management. It also includes case studies, top tips, and examples as well as a list of activities and resources to identify and monitor the use of personal data.

The nine steps are:

1. Raising awareness: demystify data protection across all staff within the school who deal with personal data. Personal data can relate to students, staff, parents and potentially others.

2. Creating a high-level data map: Recognise and create a "data ecosystem" o "map", and build up an overview of all the places personal data are stored and used in the school.

3. Turn your data map into a data asset register: Create the main framework to document the detail associated with each dataset and identify the areas of weakness/risk for a risk-management based approach.

4. Documenting the reasons for processing data: Here schools might ask do we need to

collect/ process this data? 'what am I allowed to process?'

5. Documenting how long you need to retain information: Schools can create a workable data retention policy to consult with those who best understand the uses of school data. Data retention is based on justification, if schools can justify the need to hold the information, they can do it.

6. Reassurance and risks: Identify risks that emerge from the school data asset register and assess what can be done to eliminate or reduce areas of medium/high risk and set action plans to do so.

7. Decide on your Data Protection Officer role: Understand the role of the Data Protection Officer (DPO), and specify that as a data controller, each school must designate a named DPO to comply with legislation

8. Communicate with data subjects: Remember all the key subject's rights, among which is the right to be informed. Create channels and design methods to communicate how the school is managing personal data.

9. Operationalise data protection and keep it living: Schools should identify the range of policies required to cover the procedures and processes for data protection. Understand what a data breach is, and what can be done to ensure that data protection and risk management is a core and regular part of decision-making and risk management practices within the school.

3.4 Children's data protection regulation in Latin America

The aim of this study is to examine if Latin American countries are aware of the importance of children's data protection and whether they are taking steps towards guaranteeing and surveilling this privacy and protection, not only in general but with a special focus on the education system. Therefore, besides the literature analysis and the enlisting of current regulatory frameworks in force, this paper contributes to the existing literature by charting a benchmark on the current state of children's data protection regulation in seven countries of Latin America: Argentina, Brazil, Chile, Colombia, Ecuador, Peru, and Mexico. Here we expose the existence or not of a specific regulatory framework focused on the protection of minors' data and their privacy. In addition, it also answers -at a national level- two important questions: are there any initiatives on children's data protection? And, are there any initiatives or guidelines for children's data protection related specifically to education?

The answers to those questions might provide an idea of the strength of national minor's privacy reality within the education environment and shed a light on the need for explicit and detailed guidelines or rules to help schools to make a more efficient, conscious and protective management of data provided by their students.

Analysis of data protection regulation framework by country

Argentina

General data protection framework

The right to the protection of personal data is established in the Argentine National Constitution (section 43). The current legal framework for the Argentine data protection regulation is made up of the Constitution and the:

– Personal Data Protection Law 25,326/2000

– Regulatory Decree 1558/2001

– Provisions issued by the National Directorate for Personal Data Protection (for example, Provision NDPDP 4/2009).

In 2019, the Argentinian data protection agency, AAIP, issued several rules and guidelines on data protection and international data transfers. These guidelines are in line with the EU General Data Protection Regulation (GDPR). The AAIP also approved an inspection guide on personal data in the Resol-2020-332-APN-AAIP.

Territorial scope of privacy rules

Data protection law applies to all data processing carried out in the country.

Are children's data protection rights explicitly mentioned in the law?

No, however, the new guidelines published in 2019, include specific criteria for obtaining minors' consent. A minor may give informed consent, considering their psychophysical characteristics, aptitudes, and stage of development. Otherwise, parents or legal guardians must consent. The data controller must validate their identity and authorise them to give their consent.

In addition, the AAIP published some recommendations regarding online safety for children[2] and emphasised that the Data Protection Law does recognise children as data owners and guarantees their rights.

Are there any initiatives on children's data protection?

Unknown, no information publicly available.

Are there any initiatives or guidelines for children's data protection related specifically to education?

Unknown, no information publicly available. However, in 2018 the Argentinian government implemented the program "National School ID", which under the purview of the Ministry of Education aims to guarantee the educational inclusion of children and adolescents of school age and prevent school dropout. The program consists of a digital system that allows the performance of students to be monitored, from the time they enter the educational system

until they graduate upon completing their secondary studies. Though the monitoring and prevention of school dropouts are important, this system contains a large amount of sensitive data which must be carefully processed and managed.

The National School ID system must comply with the Data Protection Law in force in the country.

Who is responsible for regulating and/or enforcing the law?

The National Directorate for Personal Data Protection is the governmental agency, within the Ministry of Justice and Human Rights responsible for regulating the processing of personal data in Argentina.

The Agency of Access to Public Information (AAIP) within the President's Chief of Staff's Office (Decree 746/17) is in charge of the enforcement of the law.

Sanctions for non-compliance with data protection laws?

Section 31 of the Personal Data Protection Law 25,326 provides sanctions for any violations of the Argentine data protection regulations which may include: warnings, suspensions, fines ranging from AR$1,000 to AR$100,000 and closure or cancellation of the file, register or database, without prejudice to any applicable civil or criminal liabilities.

Brazil

General data protection framework

The right to protect personal data is established in the Brazilian Constitution. Amendment 115, published in February 2022, made the right to data protection a constitutional right.

Furthermore, the current legal framework for the Brazilian data protection regulations is made up of:

– Law 13709/2018 on the protection of privacy and personal data (LGPD), signed into law on 14 Aug. 2018 as amended by Law 13853 of 8 July 2019

– Internet law 12965, 2014, implemented by Decree 8771/2016

Territorial scope of privacy rules

Data protection law applies to all data processing carried out in the country.

Are children's data protection rights explicitly mentioned in the law?

Yes, according to article 14 of LGPD, the processing of personal data of children and adolescents must be carried out in their best interest.

Also, to process children's personal data, the law requires the collection of specific and explicit consent provided by at least one of the parents or legal guardians. An exception

could be applied when such collection is necessary to contact the parents or the legal guardian, used a single time and without storage, or for the child's protection, and where this cannot be transferred to third parties under any circumstance.

Data requested to access online games and internet applications must be strictly necessary for the enjoyment of these applications. Information related to the processing of data must be given in a clear, simple, and accessible way, with the use of audio-visual means when appropriate, to provide necessary and adequate information to both, parents and children. No minimum age at which children can consent to the use of their data is stipulated.

Are there any initiatives on children's data protection?

The Proteja Brasil app has been developed for tablets and smartphones to facilitate the identification and notification of child rights violations.

Are there any initiatives or guidelines on children's data protection explicitly related to education?

Unknown

Specific statistics available show how many children at different levels of education access the internet through a variety of devices.

Who is responsible for regulating and/or enforcing the law?

The National Authority of Data Protection (ANPD) oversees the enforcement of the Law. This is a body of federal public administration, a member of the Presidency of Brazil.

Sanctions for non-compliance with data protection laws?

Penalties for privacy infringements applicable from 1 Aug. 2021 (art. 65, I-A of Law 13709/2018) range up to 2% of the company's revenues in the country (after deduction of taxes), capped at BRL 50m (US$8.96m) per infringement.

Chile

General data protection framework

A right to the protection of personal data is established in Art. 19(4) of the Chilean Constitution. Moreover, the current legal framework for the Chilean data protection regulations is made up of:

– Law 19628/1999, on the Protection of Private and Personal Data

– Law 20575/2012 on the Treatment of Personal Data

An update of the current legal framework is also foreseen alongside the country's national cybersecurity policy at an undefined time.

Territorial scope of privacy rules

Data protection law applies to all data processing carried out within the country.

Are children's data protection rights explicitly mentioned in the law?

Yes, but only specifically on consent. Consent must be given or authorized by the holder of parental responsibility for the child.

The law does not regulate the processing of minors' data. Nevertheless, regarding the bill, adolescents (defined as minors over 14 years of age though not yet 18 years old) may validly provide their consent in their own personal capacity, except regarding sensitive data of adolescents under 16 years of age, which can only be processed with the consent of the parents or legal guardian, unless expressly authorised or mandated by law.

Children's data processing must be performed in their best interests and progressive autonomy.

Are there any initiatives on children's data protection?

Unknown

Are there any initiatives or guidelines on children's data protection related specifically to education?

Yes, according to article 7 of the data protection law, the data collected by schools cannot be disclosed and deserve protection (Ledezma J., 2019).

The Privacy Policy set by the Chilean Ministry of Education establishes guidelines for the protection and privacy of personal information that is collected, processed, and transmitted through the Ministry's web page (www.mineduc.cl), in compliance with Law No. 19,628 and the Data Protection Policy. The Ministry of Education must adopt the necessary technical and administrative measures to provide security to personal data records, preventing their adulteration, loss, unauthorized or fraudulent use or access, according to the requirements established by current regulations.

Users are entitled, among other rights, to:

– have access to the data related to them, the purpose of storage and the information of people or organizations to which their data has been transmitted;

– request the deletion or cancellation of the data provided when desired, if they are no longer necessary or relevant for the purpose for which they were collected or recorded.

Who is responsible for regulating and/or enforcing the law?

Courts since there is not any specific data protection authority. In September 2021, President Piñera announced the creation of a national data protection authority (bill under

debate).

Sanctions for non-compliance with data protection laws?

Failure to comply with data privacy laws may result in complaints, civil actions, class actions, or private rights of action.

Colombia

General data protection framework

A right to the protection of personal data is established in the Colombian Constitution[3]. Furthermore, the current legal framework of the Colombian data protection regulations is made up of:

– Law 1581/2012 on Personal Data Protection

– Decree 1337/2013, partial implementing rules of Law 1581/2012

– Decree 886/2014, partial implementing rules of Law 1581/2012 related to a national personal data database.

Territorial scope of privacy rules

Data Protection law applies to all data processing carried out within the country.

Are children's data protection rights explicitly mentioned in the law?

Yes. Children and teenagers (individuals under 18 years of age) are subject to special constitutional protection, and therefore the processing of their data must always respect their prevalent rights. Art. 7 of the Data Protection forbids the processing of personal data of minors unless it is data of a 'public nature. However, this does not mean that the processing of minors' data is prohibited since the ruling of the Colombian Constitutional Court (Decree 1377 of 2013) provides for certain exceptions allowing the data of minors to be processed where:

– the processing of data is necessary for the protection of the minor's fundamental rights

– respecting their fundamental rights is guaranteed.

Whenever it is possible, minors' opinions concerning the processing of their data must be considered.

Are there any initiatives on children's data protection?

Unknown

Are there any initiatives or guidelines on children's data protection explicitly related to education?

Although is not specific for children's data protection, the Personal Data Protection Policy[4] published by the Colombian Ministry of Education does mention children's data protection. It mentions it is the state and the educational entities' obligation to provide information and train children and adolescents' legal representatives on the possible risks that they may face in the improper treatment of their data.

Who is responsible for regulating and/or enforcing the law?

The Superintendence of Industry and Commerce (SIC) is considered to be the primary Colombian data protection authority. This is a governmental entity with many other functions, including those of consumer protection, anti-trust, and industrial property.

Sanctions for non-compliance with data protection laws?

Failure to comply with data privacy laws may result in fines of around COP 1.56bn (US$402,702) according to art. 23 of the Personal data protection law.

Ecuador

General data protection framework

The right to the protection of personal data is established in the Ecuadorian Constitution, 2008. Moreover, the current legal framework of the Ecuadorian data protection regulations is very recent and only consists of the Personal Data Protection Organic Law published in May 2021. The new law includes rules on how data subjects can protect, access and consent to the use of their data; this becomes applicable from May 2023, so companies have a period of two years to adjust their processes to comply with the new rules.

Territorial scope of privacy rules

Data protection law applies to all data processing carried out in the country.

Are children's data protection rights explicitly mentioned in the law?

Yes, minors' data are considered to be a special category.

Children under 15 years of age need a legal representative to consent to the processing of their data. Adolescents aged 15 or over may grant consent themselves as owners, provided the purposes for data processing are specified.

Article 21 of the law establishes the right of children not to be subject to a decision based solely or partially on automated assessments, or sensitive data; neither may children and adolescents' data be processed unless expressly authorised by the owner or their legal representative.

Are there any initiatives on children's data protection?

Yes, in 2020 the Ecuadorian government published the Public Policy on Internet Safety for

children and adolescents which established a set of action lines and specific objectives to safeguard the safety of children online.

Are there any initiatives or guidelines on children's data protection explicitly related to education?

No

The Ecuadorian General Education Law and the Law of Higher Education allow education centres to collect and process the personal data of their students, to in turn be sent to the Ministry of Education in the exercise of the educational function. However, there are no express provisions on the type of information that must be handled.

Who is responsible for regulating and/or enforcing the law?

The law created the Superintendency of Protection of Personal Data (SPPD), working as an autonomous institution. The data protection authority may act ex officio or at the request of the data owner.

Sanctions for non-compliance with data protection laws?

The data protection authority may impose corrective enforcement measures on processors and controllers for infringing the law (cessation orders, data deletion, technical, legal, or administrative measures to guarantee the data adequate processing). It may also impose fines up to a percentage of the companies' annual turnover in Ecuador for the previous year:

– minor infringements: 0.1% to 0.7%

– major infringements: 0.7% to 1%

Mexico

General data protection framework

A right to the protection of personal data is a fundamental right recognised by the Constitution of Mexico published in 2009. Furthermore, the current legal framework for the Mexican data protection regulations is made up of:

– Federal Law on Protection of Personal Data Held by Private Parties, 2010

– Regulation on the Federal Law on Protection of Personal Data Held by Private Parties, 2011

– General law for the protection of personal data in possession of government entities, 2017

– Guidelines on Privacy Notices, issued by the National Institute for Access to Information and Protection of Personal Data (INAI) in 2013

Territorial scope of privacy rules

The Federal law of 2010 for the protection of personal data in possession of private entities applies to any individual or entity having a legal domicile or local offices or branches in the country (art. 2).

Are children's data protection rights explicitly mentioned in the law?

They are not.

Are there any initiatives on children's data protection?

Unknown

Are there any initiatives or guidelines on children's data protection related specifically to education?

Unknown

Who is responsible for regulating and/or enforcing the law?

The Federal Information Access and Data Protection Institute (INAI) is in charge of enforcing the law, as well as any regulations and guidelines in Mexico.

Sanctions for non-compliance with data protection laws?

Failure to comply with data privacy laws can invoke fines of up to MXN 45.34m (US$2.19m) (i.e. a fine of up to 320,000 days of the minimum wage: MXN 172.87 (US$8.33), according to art. 64 of the 2010 law).

In the case of sensitive personal data, all applicable penalties are doubled (whether the penalty is a fine or a term of imprisonment). Assessment of the gravity of infringements is carried out by INAI by 2017 enforcement rules.

Peru

General data protection framework

The right to the protection of personal data is a fundamental right recognised by the Peruvian Constitution published in 2009. Moreover, the current legal framework for the Mexican data protection regulations is made up of:

– Law 29733 of 2011 on Personal Data Protection

– Implementing rules of the Personal Data Protection Law (Supreme Decree 003-2013-JUS), 2013

– Directive 01-2020-JUS on the processing of personal data through video surveillance systems, 2020

Territorial scope of privacy rules

Data Protection Law applies to all data processing activities carried out in the country (art. 3). However, the law does not apply to companies that are established in the country, but only process data outside the country.

Are children's data protection rights explicitly mentioned in the law?

Yes, only on consent. For minors aged between 14-18 years of age, personal data may be processed with their consent, when the information required to obtain this consent has been expressed in a language they can understand. If children are under 14 years, they need their legal representatives' consent is needed (parents or guardians).

Under no circumstances may the consent for the processing minor's data be granted to access activities related to goods or services that are strictly for adults.

Are there any initiatives on children's data protection?

Unknown

Are there any initiatives or guidelines on children's data protection related specifically to education?

Unknown

Who is responsible for regulating and/or enforcing the law?

The National Authority for the Protection of Personal Data (NAPPD) within the Ministry of Justice and the National Directorate of Justice (art. 32, Data Protection Law of 2011).

In June 2021, the Presidency of the Council of Ministers (PCM) approved a bill to create the National Authority for Transparency, Access to Public Information and Protection of Personal Data.

Sanctions for non-compliance with data protection laws?

Failure to comply with data privacy laws can include fines established in Peruvian Taxation Units (UIT). Very serious infringements are sanctioned with fines of up to 100 UIT (US$ 0.12m). Under no circumstances may the fine exceed 10% of the company's annual gross income according to art. 39 of the law.

Conclusions and recommendations

Children's data protection, in a world where free and unlimited access to the Internet has provided grounds for new problems and risks, is a mission to be urgently undertaken. Since the complexity of the digital environment challenges everyone; businesses, educators, parents and the government need to exercise a shared responsibility to create a legible, transparent and privacy-respecting regulatory framework in which children can exercise genuine choice and interests.

Some countries worldwide have been progressively implementing rules to protect and guarantee minor's from their data misuse, however in Latin America, regulation is still being proposed and implemented.

This document attempted to encompass a review of the current regulatory frameworks in Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, and Peru to raise awareness on how strong the national data protection regulations in the region are and hopefully call governments and policymakers to action.

All countries researched have privacy and/or data protection rules. Argentina's and Chile's data protection laws dates back to 2000 and 1999 respectively, however, two privacy bills were recently introduced at the Argentinian congress and an update of the Chilean law is foreseen in the coming years. Mexico, Peru, and Colombia adopted their personal data protection laws over the past ten years, between 2010, 2011 and 2012.

The most recent regulation is the Ecuadorian data protection law, approved in 2021 and the Brazilian one, published in 2018. As of February 2022, the Brazilian Constitution was amended to include personal data protection as a fundamental right.

Several proposals to amend national data protection frameworks are currently under debate in Chile and Colombia.

Unfortunately, even though some data-privacy related rules are in force and governments in the region are becoming increasingly aware of the need for a specific framework to protect children, most countries analysed have not set specific regulations nor guidelines or relevant initiatives regarding children's and adolescents' data protection, therefore there is still much work to be done.

From the analysis of best practices in the US, Europe and the UK, we learnt that "fundamentals" to privacy and data protection have to be ensured at national level by the law. The concept of "best interest of the child" must be considered and expressly urged when proposing the policies and rules. Besides, rules have to specify the definition of "child" and "consent" and how this consent must be accepted and understood as well as who is in charge of providing this "consent" (parents, legal guardians or children their selves when reaching certain age).

An interesting example is provided by UK in its "tool kit" for schools. In the document the ICO explains to teachers, and parents how to protect children from all the current threats in the digital environment and guides organisations and businesses -step by step- on how to comply with the UK GDPR.

Bibliography

Bowyer a., Montague K., Wheater S., Mcgovern R., Lingam, R., Balaam M., 2018, *Understanding the Family Perspective on the Storage, Sharing and Handling of Family Civic Data,* Conference paper, the 2018 CHI Conference, available at

https://doi.org/10.1145/3173574.3173710

Burns, T. and F. Gottschalk (eds.), *Education in the Digital Age: Healthy and Happy Children*, 2020, Educational Research and Innovation, OECD Publishing, Paris, available at https://doi.org/10.1787/1209166a-en.

Desimpelaere, L., Hudders, L., and Van de Sompel, D., 2020, *Children's and parents' perceptions of online commercial data practices : a qualitative study*, Media and Communication, 8(4), 163–174. https://doi.org/10.17645/mac.v8i4.3232

Information Commissioner's Office of the UK, *Children and the UK GDPR,* available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-do-we-need-to-consider-when-choosing-a-basis-for-processing-children-s-personal-data/#a2

Howe, N., & Strauss, W. (2000). Millennials rising: The next great generation /by Neil Howe and Bill Strauss ; cartoons by R.J. Matson. New York: Vintage Books, available at https://www.scirp.org/(S(oyulxb452alnt1aej1nfow45))/reference/ReferencesPapers.aspx?ReferenceID=1450357

Krivokapic D., and Adamovic J., 2016, *Impact of general data protection regulation on children's rights in digital environment*, Anali Pravnog fakulteta u Beogradu. 64. 205-220. 10.5937/AnaliPFB1603205K.

Ledezma J., *La protección de datos personales de menores en establecimientos escolares de educación pública bajo la legislación Chilena*, 2019, available at https://repositorio.uchile.cl/bitstream/handle/2250/146469/La-protección-de-datos-personales%20-de-menores-en-establecimientos-escolares-de-educación-pública-bajo-la%20legislación-chilena.pdf?sequence=1&isAllowed=y

Lievens E., Verdoodt V., 2018, *Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation*, Computer Law & Security Review, volume 34, issue 2, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2017.09.007.

Livingstone S, Mascheroni G, Staksrud E. European research on children's internet use: Assessing the past and anticipating the future. New Media & Society, 2018, available at doi:10.1177/1461444816685930

Livingstone, S. Stoilova, M. and Nandagiri, R., 2019, *Children's data and privacy online: Growing up in a digital age*. *An evidence review*. London, London School of Economics and Political Science, available at Link

Livingstone, S. Stoilova, M. and Nandagiri, R., 2019, *Children's data and privacy online: Growing up in a digital age. An evidence review*, London: London School of Economics and Political Science.

Organization of American States, Secretariat for Legal Affairs, Department of International Law, *Principios actualizados sobre la privacidad y la protección de datos personales*, 2022, available at Link

Proteja Brasil, Unicef, 2017, available at https://www.unicef.org/brazil/media/1286/file/Protect%20Brazil%20Report%202017.pdf

Prensky, M., 2001, Digital Natives, Digital Immigrants, Part 1. On The Horizon, 9, 3-6, http://dx.doi.org/10.1108/10748120110424816

Rafferty L., Hung P., Fantinato M., Peres S., Iqbal F., Kuo S., and Yeh W., 2017, *Towards a Privacy Rule Conceptual Model for Smart Toys*, 10.1007/978-3-319-62072-5_6.

Sabourin, J., Kosturko, L., Fitzgerald, C., and McQuiggan, S., 2020, *Student privacy and educational data mining: perspectives from industry*. 164–170, available at https://www.educationaldatamining.org/EDM2015/proceedings/full164-170.pdf

Simone, van der Hof and Lievens E., *The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR,* 2017, Communications Law 2018, Vol. 23, No. 1, available at SSRN: https://ssrn.com/abstract=3107660

Stoilova M., Livingstone S., and Nandagiri R., 2020, *Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy*, Media and Communication, https://doi.org/10.17645/mac.v8i4.3407

TIC Kids Online Brasil, 2017, available at https://cetic.br/tics/kidsonline/2017/criancas/A1/

UNICEF, *State of the World's Children*, 2017, available at https://www.unicef.org/media/48601/file

UNICEF, *Good Governance of Children's Data project Office of Global Insight and Policy*, 2020, available at https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf

UNICEF, *Case for better governance of children's data: a manifesto*, 2021, available at Link

Legislations

Argentina

Personal Data Protection Law 25,326/2000, available at http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

Regulatory Decree 1558/2001[1], available at http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/texact.htm

Provisions issued by the National Directorate for Personal Data Protection (for example, Provision NDPDP 4/2009)

Data protection guidelines, available at https://www.argentina.gob.ar/noticias/cuidar-la-privacidad-en-la-ninez

Brasil

Brazilian Constitution, 1988, available at https://www.constituteproject.org/constitution/Brazil_2017?lang=es

Amendment 115, 2022, available at https://www.in.gov.br/en/web/dou/-/emenda-constitucional-n-115-379516387

Law 13709/2018 on the protection of privacy and personal data, 2018, available at https://www.dataguidance.com/sites/default/files/lgpd_translation.pdf

Internet Law, LEI Nº 12.965, 2014, available at https://www2.camara.leg.br/legin/fed/lei/2014/lei-12965-23-abril-2014-778630-publicacaooriginal-143980-pl.html

Decree 8771-11-2016, 212016, available at https://www2.camara.leg.br/legin/fed/decret/2016/decreto-8771-11-maio-2016-783094-publicacaooriginal-150360-pe.html

Law 13709/2018, 2018, available at http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Chile

Chilean Constitution, 1980, available at https://www.camara.cl/camara/doc/leyes_normas/constitucion_politica.pdf

Law 19628, 2020, available at https://www.bcn.cl/leychile/navegar?idNorma=141599

Law 575, 2012, available at https://www.bcn.cl/leychile/navegar?idNorma=1037366

Bill on the data protection and treatment and the creation of a data protection agency, Camara de Diputados y Diputadas, 2017, available at https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=11661&prmBoletin=11144-07

Colombia

Colombian Constitution, 2015, Link

Ministry of Education, *Personal Data Protection Policy*, 2019, https://www.mineducacion.gov.co/1759/articles-353715_recurso_5.pdf

Data Protection Law, Law 1581, 2012, available at https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Decree 1337, 2013, available at https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646#0

Decree 886, 2014, available at https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=57338

Ecuador

Ecuadorian Constitution, 2008, available at Link

Data Protection Law, 2021, available at Link

Intercultural Education Law, 2017, available at Link

Law of Higher Education, LOES, 2010, available at https://www.ces.gob.ec/documentos/Normativa/LOES.pdf

Public Policy on Internet Safety for children and adolescents, 2020, available at https://www.igualdad.gob.ec/wp-content/uploads/downloads/2020/09/pol%C3%ADtica_publica_internet_segura.pdf

Europe

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, available at https://eur-lex.europa.eu/eli/reg/2016/679/oj

Mexico

Mexican Constitution, 2009, available at https://web.oas.org/mla/en/Countries_Intro/en_mex-int-text-const.pdf

Federal Law on Protection of Personal Data Held by Private Parties, 2010, available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Regulation on the Federal Law on Protection of Personal Data Held by Private Parties, 2011, available at http://inicio.inai.org.mx/English/2%20Regulations%20to%20the%20FLPPDHPP.pdf

General law for the protection of personal data in possession of government entities, 2017, available at https://mexico.justia.com/federales/leyes/ley-general-de-proteccion-de-datos-personales-en-posesion-de-sujetos-obligados/

National Institute for Access to Information and Protection of Personal Data, Guidelines on Privacy Notices, 2013, available at https://home.inai.org.mx

Guidelines on enforcement of the law, 2017, available at http://www.dof.gob.mx/nota_detalle.php?codigo=5469198&fecha=17/01/2017

Peru

Political Constitution of Peru, 2009, available at https://www.congreso.gob.pe/Docs/files/CONSTITUTION_27_11_2012_ENG.pdf

Law 29733 on Personal Data Protection, 2011, available at https://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

Implementing rules of the Personal Data Protection Law, 2013, available at Link

Directive 01-2020, 2020, available at https://www.minjus.gob.pe/wp-content/uploads/2020/01/Directiva-N°-01-2020-DGTAIPD-1.pdf

United Kingdom

Data Protection Act 2018, available at Link

Ministry of Education, *Data protection: a toolkit for schools,* 2018, available at Link

United States

Children's Online Privacy Protection Act, 1998, available at https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

Federal Trade Commission, 2015, Complying with COPPA: Frequently Asked Questions, available at https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

Acerca de la autora

Alexandra Contreras Flores: Alexandra is an economist with 10 years of experience. Her work experience includes the assessment of public policy in the field of competition and regulatory policies for the telecommunications sector, both as a policymaker and researcher in Ecuador, Turkey and Spain. She worked for the Ecuadorian telecom regulator Arcotel and the mobile operator Vodafone in Turkey. Her academic background includes a master's degree in Industrial Economics with a major in telecommunications at Carlos III de Madrid University. Alexandra is currently working for Cullen International, a regulatory intelligence provider based in Brussels. Her professional focus is on telecommunications, spectrum, digital economy, and data protection regulation.

Notas

↑1 State of the World’s Children, UNICEF, 2017, available at https://www.unicef.org/media/48601/file

↑2 Available at https://www.argentina.gob.ar/noticias/cuidar-la-privacidad-en-la-ninez

↑3 Colombian Constitution, 2015, available at https://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia%20-%202015.pdf

↑4 Personal Data Protection Policy, 2019, available at https://www.mineducacion.gov.co/1759/articles-353715_recurso_5.pdf