

CHILDREN AND DIGITAL ENVIRONMENTS: REGULATORY TRENDS IN LATIN AMERICA

Derechos Digitales
AMÉRICA LATINA

Children and digital environments:
Regulatory trends in Latin America

This publication was produced by Derechos Digitales, an independent non-profit organization, founded in 2005, whose mission is to defend, promote and develop fundamental rights in digital environments in Latin America.

This publication was possible thanks to the support of Luminate.

General Supervision and Review: Jamila Venturini

Research, Analysis and Drafting: Marina Meira

Style Review: Gastón Wahnish

Design: Alter Studio

Translation to English: Selex Idiomas

NOVEMBER, 2026

How to quote this article: Derechos Digitales. (2026). Children and digital environments: Regulatory trends in Latin America). https://www.derechosdigitales.org/en/recursos/children-and-digital-environments-regulatory-trends-in-latin-america/



CC-BY 4.0
This work is available under a Creative Commons Attribution 4.0 International License
https://creativecommons.org/licenses/by/4.0/deed.es

CONTENTS

INTRODUCTION 4

1. BACKGROUND 6

1.1. Criminal Law Frameworks and Associated Tensions 9

1.2. General Comment No. 25 of the United Nations Committee on the Rights of the Child as a Rights-Based Framework 12

1.3. Regulatory Models Aimed at Digital Services 13

2. LEGISLATIVE TRENDS IN LATIN AMERICA FOR THE PROTECTION AND PROMOTION OF CHILDREN AND ADOLESCENTS' RIGHTS IN DIGITAL ENVIRONMENTS 17

2.1. Argentina 18

2.2. Bolivia 20

2.3. Brazil 21

2.4. Chile 23

2.5. Colombia 25

2.6. Ecuador 26

2.7. Mexico 29

2.8. Panama 30

2.9. Paraguay 32

2.10. Peru 33

2.11. Uruguay 35

3. MAIN REGULATORY TRENDS IN THE REGION 38

3.1. Expansion of Criminal Law Responses and Surveillance 38

3.2. Age Restrictions and the Expansion of Age Determination 42

3.3. From Restricting Access to Regulating Digital Services 45

3.4. Two Emerging Agendas: Participation in Digital Economic Activities and Artificial Intelligence 47

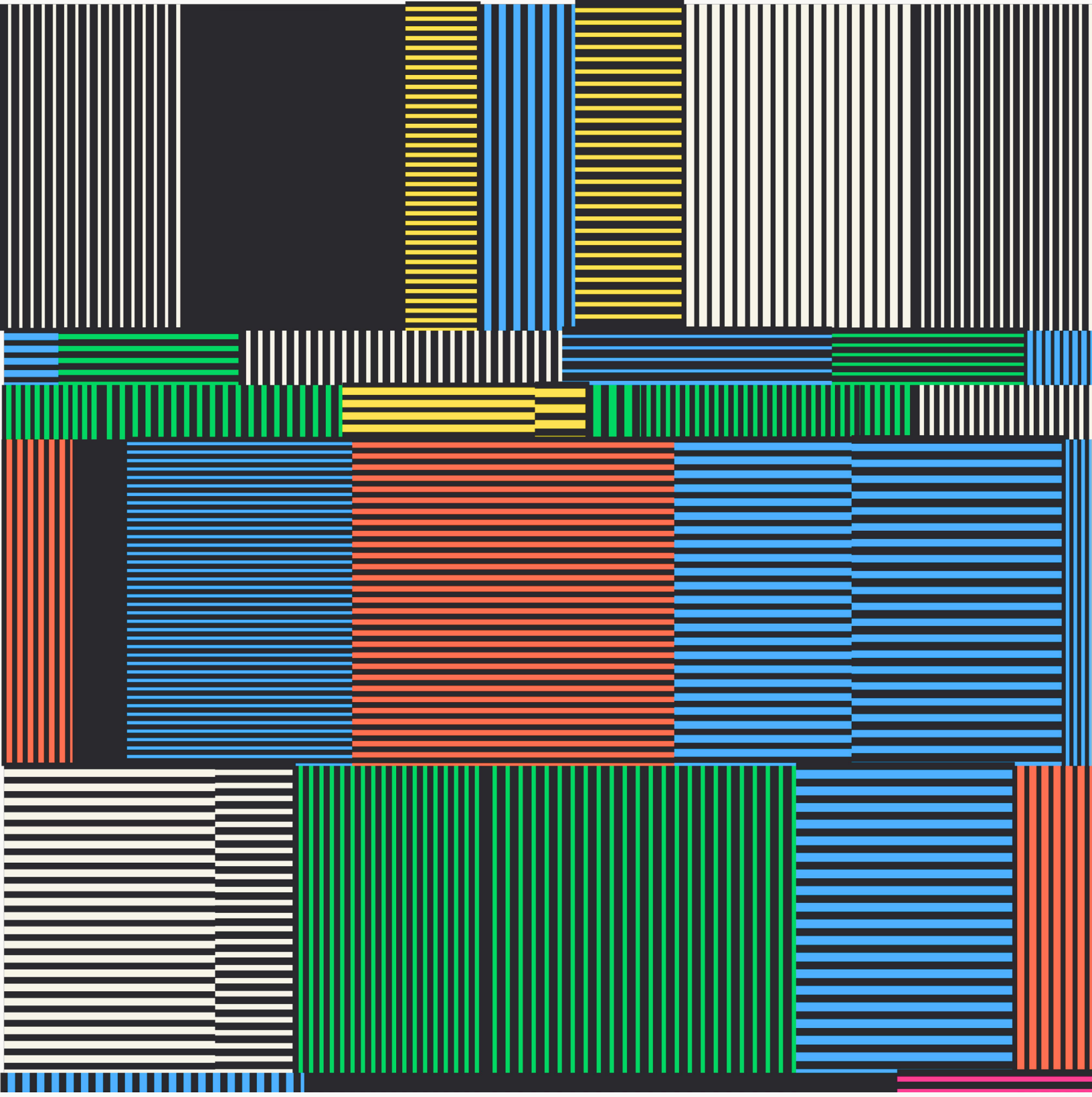
4. FINAL CONSIDERATIONS 51

INTRODUCTION

This publication presents an overview of the main legislative trends on the protection of children and adolescents (NNA, in Spanish) in digital environments in Latin America. Based on laws, regulations, and bills identified between June 2024 and September 2026 in 11 countries, it aims to detect the risks that guide these responses and the different regulatory models adopted or proposed. The analysis uses human rights as a reference, considering both rights of children and adolescents, as well as the implications of these measures for the set of Internet users.

The report is not intended to provide a comprehensive inventory of initiatives in the region or to assess the outcomes of implementing the standards. It focuses on nationwide initiatives directly related to the protection of children and adolescents in digital environments, excluding measures focusing exclusively on the use of devices in educational institutions and general data protection or artificial intelligence frameworks whose main purpose is not the protection analyses in this report.

This document is organized in four parts. First, it presents the background and reference frameworks for the debate. Then, it describes the initiatives identified by country and analyzes the main regional trends, which include reinforcing criminal responses, age restrictions on access to social media, broader digital services regulations and emerging agendas related to the economic participation of children and adolescents in digital environments and artificial intelligence (AI). It then identifies the main regional trends and, finally, raises considerations to guide a Latin American agenda that guarantees comprehensive rights-based protection.



01

BACKGROUND

01

1. BACKGROUND

Protection of children and adolescents (NNA, in Spanish) in digital environments has acquired, in recent years, a growing presence in regulatory and public policies agendas both in Latin America and other regions of the world. This process accompanies, first, a growing expansion trend in terms of Internet access and use that also reaches younger generations. Children and adolescents access the Internet from an increasingly early age and use digital technologies for various activities, ranging from studying and searching for information to communicating, playing and accessing audiovisual content.

As early as 2017, UNICEF estimated that one in three Internet users worldwide was under the age of 18. In Latin America, the expansion of connectivity in recent years has deepened this trend. A study published by ECLAC in June in 2026, based on comparable data from the Kids Online initiative in Argentina, Bolivia, Brazil, Chile, Costa Rica and Uruguay, shows that Internet access at home currently exceeds 90% in most of these countries. The mobile phone has also established itself as the main connecting device and is increasingly acquired at younger ages. The most widespread practices among children and adolescents on the Internet include audiovisual entertainment, interpersonal communication, and informal learning, with a prominent presence of messaging and social media platforms such as WhatsApp, YouTube and TikTok[1].

These data, however, do not describe a homogeneous experience. Speaking of the relationship between children and technologies in Latin America involves considering the region's deeply-rooted inequalities. Socio-economic conditions, territory, genre, race and ethnics, access to education conditions as well as family and care structures affect both possibilities of access to technologies and the ways in which they are used and mediated. In this sense, it is more appropriate to speak of *childhoods* and their different relationships with digital environments, in plural[2].

In other words, the experiences of boys and girls differ based on their social, economic, cultural and territorial conditions, and those inequalities also impact their relationship with the digital environment. Regional evidence, in turn, confirms the persistence of these differences. Although domestic Internet access is approaching

1 Magdalena Claro, Patricio Cabello and Carolina Castro Grau. *Experiencia digital en la niñez y adolescencia en América Latina: Argentina, Bolivia (Estado Plurinacional de), Brasil, Chile, Costa Rica y Uruguay. CEPAL*. (Santiago, 2026). Available at: https://www.cepal.org/es/publicaciones/90132-experiencia-digital-la-ninez-adolescencia-america-latina-argentina-bolivia

2 Isabella Henriques, Marina Meira and Pedro Hartung. "*As múltiplas infâncias e a invisibilidade da criança", O Futuro da Infância no Mundo Digital. (São Paulo, 2021),* 237-243. Available at: https://criancaeconsumo.org.br/wp-content/uploads/2021/11/o-futuro-da-infancia-no-mundo-digital-ensaios-sobre-liberdade-seguranca-e-privacidade.pdf

high levels in the six countries analyzed by ECLAC, there still are significant socioeconomic gaps, particularly in access to computers and other devices that allow for more diversified and complex uses[3].

Inequalities also affect the possibilities of family accompaniment. National studies of the Kids Online series have shown associations between socioeconomic and educational conditions of households and forms of mediation of Internet use. In general, the schooling of parents and those in charge of families is associated with the orientation and mediation actions of the digital experience for their sons and daughters[4]. This is particularly relevant in a region characterized by high levels of informal employment, an unequal distribution of caregiving responsibilities, and limited time and resources in many households. These conditions alone do not determine the digital practices of children and adolescents, but they are part of the context in which families can (or cannot) accompany those experiences.

The expansion of access to digital environments has also been accompanied by a growing concern about the risks children may face online. Because they are in stages of physical, cognitive and psychosocial development, children and adolescents may be particularly susceptible to certain forms of manipulation, exploitation, violence and commercial practices, with characteristics and levels of exposure that vary according to age, the evolution of their abilities and their individual and social contexts.

The typology developed by the OECD allows us to measure the complexity of these risks, sorting them in four big categories: Content, Conduct, Contact and Consumer[5]. The first refers to exposure to content that may be harmful, illegal or inappropriate, such as hate speech, disinformation or certain violent or sexual content. Conduct risks arise from children and adolescents' interactions in digital environments and include, for example, cyberbullying, peer-to-peer sexual content exchanges, and other potentially harmful conducts. Contact risks, however, occur in interactions with adults who may expose children and adolescents to situations of sexual harassment, manipulation, abuse or exploitation. Finally, consumer risks are related to their participation as users

3 Magdalena Claro, Patricio Cabello and Carolina Castro Grau. *Experiencia digital en la niñez y adolescencia en América Latina: Argentina, Bolivia (Estado Plurinacional de), Brasil, Chile, Costa Rica y Uruguay.CEPAL*. (Santiago, 2026). Available at: https://www.cepal.org/es/publicaciones/90132-experiencia-digital-la-ninez-adolescencia-america-latina-argentina-bolivia

4 Ibid.

5 OECD. Children in the digital environment: revised typology of risks. (Paris, 2021). Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/01/children-in-the-digital-environment_9d454872/9b8f222e-en.pdf

and consumers of digital services and include, among others, inappropriate business practices, commercial profiling, fraud and induced expenses.

These categories do not operate in isolation and intersect with other human rights. One given experience may combine content, contact, consumer, conduct, consumption and privacy, while certain characteristics of the design of digital services may contribute to amplifying them. Social media recommendation systems can increase repeated exposure to certain inappropriate content; mechanisms aimed at maximizing interaction can incentivize certain harmful behaviors; and data collection for profiling can expose them to commercial exploitation practices such as targeted advertising.

This mix of dimensions is important to understand the growing regulatory attention on this issue, but also to critically analyze the responses that have been put on the table. Given that risks affecting children and adolescents have different causes, are intertwined and depend on bigger socio-economic conditions, it would be really difficult to address them with a single technological or legal measure.

The growing political centrality of the issue is also explained by a progressive accumulation of evidence on these risks. Another reason is that, in different countries, serious cases of violence, abuse or death of children and adolescents related in some way to the use of digital services have acquired a strong public impact and contributed to accelerating regulatory debates. These episodes often play a catalytic role in making visible risks that have not been discussed until then and in generating pressure for public authorities to respond. At the same time, the context of urgency and upheaval surrounding them may favor reactive and risk-focused legislative responses that have gained greater public visibility, even if this is only one dimension of a broader problem.

This growing political attention is also expressed in spaces for regional articulation. On 20 December 2025, Argentina, Bolivia, Brazil, Paraguay and Uruguay, as Member and Associate States of MERCOSUR, adopted a declaration on the protection of children and adolescents in digital environments[6]. The document recognizes the progressive autonomy and importance of technologies for the exercise of rights and urges companies to adopt high levels of security from the design and protection of privacy. It also promotes cooperation in investigating crime, assisting victims and strengthening institutional capacities, and stresses that the safeguards offered by digital services should not be asymmetric among countries. The declaration thus reflects the inclusion

6 Declaración especial del MERCOSUR sobre protección de la infancia y adolescencia en entornos digitales (Special declaration of MERCOSUR on the protection of children and adolescents in digital environments). 20 December 2025. Available at: www.mercosur.int/declaracion-especial-del-mercosur-sobre-proteccion-de-la-infancia-y-adolescencia-en-entornos-digitales

of the topic in a regional agenda that covers both corporate responsibilities and coordinated action by States.

Likewise, the relationship between children and adolescents and technologies should not be addressed solely from the risk perspective. The Internet and digital technologies constitute spaces for the exercise of rights, including access to information and education, freedom of expression, participation, play, culture and socialization. A protection-oriented policy must therefore be able to reduce risks without eliminating the opportunities and rights associated with access to and participation of children and adolescents in digital environments.

The Convention on the Rights of the Child[7] is based on the recognition of children and adolescents as subjects and holders of human rights, which must also be guaranteed throughout the various stages of their development. At the same time, their particular development stage underpins the right to special measures of protection and care, which must accompany their evolving capacities and their progressive autonomy. This twofold dimension, the full exercise of rights and the guarantee of special protection, is key to address their relationship with digital environments and prevent children and adolescents from being treated only as objects of protection, rather than as right holders, who should be able to exercise and fully enjoy them also in these spaces.

1.1. Criminal Law Frameworks and Associated Tensions

This legislative concern about the risks posed by technology to children and adolescents is not new in Latin America. Long before the current proliferation of legal initiatives, several countries in the region had reformed their criminal laws to respond to forms of violence, especially sexual violence, facilitated by technologies, particularly the production and circulation of child sexual abuse material and grooming, understood as the approach of an adult person to children and adolescents through digital means for sexual purposes.

In 2013 for instance, Argentina criminalized[8] contact with children and adolescents by electronic means with a view to committing crimes against their sexual integrity by means of Act No. 26,904. The following year, Peru adopted Act 30,171[9], which incorporated into its criminal legislation proposals to children and adolescents for sexual purposes made through the Internet or other technological means. Costa Rica,

7 Available at: https://www.un.org/es/events/childrenday/pdf/derechos.pdf

8 Available at: https://www.argentina.gob.ar/normativa/nacional/223586/texto

9 Available at: https://img.lpderecho.pe/wp-content/uploads/2023/07/Ley-30171-LPDerecho.pdf

in turn, in 2021 adopted Act No. 10,020[10] to prevent and punish grooming, amending several provisions of its Criminal Code and also creating an inter-institutional commission dedicated to the matter. A regional comparison published by ECPAT in 2022 then identified five Latin American countries (Colombia, Costa Rica, Honduras, Peru and Uruguay) whose legislation expressly criminalized grooming for sexual purposes, including through the Internet and other information and communication technologies, in addition to seven others who did it partially[11].

Brazil followed a related trajectory, but with different instruments. Apart from the provisions set forth in *Estatuto da Criança e do Adolescente* (Statute of the Child and Adolescent) which criminalize acts related to the production, distribution and possession of child sexual abuse material, in 2017 Act No. 13,441[12] authorized undercover police infiltration on the internet to investigate crimes targeting the sexual dignity of children and adolescents.

This background allows identifying an important characteristic of the first state responses to the relationship between children and the Internet: it is clearly focused on criminal law and, particularly, sexual violence and exploitation. At a still early stage of developing legal frameworks specifically aimed at behavior conducted or facilitated in digital environments in Latin America, these responses were mainly geared toward adapting existing criminal types and investigative tools, or creating new ones to respond to the forms that these behaviors acquired with the use of digital technologies.

Some of these responses also generated tensions with other rights and guarantees related to the use of the Internet. Over time, these controversies contributed to building a pretended opposition between two agendas that should actually be complementary: the protection of children and adolescents in digital environments and the defense of human rights on the Internet. The debate on cryptography is a particularly clear example. In different countries, combating the abuse and sexual exploitation of children and adolescents and the circulation of child sexual abuse materials has been used as an argument to propose mechanisms for accessing or scanning private communications.

10 Available at: https://vlex.co.cr/vid/asamblea-legislativa-republica-costa-915230449

11 ECPAT. *Latin America – Summary of Recommendations: Legal Interventions in Latin America*. (2022). Available at: https://ecpat.org/resource/latin-america-summary-of-recommendations-legal-interventions-in-latin-america/

12 Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13441.htm

weakening the guarantees offered by end-to-end cryptography[13]. The debate is often raised as a choice between children and adolescents' security and privacy protection. This idea, however, is based on a false premise[14]. Cryptography also protects children and adolescents by preserving the confidentiality of their communications, contributing to their security and enabling the exercise of rights such as privacy and freedom of expression. At the same time, its weakening has implications that go beyond this group, as it affects a technology critical to security and trust in the digital ecosystem, used to protect communications, transactions, personal data and multiple services and infrastructures from unauthorized access. Measures taken to respond to a specific risk can thus introduce vulnerabilities with consequences for all Internet users.

Similar tensions appear in the face of the massive adoption of surveillance technologies in public spaces with the goal of protecting children and adolescents. Technologies such as facial recognition, for example, have been presented as tools to help identify and locate missing children and adolescents. Although such goal is indisputably legitimate, there is insufficient evidence that the deployment of facial recognition systems is an effective and necessary response to meet that goal. Instead, there is documented evidence of the risks and harms associated with these technologies, including misidentification, discriminatory impacts (particularly on black people and other groups historically under surveillance), undue arrests and the expansion of mass surveillance infrastructures[15]. In Latin America, where facial recognition systems have already been deployed for public safety and urban surveillance purposes, expanding these infrastructures in the name of children protection can contribute to standardizing technologies whose impacts on privacy, non-discrimination and other human rights have already been documented.

13 Child Rights International Network, defenddigitalme. Privacy and Protection: A children's rights approach to encryption. (United Kingdom, 2023). Available at: https://home.crin.org/readlistenwatch/stories/privacy-and-protection

14 Meira, M. & Amaral, P., "*As falhas da oposição entre criptografia e proteção de crianças e adolescentes", Observatório da Criptografia (2023).* Available at: https://obcrypto.org/as-falhas-da-oposicao-entre-criptografia-e-protecao-de-criancas-e-adolescentes/

15 ALSUR, *Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa (Facial recognition in Latin America: Trends in the implementation of a perverse technology)*. (2021). Available at: https://www.alsur.lat/reporte/reconocimiento-facial-en-america-latina-tendencias-en-implementacion-una-tecnologia; ALSUR, *Reconocimiento facial y tecnologías de vigilancia en América Latina: casos, proveedores y dinámicas comerciales (Facial recognition and surveillance technologies in Latin America: Cases, suppliers and business dynamics)*. (2025). Available at: https://www.alsur.lat/reporte/reconocimiento-facial-tecnologias-vigilancia-en-america-latina-casos-proveedores-dinamicas

These examples do not imply denying the problems these measures seek to face. Instead, they show why the severity of the risks affecting children and adolescents requires careful assessment of the effectiveness and impacts of proposed legal responses and public policies. Nor is it productive to treat the protection of children and adolescents and the defense of human rights on the Internet as opposing agendas. This opposition may lead, on the one hand, to legitimate concerns about privacy, security or freedom of expression being presented as obstacles to the protection of children and, on the other hand, to measures to protect children and adolescents being analyzed exclusively on the basis of their possible restrictive effects; without properly considering the risks and violence they seek to address.

1.2. General Comment No. 25 of the United Nations Committee on the Rights of the Child as a Rights-Based Framework

This set of tensions helps understand the emergence of a wider approach on the relationship between children and adolescents and digital environments. Unlike the previous generation of responses, which was mainly focused on the criminalization of certain behaviors and the protection against specific risks, a perspective oriented towards thinking about the digital environment from the point of view of all the rights held by children and adolescents began to consolidate. This shift did not mean to abandon the responses adopted against serious forms of violence, but to expand the framework of analysis, incorporating the necessary conditions for children and adolescents to exercise their rights and participate in digital environments, in such a way that is safe and matches their evolving autonomy.

The major milestone in this process was the adoption, in 2021, of the General Comment No. 25 on children's rights in relation to the digital environment[16], by the United Nations Committee on the Rights of the Child. The document interprets the obligations set forth by the Convention on the Rights of the Child in the face of transformations brought about by digital technologies and establishes that States must respect, protect and fulfill the rights of children and young persons in these settings as well. It included a consultative process involving more than 700 children and adolescents from 27 countries.

The relevance of General Comment No. 25 lies, among other aspects, in shifting the debate from a logic exclusively aimed at protecting children and adolescent from the Internet towards a discussion on how to guarantee their rights in the digital environment. The document recognizes both the risks and opportunities associated with technologies, and places Convention principles, such as best interests, non-

16 Available at: https://docs.un.org/es/crc/c/gc/25

discrimination, evolving autonomy and capacity development and the right to be heard, at the heart of digital policies. The text points out that significant access to technologies can contribute to the exercise of civil, political, economic, social and cultural rights. Protection measures should therefore also be assessed in the light of their potential impacts on those rights.

At the same time, the General Comment provides a framework for translating the principles and obligations of the Convention into the formulation of public policies and regulatory frameworks on digital technologies. By addressing issues such as data protection and privacy, business practices, service design, content access, security, digital literacy and responsibilities of the business sector, the document provides a common regulatory basis from which states can develop concrete regulatory responses. In this sense, its adoption not only contributed to consolidating a rights-based approach to the relationship between children and technologies, but also became a relevant precedent for the new generation of policies and regulations aimed at children and adolescents in digital environments.

1.3. Regulatory Models Aimed at Digital Services

As this international framework of rights began to consolidate, there appeared multiple regulatory initiatives focused on the relationship of children and adolescents with digital services and environments. This movement developed at the confluence of a growing incorporation of an approach of children and adolescents' rights in the digital environment, driven, among other instruments, by General Comment No. 25, and the advancement of comprehensive regulatory frameworks for digital platforms.

This movement initially acquired greater intensity in countries of the Global North, particularly in Europe and Australia. In these contexts, regulatory responses went beyond addressing illicit behaviors and began to incorporate measures aimed at intervening on the characteristics and practices of digital services themselves. Thus, obligations for companies, including those related to the processing of personal data and the design and operation of digital products and services, became more relevant.

One of the first benchmarks of this new regulatory generation was the *Age Appropriate Design Code* in the United Kingdom[17], developed by the Information Commissioner's Office (ICO). It was produced by virtue of a mandate established by the Data Protection Act of 2018, which instructed the ICO to adopt a specific code of practice on age-appropriate design standards in information society services that could be used by

17 Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

children and adolescents. The Code established 15 standards for digital services likely to be used by children and adolescents, including consideration of their best interests, high privacy settings by default, data minimization, limitations on profiling and geolocation, as well as restrictions on the use of design techniques intended to induce them to provide unnecessary personal data or reduce their privacy protections.

The UK regulatory framework was subsequently expanded with the *Online Safety Act*[18], which establishes obligations for interaction services between users, search engines and certain services that publish pornographic content, with differentiated requirements according to the type of service and the risks involved. In 2025, the Office of Communications (Ofcom) — the regulatory authority for broadcasting, internet, telecommunications and postal services[19] — published the specific codes of practice for the protection of children and adolescents applicable to interaction services between users and search engines, thus deepening a regulatory approach that, in addition to the guarantees linked to privacy and design, incorporates obligations of assessment and mitigation of risks on the part of suppliers.

At the same time, at European Union level, the adoption of the *Digital Services Act* (DSA)[20] in 2022 incorporated the protection of children and adolescents into the general regulatory framework for digital services. Unlike the UK Code, the DSA is not a regulation specifically aimed at children and adolescents, but a general regulatory framework for digital services that incorporates specific provisions for their protection. Among them is the requirement that platforms accessible to children and adolescents adopt appropriate and proportionate measures to ensure a high level of privacy, security and protection in their services. It also prohibits the presentation of advertising based on profiling from personal data, when the platform knows with reasonable certainty the age of the user. These provisions reflect some of the discussions also present in General Comment No. 25, particularly in relation to the processing of personal data and business practices directed at children and adolescents.

Australia, in turn, has its own track record of regulating online safety. In 2015, the *eSafety Commissioner* was created as an independent authority responsible for online safety in the country, initially focused on the protection of children and adolescents from cyberbullying and the circulation of child sexual abuse materials. Its mandate was

18 Available at: https://www.legislation.gov.uk/ukpga/2023/50/contents

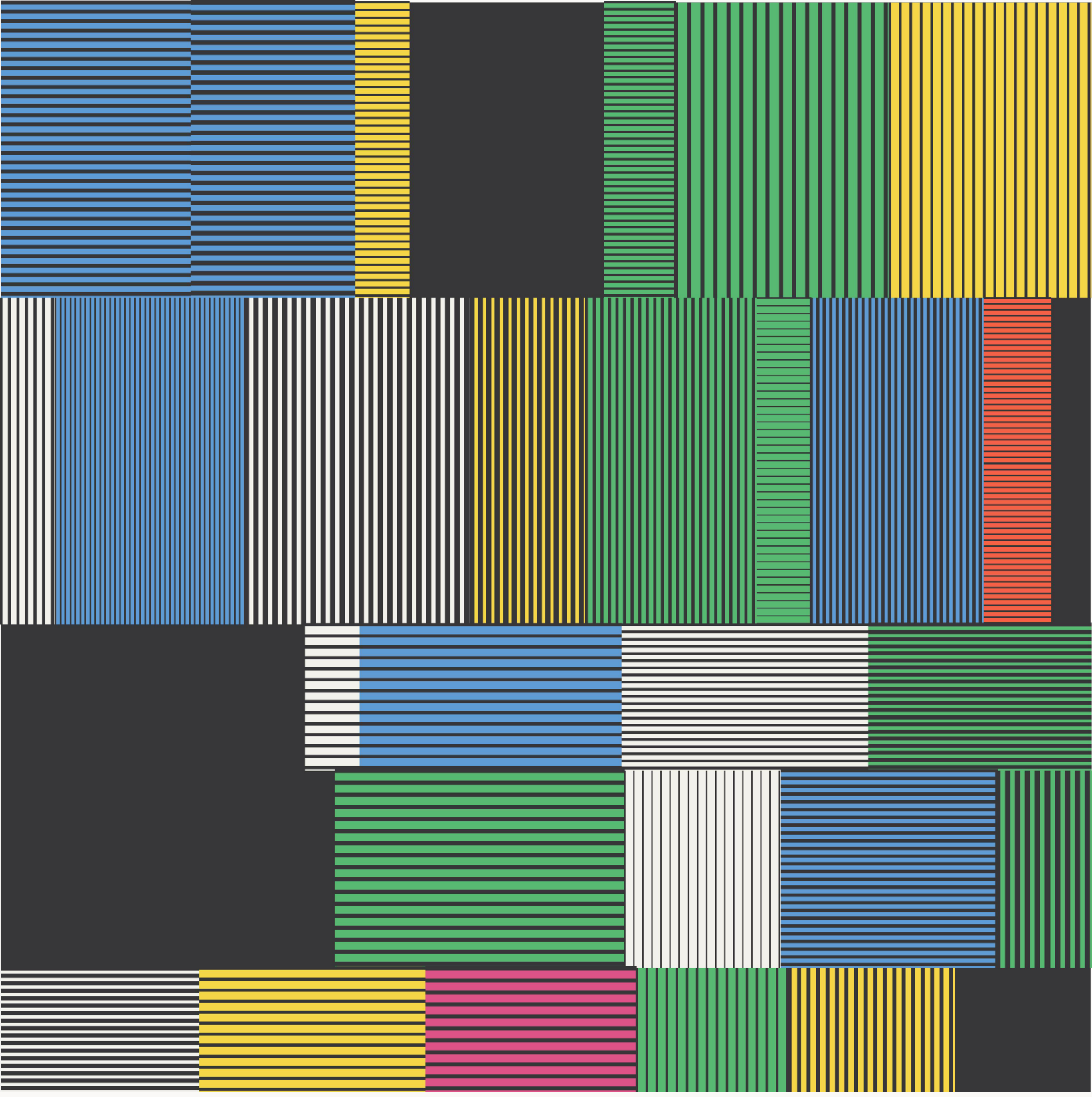
19 Available at: https://www.ofcom.org.uk/

20 Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022R2065

subsequently expanded and consolidated through the *Online Safety Act* of 2021[21]. On this regulatory trend, in December 2024 the country adopted a different and particularly influential approach in the recent debate, by passing an amendment to the *Online Safety Act* that requires certain social media to take reasonable measures to prevent people under 16 from maintaining accounts. The obligation came into force in December 2025. Unlike models focused mainly on introducing safeguards in the design and operation of services, this approach places age as a condition of access, simultaneously opening debates on mechanisms to determine the age of users, privacy, progressive autonomy, and access to information.

These models did not remain confined to the jurisdictions where they emerged. As has happened in other areas of digital regulation, its concepts and instruments have influenced discussions in other countries and regions, including Latin America.

21 Available at: https://www.legislation.gov.au/C2021A00076/latest/text



02

LEGISLATIVE TRENDS IN LATIN AMERICA FOR THE PROTECTION AND PROMOTION OF CHILDREN AND ADOLESCENTS' RIGHTS IN DIGITAL ENVIRONMENTS

02

2. LEGISLATIVE TRENDS IN LATIN AMERICA FOR THE PROTECTION AND PROMOTION OF CHILDREN AND ADOLESCENTS' RIGHTS IN DIGITAL ENVIRONMENTS

In recent years, the protection of children and adolescents in digital environments has gained relevance in public debate and legislative agendas from different Latin American countries. The following mapping presents the laws passed and some of the major bills discussed in the region between June 2024 and September 2026. This period of just over two years was selected to examine the recent evolution of legislative agendas on the protection of children and adolescents in digital environments in the region. During this time window, the adoption of age restrictions for the use of social media in Australia, the proliferation of similar projects in Latin America, and the discussion and passing of laws of broader scope regulating digital services for the protection of children and adolescents in the region converged.

The analysis is organized by country and comprises Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Paraguay, Peru and Uruguay. These countries were selected for the relevance of the initiatives identified throughout the period and because they feature a diversity of regulatory approaches for the protection of children and adolescents in digital environments. The inclusion of the countries indicated in the mapping does not imply any kind of assessment of their degree of development in terms of digital policies or child protection frameworks.

The initiatives were identified through searches at government and legislative bodies official websites in the countries of the region, complemented by reviewing news and publications from civil society organizations.

The mapping includes, on the one hand, new laws and regulations passed during the period, with particular emphasis for Bolivia, Brazil, Colombia, Panama, Peru and Uruguay, where frameworks aimed at different aspects of children and adolescent protection in digital environments were adopted. On the other hand, we have examined bills that were still under discussion at the end of the period analyzed, but that are relevant both for their scope and for the regulatory models they propose. In most countries, in fact, much of the legislative activity identified was still in this second phase.

It is worth mentioning that the objective of this report is not to make an exhaustive inventory of all the initiatives presented in these countries, but to identify cases that allow observing the different regulatory models that have been adopted or discussed. Therefore, nationwide initiatives directly related to the protection of children and adolescents in digital environments were given priority.

This delimitation implies leaving out of the mapping some initiatives that are also part of the broader debate on children and technologies, but whose main purpose is not the regulation of digital environments. In particular, rules and projects specifically focused on restricting or regulating the use of cell phones and other devices in educational institutions are not included. Although these measures have gained a significant presence on the legislative agendas of different countries in the region and may address concerns related to the digital well-being of children and adolescents, they raise specific debates about education policies and device use that go beyond the focus of this report. Nor does it include broader regulatory frameworks that may eventually contain specific devices on the protection of children and adolescents, such as data protection laws or the regulation of Artificial Intelligence.

2.1. Argentina

The main framework for child protection in Argentina is Act No. 26,061[22] of 2005 on the Comprehensive Protection of the Rights of Children and Adolescents. The country also has specific legislation on some forms of violence facilitated by technologies, such as grooming. However, it has not adopted a national legislative framework specifically aimed at comprehensively regulating the rights and protection of children and adolescents in digital environments. This has been the objective of several specific projects presented in 2026. Among the most far-reaching initiatives is Bill No. 2,733-D-2026, Law on Digital Care and Welfare - Responsible Use of Devices and Social Media for Children and Adolescents[23], presented in June. It seeks to establish a general framework for the use of social media platforms and similar services, based, among other principles, on the best interest, progressive autonomy, privacy and protection of personal data, secure design and default protection, as well as enhanced liability of digital service providers.

The project establishes broad obligations for platforms and other digital service providers. These include duties of prevention, mitigation and redress against foreseeable risks for children and adolescents, as well as restrictions on design and profiling mechanisms aimed at maximizing the time spent or exploiting vulnerabilities. The proposal prohibits behavioral advertising targeting children under the age of 16 and establishes specific conditions for advertising targeting adolescents aged 16 and 17. It also identifies as risk factors certain features of the design of the services, such as dark patterns, autoplay, intrusive notifications, recommendation systems aimed at maximizing time spent and unrestricted interactions with third parties.

22 Available at: https://servicios.infoleg.gob.ar/infolegInternet/anexos/110000-114999/110778/norma.htm

23 Available at: https://www.hcdn.gob.ar/proyectos/detalle_tp_adjunto/index.html?id=292460

In terms of access to social media, the project establishes an age-based stage system. Although it does not define what is meant by "social media", the proposal expressly mentions platforms such as X, Instagram, Facebook, YouTube and TikTok, in addition to "other similar services". According to the text, the platforms could not allow the creation or maintenance of accounts by people under the age of 14, even with parental consent. Between 14 and 16, access would require parental consent. To enforce these restrictions, the proposal requires technical systems to determine the age, excluding self-declaration as the only mechanism. The bill also provides for a State verification mechanism that would inform the platforms only if the person meets the applicable age threshold, without transferring data such as document number, address, biometric image or exact date of birth.

Alongside this broader proposal, other initiatives focused particularly on the conditions of access to social media were presented during 2026. Bill No. 1,114-D-2026[24], presented in April, proposes to create a regime of protection, responsible use and parental support. The initiative also establishes a system that is phased according to age, although with different thresholds: under 13, the creation of accounts is prohibited, with certain exceptions based on their best interests; between 14 and 16, access depends on parental consent; and between 16 and 18 the creation and use of accounts is allowed, unless there is a judicial restriction. The proposal also establishes obligations for digital service providers, including the implementation of age determination systems and mechanisms to verify parental consent where appropriate.

In September 2026, Bill No. 4,477-D-2026 was also presented[25], which proposes to establish a "digital legal age" at 15, to access to social media. People under 15 would require authorization from their parents/guardians to access these services. The proposal also incorporates obligations for the platforms, including mechanisms for determining age and parental consent, settings of maximum privacy and security by default, deactivation of geolocation and limitations on profiling for advertising purposes and certain recommendation systems. The data used to verify age or parental consent could not be used for different purposes.

Updating the criminal response to technology-facilitated forms of violence was also part of the recent legislative debate. In April 2026, for example, Bill No. 1,241-D-2026[26], which proposes to amend article 131 of the Criminal Code, on grooming, was introduced.

24 Available at: https://www.hcdn.gob.ar/proyectos/detalle_tp_adjunto/index.html?id=290679

25 Available at: https://www.hcdn.gob.ar/proyectos/detalle_tp_adjunto/index.html?id=294254

26 Available at: https://www.hcdn.gob.ar/proyectos/detalle_tp_adjunto/index.html?id=290893

The initiative seeks to update the criminal offense applicable to contact with children through electronic communications, telecommunications or other technologies of transmission of data for sexual purposes. In June, Bill No. 2,744-D-2026[27], which proposes to amend the Criminal Code to explicitly incorporate the use of artificial intelligence techniques in the generation and dissemination of images of sexual content, was also presented, expanding the criminal response to new forms of production of sexual material involving or representing children.

2.2. Bolivia

Bolivia has had, since 2014, a comprehensive protection framework for children and adolescents called Girls, Boys and Adolescents - Act No. 548, 2014)[28] (Código Niña, Niño y Adolescente, in Spanish). In September 2025, Act No. 1,636 on the Protection of Sexual Integrity of Children and Adolescents in Digital Environments[29] was passed. This was the main legislative change in the country within the period analyzed. This regulation aims to identify, investigate and punish crimes against the sexual integrity of children and adolescents committed using information and communication technologies and is presented as the first Bolivian law specifically aimed at sexual violence against children and adolescents in digital environments.

Act No. 1,636 maintains a strong focus on criminal law and the prosecution of offenses. Among other changes, it amends the Criminal Code to incorporate or update sexual violence-related behavior in digital environments and establishes instruments to facilitate its investigation. According to the Attorney General's Office (*Fiscalía General del Estado, in Spanish*), the legislation sought to respond to difficulties in investigating and punishing phenomena such as grooming, sextortion and the production and circulation of child sexual abuse material[30].

The regulation, however, also provides mechanisms to prevent, protect, repair, and rehabilitate victims. Besides, it instructs the Ministry of Health and Sports to implement plans, programs and specialized mental health services for children and adolescents that have been victims of crimes in digital environments. Among them, Act No. 1,636 obliges these companies to provide the competent authorities, within 24 hours, with the information and documentation required for the investigation of offenses provided for by law, and to

27 Available at: https://www.hcdn.gob.ar/proyectos/detalle_tp_adjunto/index.html?id=292465

28 Available at: https://www.coordinadoradelamujer.org.bo/observatorio/archivos/marco/l548_389.pdf

29 Available at: https://www.lexivox.org/norms/BO-L-N1636.xhtm

30 Available at: https://www.fiscalia.gob.bo/fiscalias-superiores/fiscalia-superior-en-razon-de-genero/ley-n1636

retain for at least two years data and metadata derived from the communications, including IP addresses, geographical origin, frequency and browsing data.

It also establishes specific responsibilities for public and private companies that provide telecommunications services and information and communication technologies, such as the prohibition of the dissemination of personal data or images of victims and the immediate removal of child sexual abuse material from digital platforms.

2.3. Brazil

Since 1990, Brazil has had the *Estatuto da Criança e do Adolescente* (ECA)[31] as a general framework for the protection of children and adolescents. During the period under study, it adopted Act No. 15,211 (Digital ECAl) in September 2025[32], which establishes rules for the protection of children and adolescents in digital environments and applies to information technology products and services targeted to this group, regardless of the location of the company responsible for their development, offering or operation.

The regulation addresses different dimensions of the relationship between children and adolescents and digital services. It establishes obligations of prevention and mitigation of risks related, among others, to sexual exploitation and abuse, violence and cyberbullying, self-harm and suicide, gambling, harmful commercial practices and pornographic content. Furthermore, the legislation incorporates a logic of protection by design, which means that products and services aimed at, or likely to be accessed by, children and adolescents must by default adopt the most protective configuration available in terms of privacy and protection of personal data. The framework also establishes requirements for parental supervision tools, child monitoring products, and interaction capabilities in electronic games.

With regard to access to social media, as per this Act, accounts of children under 16 must be linked to the account of a legally responsible person. On the other hand, the creation of profiles of children and adolescents for commercial advertising purposes is prohibited. Likewise, the use of certain technologies, including emotional analysis, augmented reality, extended or virtual, is prohibited for this purpose.

Finally, the regulation establishes the obligation to remove, and notify the relevant authorities about, content related to sexual exploitation or abuse, kidnapping and grooming. As per this legislation, the National Data Protection Agency (ANPD, in Spanish) is in charge of regulatory and supervisory functions.

31 Available at: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm

32 Available at: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm

According to Decree 12.880/2026[33], which regulates the Digital ECA and establishes the National Policy for the Promotion and Protection of the Rights of Children and Adolescents in the Digital Environment, principles such as proportionality, necessity, security, privacy and protection of personal data must be observed in the mechanisms of age determination. The decree develops the provisions of the Act relating to issues such as addictive design and regulates the participation of children as creators of digital content for commercial purposes, establishing the requirement of prior judicial authorization for the monetization or remunerated promotion of content on social media and other digital platforms.

Despite the approval of the Digital ECA and the publication of its regulatory decree, projects such as Bill No. 2.387/2025[34] and the initiatives attached to it, which propose to prohibit access to social media for children under 16, which would be a stricter restriction, are still under way.

Another aspect of Brazilian regulation during the period focused on a criminal approach to sexual violence facilitated by digital technologies. In August 2026, Act No. 15.487/2026[35] was adopted, amending the *Estatuto da Criança e do Adolescente* (ECA), the Criminal Code, the Code of Criminal Procedure and other regulations to broaden and strengthen the criminal treatment of various behaviors related to sexual violence against children and adolescents, including those practiced in digital environments and through Artificial Intelligence.

The resolution covers the production, transmission, storage and access to sexual violence material and expressly includes content produced, manipulated or generated with Artificial Intelligence, *deepfakes* and other resources used to alter image or videos. It also stipulates a one to two thirds increase in sentences, when offenses are committed through techniques of masking, hiding, falsifying, altering or anonymizing IP addresses or other digital identifiers such as, among others, the use of virtual private networks (VPN). It also recognizes the right of children and adolescents, victims or witnesses of sexual violence, to receive individual, specialized, continuous and comprehensive psychological and psychosocial care.

33 Available at: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm

34 Available at: https://www.camara.leg.br/proposicoesWeb/prop_visual_impress?idProposicao=2511795&ord=1

35 Available at: https://planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15487.htm

2.4. Chile

Chile has a general framework for the protection of the rights of children and adolescents established by Act No. 21,430[36] of 2022, on the guarantees and comprehensive protection of the rights of children and adolescents, which expressly recognizes rights related to private life, protection of personal data and access to information and technologies. During the period under study, an increasing number of projects specifically designed for the protection of children and adolescents in digital environments were presented to support the current general framework.

In June 2025, Bill No. 17,624-19[37] was presented, which proposes to regulate the content that digital services platforms offer to children and adolescents and prevent their addiction to social media. The proposal starts from the risks posed by certain characteristics of the platforms on the welfare of children and adolescents and sets out obligations aimed at reducing their exposure to content and dynamics considered harmful.

In 2026, this debate broadened considerably. In April, Bill No. 18.224-18[38], which aims to establish a comprehensive framework to protect children and adolescents in the use of social media, was presented. In the following months, this initiative was merged with other projects that address, from different perspectives, protection against the addictive use of technologies, algorithmic responsibility and digital protection of children and adolescents, and the incorporation of child protection principles in the cybersecurity framework.

Among the restated projects, Bill No. 18,318-19[39] stands out, proposing a regulation on algorithmic responsibility and digital protection of children and adolescents. The initiative provides for the regulation of access to platforms based on their evolving autonomy, prohibition of addictive algorithmic design and dark patterns aimed at children and adolescents, restrictions on behavioral advertising and algorithmic profiling, reinforced standards on the protection of personal data and a specific regime of liability for digital platform suppliers.

36 Available at: https://www.bcn.cl/leychile/navegar?idNorma=1173643

37 Available at: https://www.camara.cl/verDoc.aspx?prmID=17852&prmTIPO=INICIATIVA

38 Available at: https://www.camara.cl/verDoc.aspx?prmID=36328&prmTipo=DOCUMENTO_COMISIONDOCUMENTO

39 Available at: https://www.bcn.cl/asesoriasparlamentarias/detalle_documento.html?id=85850

Age determination is also at the heart of these proposals. Bill No. 18,224-18[40] requires operators to implement technically feasible mechanisms proportionate to the risk level of the service, compatible with privacy and the protection of personal data. The project envisages preventing access by people under 14 without verifiable consent of their guardians and requiring age confirmation mechanisms for adolescents between 14 and 17. It also establishes that the data used for this purpose cannot be reused for advertising, commercial profiling, content customization, or other purposes beyond age determination.

At the same time, there appeared other stricter proposals to restrict access based on age. In January 2026, Bill No.18,090-19[41] was presented, "with the purpose of protecting the physical, psychological, social and moral well-being of children and adolescents", it seeks to prohibit access to social media platforms to people under 16 and establishes specific requirements for their suppliers. Other initiatives with different thresholds and mechanisms were presented in the following months.

Another aspect is the incorporation of children and adolescents' protection directly into the general framework of children's rights. Bill No. 18,320-18[42], presented in June 2026, proposes to amend Act No. 21,430 to incorporate specific measures for the protection of children and adolescents in digital environments. The initiative is based on the existing comprehensive protection framework and seeks to complement it against risks arising from the use of the Internet, social media, and other digital technologies.

Updating the criminal response to technology-facilitated forms of violence is also part of the Chilean legislative debate. In May 2025, Bill No. 17,534-07[43] was presented to amend the Criminal Code so as to broaden grooming crime scenarios. The initiative seeks to extend the scope of criminal offense against sexual interactions with children and adolescents through technological means.

40 Available at: https://www.camara.cl/verDoc.aspx?prmID=36328&prmTipo=DOCUMENTO_COMISIONDOCUMENTO

41 Available at: https://obtienearchivo.bcn.cl/obtienearchivo?id=recursoslegales/10221.3/81963/4/20260303_97_18090-19.pdf

42 Available at: https://camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=18993&prmBOLETIN=18320-18

43 Available at: https://www.camara.cl/legislacion/proyectosdeley/tramitacion.aspx?prmID=18174&prmBOLETIN=17534-07

2.5. Colombia

Colombia has the Children and Adolescents Code, approved by Act No. 1,098[44] of 2006, as a general framework for the protection of children and adolescents. During the period under study, the country adopted a series of legislative measures related to the protection of children and adolescents in digital environments.

Act No. 2,489[45] was passed in July 2025 and established provisions for the development of safe and healthy digital environments for children and adolescents. Its purpose is to promote a public policy that articulates actions by the State, families, businesses, non-profit organizations and civil society to prevent online risks, promote healthy habits in the use of technologies and guarantee the rights of children and adolescents. Although the Act is based on the principle of co-liability among different actors, its provisions are mainly concentrated on obligations borne by the State. These include the formulation of prevention, education and awareness-raising policies, the promotion of digital skills, and the creation of monitoring and evaluation mechanisms.

The framework was subsequently regulated by Decree 769 of 2026[46], which set forth the responsibilities of private actors involved in the configuration of digital environments. The decree covers, among others, providers of telecommunications networks and services, digital platforms and services, applications, video games and artificial intelligence systems accessible to children and adolescents in Colombia. Its provisions include security and privacy standards from design and default, as well as due diligence and risk management measures associated with digital services.

In January 2026, Act No. 2,564 was also passed[47], specifically aimed at mental health and different forms of violence in the digital environment. The regulation establishes awareness-raising, prevention, protection and care measures and identifies manifestations of digital violence such as grooming, sextortion, *stalking,* cyberbullying, and happy slapping. Its development stage was marked by the lobby of large technology companies and associations representing their interests, aimed at

44 Available at: https://www.icbf.gov.co/sites/default/files/codigoinfancialey1098.pdf

45 Available at: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=260756

46 Available at: https://www.arielapp.co/es/biblioteca/documento/decreto-769-de-2026-cc36e219

47 Available at: https://dapre.presidencia.gov.co/normativa/normativa/LEY%20No.%202564%20DEL%208%20DE%20ENERO%20DE%202026.pdf

limiting the obligations and liabilities that the project imposed on digital platforms[48]. As a result, provisions seeking to regulate content potentially harmful to the mental health of children and adolescents were amended during the legislative process, and the text finally adopted does not establish material obligations for service providers.

During the period under review, various initiatives were also presented that have not been adopted. Among them is Bill No. 3.06/2025C[49], which seeks to establish measures to prevent, criminalize and punish grooming or abusive digital sexual approaches against children and adolescents. The initiative seeks to incorporate a specific criminal response to these behaviors and complement it with prevention and education measures.

Also, in 2025, Bill No. 394/2025C[50] was presented to regulate the activity of creators of digital content and, in this area, also to establish specific provisions for the protection of the rights of children and adolescents. The initiative includes obligations for digital platforms and other intermediaries related to, among other aspects, the identification, moderation and removal of certain content and to the protection of children and adolescents involved in the creation of content.

Finally, age restrictions on access to social media also gained space in the Colombian Congress. In August 2026, the draft statutory law "Children without networks" (208/2026)[51] was presented, which proposes to establish the age limit of 16 for the creation and maintenance of accounts in social media, age determination mechanisms and safety obligations and responsible design for suppliers.

2.6. Ecuador

Ecuador has had since 2003 the Code of the Child and Adolescents (Act No. 100)[52], which establishes a general framework for the comprehensive protection and guarantee of the rights of children and adolescents throughout the country. Within the period under review, several legislative initiatives were discussed covering issues

48 Olga Lucia Camacho, "El lobby de las Big Tech frena la regulación en Colombia" (Big Tech Lobby stops regulation in Colombia), *La Silla Vacía* (19 May 2026), Available at: https://www.lasillavacia.com/red-de-expertos/red-de-democracia-y-tecnologia/el-lobby-de-las-big-tech-frena-la-regulacion-en-colombia/

49 Available at: https://www.camara.gov.co/ley-contra-el-grooming-067/

50 Available at: https://leyes.senado.gov.co/p-ley/2024-2025/PL%20394-25%20CONTENIDO%20DIGITAL.pdf

51 Available at: https://www.camara.gov.co/ninos-sin-redes/

52 Available at: https://www.igualdad.gob.ec/wp-content/uploads/downloads/2017/11/codigo_ninezyadolescencia.pdf

such as the regulation of social media and Artificial Intelligence, sexual exploitation facilitated by digital technologies and the economic exposure of children and adolescents in digital platforms.

One of these discussions took place within the framework of the construction of general legislation on Artificial Intelligence. The draft Organic Law on Digital Use and Artificial Intelligence for Children and Adolescents[53], presented in 2024, sought to guarantee the safe use of the Internet, social media and digital platforms by children and adolescents, and set forth specific provisions on the development and use of artificial intelligence systems related to this audience. The initiative was later consolidated into two other proposals on the issue — the draft Organic Law on the Regulation and Promotion of Artificial Intelligence[54], and the Bill for the Promotion and Development of Artificial Intelligence[55] — in a general proposal for AI regulation. The report for the first debate was presented in September 2026 and recommended dismissing the initiative, a decision that was finally adopted by the Plenary Session of the National Assembly[56].

Another regulatory line was developed through a proposal to reform the Code on Children and Adolescents[57]. The proposal prohibits access and use of social media to children and adolescents under 15, and establishes that companies and private technology platforms that offer these services shall take the necessary and effective measures to ensure compliance with this restriction, including the establishment of age determination mechanisms.

During the period, a draft Organic Law for the Responsible Use of Social Media was also discussed, aimed at both children and citizens in general. However, in June 2026, the Plenary Session of the National Assembly unanimously decided not to pass it[58]. Among the reasons given by the Legislative Committee there were: possible disproportionate restrictions on freedom of expression and access to information; the excessively

53 Available at: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/99931-proyecto-de-ley-organica-de

54 Available at: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/97303-proyecto-de-ley-organica-de-regulacion

55 Available at: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/98762-proyecto-de-ley-para-el-fomento-y

56 Available at: https://www.lexis.com.ec/noticias/pleno-de-la-asamblea-naciona-archiva-proyecto-de-ley-de-inteligencia-artificial-en-primer-debate

57 Available at: https://www.asambleanacional.gob.ec/es/node/111803

58 Available at: https://www.asambleanacional.gob.ec/es/noticia/117423-pleno-archiva-el-proyecto-de-ley-para-el-uso

punishable nature of the proposal; gaps in the protection of personal data, and the lack of clarity about the institutions responsible for its supervision and punishment. The Committee further considered that the proposal did not adequately incorporate enhanced protection of children and adolescents and the specific risks associated with the use of social media.

Regarding the criminal response to the production and circulation of child sexual abuse material, two legislative initiatives were presented in 2026. In March, the Organic Law Criminalization of Conduct linked to the Sexual Exploitation of Children and Adolescents through Artificial Intelligence and other information technologies[59], which proposed to penalize the creation, simulation, and dissemination and use of sexual material generated or manipulated by AI or other technologies, with sentences of up to 13 years.

In April, a second initiative was presented, later called the Organic Bill for the Prevention, Eradication and Punishment of Crimes related to Child Sexual Abuse Material (Safe Childhood Act)[60]. With a broader scope, it combines preventive and protective measures with criminal and telecommunications law reforms. During its development stage, the use of Artificial Intelligence for the creation of child sexual abuse material, the obligations of Internet service providers and content blocking mechanisms were addressed, among other issues.

Finally, in another area, the draft Organic Law on the Comprehensive Protection of Children and Adolescents in Digital Environments and on their Economic Exposure[61] was presented in July 2026, which addresses the monetization of the image and activity of children and adolescents on digital platforms. Its scope includes activities in which their image, voice, identity, talent or public presence are used to generate income or economic benefits and proposes patrimonial safeguards, due diligence mechanisms and administrative liabilities in the face of economic exploitation and overexposure situations.

2.7. Mexico

Mexico has a general framework for the protection of the rights of children and adolescents established by the General Law on the Rights of Children and Adolescents

59 Available at: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/115385-proyecto-de-ley-organica-reformatoria

60 Available at: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/116939-proyecto-de-ley-organica-para-la

61 Available at: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/118717-proyecto-de-ley-organica-de-proteccion

(LGDNNA, in Spanish)[62] of 2014, which contains provisions related to access and safe use of the Internet, privacy and protection of personal data. During the period under review, several initiatives to broaden this framework were presented in the face of the risks associated to social media and new technology-facilitated forms of violence.

One of the most significant proposals was presented by the Senate on 18 February 2025[63]. The initiative seeks to modify the LGDNNA and the Federal Act on Telecommunications and Broadcasting to prevent access to social media to people under 14, and to request consent from parents or guardians in the case of teenagers between 14 and 17. It also requires age determination and parental control mechanisms, establishes maximum privacy settings by default for adolescent accounts, and considers their personal data as sensitive information. It also assigns platforms the obligation to implement security measures, actively prevent access to inadequate services, and establish complaint and redress mechanisms.

On 9 September 2025, another project was presented seeking to incorporate into LGDNNA the right of children and adolescents to a secure digital environment by adding a section XXI to Article 13[64]. The initiative recognizes the right to participate and develop in digital spaces protected from violence, exploitation, harassment, manipulation, extortion, and exposure to inappropriate content, as well as breaches of privacy. It also stipulates that relevant authorities promote prevention, protection, and digital orientation measures.

That same month, another initiative was presented to reform Articles 66 and 76 of the LGDNNA[65], with emphasis on the risks arising from access to and use of technologies, social media and information systems and on the protection of privacy and personal data. The explanatory statement further develops the need to establish responsibilities for platforms, including age-determination mechanisms, maximum privacy settings by default and content moderation tools.

62 Available at: https://www.gob.mx/cms/uploads/attachment/file/918955/LGDNNA_Ultima_Reforma__27052024.pdf

63 Bill proposing a decree to amend and supplement various provisions of the General Law on the Rights of Children and Adolescents and the Federal Telecommunications and Broadcasting Law. Available at: https://www.senado.gob.mx/66/gaceta_del_senado/2025_02_18/3562

64 Initiative that adds section XXI of Article 13 of the General Law on the Rights of Children and Adolescents, in the area of a safe digital environment. Available at: https://gaceta.diputados.gob.mx/PDF/66/2025/sep/20250909-II-1-1.pdf

65 Initiative that adds several provisions to the General Law on the Rights of Children and Adolescents. Available at: https://gaceta.diputados.gob.mx/PDF/66/2025/sep/20250923-II-1.pdf

On issues of cybersecurity and violence facilitated by technologies, a Bill presented in March 2026 seeks to incorporate a chapter on the right to security and protection in the digital environment into the LGDNNA[66]. Among its provisions, the initiative establishes state obligations to prevent cyberbullying, grooming, and digital sexual exploitation. It provides for warning and reporting mechanisms, as well as cooperation with platforms for the removal of content that violates their rights; and expressly prohibits the creation or dissemination of digitally manipulated content that simulates intimate images of children using Artificial Intelligence.

In March 2026, an initiative to criminalize grooming in the Federal Criminal Code was also presented under the name of "sexual induction through digital deception"[67]. The proposal stipulates the establishment of a bond of trust with a person under 18 through digital media to induce them to generate intimate sexual content or to arrange a sexual encounter, even if these do not actually happen. It provides for increased sentences when generative artificial intelligence, automation, false identities and profiles, or technologies are used to modify appearance or voice. It also establishes preventive measures for digital services, such as security by design, parental controls enabled by default, and priority reporting and blocking channels.

2.8. Panama

Panama has a general framework for the protection of children and adolescents established by Act No. 285 of 2022, which creates the System of Guarantees and Comprehensive Protection of the Rights of Children and Adolescents[68]. In the period under review, the country made progress in updating its criminal legislation against violence facilitated by technologies through Act No. 478 of 4 August 2025[69], which amends and adds provisions to the Criminal Code, the Code of Criminal Procedure and the legislation on international legal assistance in criminal matters.

66 Initiative that adds several provisions to the General Law on the Rights of Children and Adolescents, in the area of cybersecurity and digital protection. Available at: https://gaceta.diputados.gob.mx/PDF/66/2026/mar/20260318-II-6.pdf

67 Initiative that modifies and adds various provisions of the Federal Criminal Code, the General Education Law and the General Law on the Rights of Children and Adolescents, in the area of digital protection and sexual induction through deception. Available at: https://gaceta.diputados.gob.mx/PDF/66/2026/mar/20260318-II-3.pdf

68 Available at: https://www.defensoria.gob.pa/wp-content/uploads/LEY-285-SISTEMA-DE-GARANTIAS-Y-PROTECCION-INTEGRAL-DE-LOS-DERECHOS-DE-LA-NINEZ-Y-LA-ADOLESCENCIA.pdf

69 Available at: https://igc-panama.org/wp-content/uploads/2025/08/Ley-478.-Ciberdelincuencia.pdf

With regard to the protection of children and adolescents, the Act penalizes the production, marketing, dissemination and distribution of child sexual abuse material depicting people under 18 in actual or simulated sexual activities, as well as the possession for their own use of voluntarily acquired material. It also criminalizes contact with children and adolescents for the purpose of committing crimes against their sexual freedom and integrity, including through digital means. The reform also incorporates criminal investigation measures relating to the recording, seizure, retention, and provision of computer data.

As for the legislative debate, Bill No. 426[70] seeks to regulate online services and social media for the digital protection of children and adolescents. As one of the most significant under discussion, the initiative stemmed from citizen participation mechanisms of the National Assembly to be later adopted for legislative debate[71]. The bill establishes specific rules for children and adolescents' access to social media, including prohibiting access to people under 14. In addition, it establishes obligations for providers to implement age determination mechanisms and parental control tools. The proposal also provides for measures to reduce exposure to harmful content and establishes responsibilities for providers for the safety of children and adolescents in their services.

The initiative also incorporates transparency and accountability responsibilities for online service providers and social media that offer services to people in Panama, as well as obligations to collaborate with the competent authorities in the face of possible crimes committed through their services. Thus, the project combines age-based access restrictions with obligations for the online service providers themselves.

2.9. Paraguay

Paraguay has a general framework for the protection of children and adolescents established through Act No. 1,680 of 2001, Code of the Child and Adolescent[72]. During the period under review, the country adopted Act No. 7,549/2025[73], which establishes the obligation to retain data in order to combat the dissemination of child sexual abuse content. The regulation obliges all providers operating in the country under telecommunications legislation to retain for a minimum period of 12 months traffic data

70 Available at: https://sistemas.asamblea.gob.pa/segLegis/viewsPublico/SeguimientoLegislativo

71 "*Estudiantes de Derecho de la USMA promueven proyecto de ley sobre protección digital de menores*" (USMA Law Students Promote Bill on Digital Protection of Minors), *Haciendo Universidad*. March 11, 2026. Available at: https://info.usma.ac.pa/estudiantes-de-derecho-de-la-usma-promueven-proyecto-de-ley-sobre-proteccion-digital-de-menores/

72 Disponível em: https://www.bacn.gov.py/leyes-paraguayas/5261/codigo-de-la-ninez-y-laadolescencia

73 Available at: https://silpy.congreso.gov.py/web/descarga/ley-146014?preview

such as IP address, date and time of connection and disconnection as well as location data, to allow the identification of persons investigated for these crimes. Furthermore, it expressly excludes the content of communications and establishes that access to the data stored may only be requested by the Public Prosecutor's Office through a court order in the context of criminal investigations covered by the regulation.

During 2026, the debate on broader children and adolescents' protection frameworks in digital environments and restrictions on access to social media gained greater relevance in Paraguay. These discussions stem from Act No. 5,653/2016, on the Protection of Children and Adolescents against Harmful Internet Content[74], regulated by Decree No. 8,098/22[75], which obliges Internet service providers to provide mandatory and free software with content blocking systems. In addition, it creates the National Observatory for the Protection of the Rights of Children and Adolescents on the Internet, which has among its functions "to plan, present and implement the annual plan for the protection and promotion of the rights of children and adolescents on the Internet".

In March 2026, the Senate announced a public hearing on a bill amending and expanding Act No. 5,653/2016 to include, among other providers' obligations, the provision of parental control and digital security tools that can operate at the network or operating system level. It also includes measures to prevent children and adolescents from accessing platforms, services or functionalities that promote intensive use patterns or that are potentially harmful to their physical and mental well-being. In the same month, the Commission on Science, Technology, Innovation and Future reported that its agenda included the analysis of a proposal to regulate or prohibit the use of social media by people under 16[76].

In addition to the legislative proposals under way, during 2026, a process promoted by the Ministry of Children and Adolescents, the Ministry of Information and Communication Technologies and other players was added to develop a framework for the protection of children and adolescents in digital environments. Although the proposal has not yet been made public, official information indicates that the proposal would be aimed at combining digital education, family participation and measures against risks associated with digital platforms, cybercrimes and content generated by Artificial Intelligence[77].

74 Available at: https://baselegal.com.py/docs/4870f1b5-5c8a-11ed-be69-525400343722

75 Available at: https://baselegal.com.py/docs/ec914bf2-5c8c-11ed-be69-525400343722

76 Available at: https://www.senado.gov.py/index.php/menu-dircom/sub-menu-noticias-generales/analizaran-propuesta-legislativa-sobre-uso-de-redes-sociales-en-menores-2026-03-05-15-48-52.html

77 Available at: https://www.ip.gov.py/ip/2026/05/26/paraguay-impulsa-proyecto-de-ley-que-apunta-a-establecer-entornos-digitales-seguros-para-ninos-y-adolescentes/

From the criminal perspective, in November 2024, Bill D-2481664[78] was presented with the aim of establishing a specific framework for the prevention, detection, punishment and eradication of grooming.

2.10. Peru

Peru counts with the Children and Adolescents Code, approved by Act No. 27,337 of 2000[79], as a general framework for the protection of children and adolescents. Besides, in 2014, they passed Act No. 30,254 on the Promotion of Safe and Responsible Use of Information and Communication Technologies by Children and Adolescents[80]. Still, the debate on the protection of children and adolescents in digital environments grew during the period under review.

One of the main legislative amendments adopted was in the criminal field. It is Act No. 32,314[81] of 2025, which amends the Criminal Code and Act No. 30,096, on Computer-related Crimes, which includes the use of AI to commit such crimes. Among other amendments, the Act amended Article 129-M of the Criminal Code, on child sexual abuse materials, to specifically include *deepfakes* and other AI-generated multimedia content.

Other legislative initiatives still under discussion seek to establish broader protection frameworks. Among them, Bill No. 10,880/2024-CR[82], which — among other measures — included provisions to limit access to mobile devices and social media by minors, stands out. As for social media, it prohibited the creation of accounts by children under 16.

The initial version of the project was the target of criticism due to the inclusion of biometric identification measures to verify age, restrictions and obligations related to VPN services and technical measures to control and block content. The proposal was amended during its debate. In November 2025, the Women and Family Committee adopted a substitute text[83] focused on establishing principles such as best interests, evolving autonomy, co-responsibility among the State, families and technological

78 Available at: https://silpy.congreso.gov.py/web/expediente/138173

79 Available at: https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/3366849-27337

80 Available at: https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/292146-30254

81 Available at: https://img.lpderecho.pe/wp-content/uploads/2025/04/Ley-32314-LPDerecho.pdf

82 Available at: https://vlex.com.pe/vid/proyecto-ley-n-10880-1076983759

83 Available at: https://comunicaciones.congreso.gob.pe/despacho-informa/comision-de-mujer-y-familia-aprueba-proyecto-que-garantiza-entornos-digitales-seguros-para-ninos-y-adolescentes/

companies, as well as technological and network neutrality. It also includes measures to reduce exposure to harmful content and prevent forms of violence such as cyberbullying, grooming and sextortion.

The project continued to move forward throughout 2026. In February, the Health and Population Committee passed another decision on Bills No. 8017/2023-CR, 10880/2024-CR and 13453/2025-CR and placed greater emphasis on the promotion and prevention of mental health of children and adolescents in digital environments[84]. The text adopted a preventive approach, with responsibilities for the State, educational institutions and families and explicit references to the best interests, evolving development and rights approach.

Finally, Bill No. 00498/2026-2031-CD[85] took these initiatives as background, maintaining the prohibition on the creation of personal accounts on social media by children under 16. The proposal requires service providers to take reasonable and proportionate age determination measures, but does not prescribe biometric identification or set specific obligations on VPN services such as the original version. Furthermore, it limits the use of the data obtained for age verification, and stipulates its elimination at the end of the process, except when there is a legal obligation of conservation. For teens aged 16 and 17, the law sets specific criteria for their social media accounts.

2.11. Uruguay

Uruguay has the Children and Adolescents Code[86] of 2004, as a general framework for the protection of children and adolescents. During the period under review, the country approved amendments to its criminal legislation, applicable to behaviors in digital environments with implications in childhoods.

Act No. 20,327 of 2024[87] incorporated new offenses and aggravating factors into the Criminal Code, criminalizing "telematic harassment" and establishing as an aggravating circumstance that the conduct is carried out against children and adolescents. It also incorporated specific aggravating factors to the offense under Article 277 bis of the

84 Available at: https://comunicaciones.congreso.gob.pe/noticias/aprueba-dictamenes-para-proteger-la-salud-mental-infantil-y-uso-seguro-de-internet/

85 Available at: https://img.lpderecho.pe/wp-content/uploads/2026/10/PL-00498-2026-2031-CD-LP-Derecho.pdf

86 Available at: https://www.impo.com.uy/bases/codigo-ninez-adolescencia/17823-2004

87 Available at: https://www.impo.com.uy/bases/leyes-originales/20327-2024

Criminal Code, related to contact with children by means of technologies for sexual purposes, including cases involving coercion, intimidation or deception; a relationship of kinship or affinity or when contact occurs with a person under the age of 13. Under this Act, in the case of data breach offenses, the fact that the victim is a child or adolescent also represents an aggravating factor.

Still in the criminal field, the Bill on the dissemination of sexual content produced using AI (File 691/2025)[88] proposes to extend the offense of the non-consensual disclosure of intimate or sexual images or recordings to simulated content using artificial intelligence, digital editing or other technologies. Among other provisions, it is expressly stated that the authorization granted by children and adolescents for the dissemination of these materials is invalid.

Age restrictions on access to social media also entered the legislative agenda during 2026. In July, the Bill on the Use of Social Media by Minors (File 2979/2026) was presented[89], which seeks to establish 15 as the minimum age for the creation of social media accounts. The initiative states that platforms shall be responsible for the adoption of mechanisms to prevent the creation of accounts by people below the threshold and provides for a system of control and sanctions.

These projects are developed in parallel with a broader discussion process on the protection of children and adolescents' rights in digital environments. During 2026, the Parliament, together with public bodies and other institutions, promoted discussion spaces and a public consultation on children, digital environments and artificial intelligence[90]. The process addressed issues such as platform responsibilities, privacy and data protection, digital violence, age determination mechanisms and children and adolescent participation, with the aim of generating inputs for future public policies and legislative initiatives. By the end of the period under review, however, this process had not yet resulted in the submission of a bill.

88 Available at: https://documentos.diputados.gub.uy/docs/L50/Repartid/R0346.pdf

89 Available at: https://propaci.parlamento.gub.uy/sipfront/servlet/com.sipfront.unproyectoley?174431

90 Available at: https://www.anep.edu.uy/uruguay-avanza-hacia-ley-proteccion-ninas-ninos-adolescentes-en-entornos-digitales



03

MAIN REGULATORY TRENDS IN THE REGION

03

3. MAIN REGULATORY TRENDS IN THE REGION

The mapping allows for the identification of some trends in the legislative responses that have been adopted or discussed in Latin America. These trends are not mutually exclusive. On the contrary, in several countries there are criminal reforms, proposals for age restrictions, obligations aimed at platforms and new regulations on other issues such as the economic activities developed by children and adolescents in digital environments. By analyzing them all together, we can identify which are the main issues that have mobilized recent legislative activity, as well as where State responses are concentrating.

3.1. Expansion of Criminal Law Responses and Surveillance

Criminal law continues to be at the heart of legislative responses in the region, especially in the face of technology-facilitated sexual violence and exploitation. This is not a new trend. The criminalization of grooming and behavior related to child sexual abuse material is one of the regional precedents in the protection of children and adolescents. Over the decades, criminal responses have raised tensions between expanding state surveillance powers and guaranteeing rights in digital environments, as illustrated by the debates over restrictions on encryption to facilitate crime investigation. However, in the period analyzed we have identified a new stage of updating and expanding these frameworks.

Among the regulations approved, Brazil adopted Act No. 15,487/2026[91], extending the criminal treatment of several forms of sexual violence against children and adolescents; Bolivia adopted Act No. 1,636/2025[92], which incorporated and updated criminal offenses related to sexual violence in digital settings and expanded investigative instruments; Panama adopted Act No. 478/2025[93], which amended its legislation to incorporate provisions applicable to forms of digital sexual violence against children and adolescents; Paraguay adopted Act No. 7,549/2025[94], which establishes data retention obligations for the investigation of offenses related to child sexual abuse material and related punishable acts; and Uruguay adopted Act No. 20,327/2024[95],

91 Available at: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15487.htm

92 Available at: https://www.lexivox.org/norms/BO-L-N1636.xhtml

93 Available at: https://igc-panama.org/wp-content/uploads/2025/08/Ley-478.-Ciberdelincuencia.pdf

94 Available at: https://silpy.congreso.gov.py/web/ley/146014

95 Available at: https://www.impo.com.uy/bases/leyes-originales/20327-2024

which introduced new offenses and aggravating factors for certain behaviors carried out using technologies. In addition to these reforms, there are numerous bills still under discussion. The updating of responses to grooming and the production, possession and dissemination of child sexual abuse material is prominent in this set of initiatives.

Despite their popularity, criminalizing measures such as the creation of new offenses or increased sentences do not, on their own, guarantee greater capacity for prevention, investigation, or protection of victims. This limit is particularly relevant in Latin America, where the enforcement of existing regulations must deal with problems related to resources, specialization, and technical skills to produce and analyze digital evidence. A recent study on the case of Brazil shows that, according to professionals in the area, the gaps in the protection of children and adolescents are primarily in the implementation of existing frameworks and include limited resources, lack of clarity on the responsibilities of different actors and insufficient multisectoral coordination[96].

On the other hand, the analysis shows that the tightening of the criminal response is accompanied, in several of the initiatives analyzed, by an expansion of surveillance capacities. The creation of offenses and aggravating factors is linked to new state powers of access to information, covert investigation techniques and obligations to preserve, monitor and deliver data on the part of suppliers. Thus, the punitive impulse can also extend control over the digital activities of people who are not being investigated, with impacts on privacy and communications security.

In Bolivia, Act No. 1,636/2025[97] allows the use of undercover agents in digital environments when the means of evidence are non-existent or insufficient, through a substantiated request from the Public Prosecutor's Office and judicial authorization. In Brazil, Act No. 15,487/2026[98] extends the crimes that may be investigated through police infiltration on the Internet and enables automated patrolling of public digital spaces without prior judicial authorization. In situations of flagrancy or risk to the life or physical integrity of children and adolescents, it also allows to directly request connection records or registration data from suppliers, with subsequent judicial control. It should be noted that such measures carry serious risks to the exercise of

96 Available at: https://www.unicef.org/brazil/media/37356/file/DH%20Brazil%20Report%20(pt)%20FINAL

97 Available at: https://www.lexivox.org/norms/BO-L-N1636.xhtml

98 Available at: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15487.htm

human rights in digital environments[99]. The intrusion that these actions may involve requires the delimitation of their scope, duration and conditions of use, the protection of the information of third parties and the establishment of guarantees against the provocation of crimes and the exposure or revictimization of children and adolescents.

Another dimension of this expansion is the retention of data of innocent people. In Paraguay, Act No. 7,549/2025[100] requires that identification and connection data of users be kept for at least 12 months. Although it excludes the content of communications and requires a court order to access records, the retention obligation is applied in general. Judicial control over access does not eliminate risks, for example, of misuse or leakage. While the Paraguayan case reflects a broader trend in the region[101], the measure has attracted criticism from civil society organizations, especially when protection obligations shift surveillance functions to the platforms themselves. TEDIC warned that the monitoring and detection provisions provided for in the Paraguayan grooming bill could affect privacy and encryption of communications and violate fundamental rights in the digital environment[102].

The treatment of anonymization tools raises another concern. In Brazil, Act No. 15,487/2026 increases sentences, by one and two thirds, when certain crimes are committed using techniques of concealment or anonymization of digital identifiers to prevent or hinder the identification of the perpetrator. The measure has been criticized by several civil society organizations for introducing into the national legal system a differentiated treatment of technologies developed to protect the privacy and security of people, such as VPNs, despite an exception to legitimate uses[103]. It should be

99 See Derechos Digitales (Digital Rights), *Perfilamiento en redes sociales y ciberpatrullaje como nuevas modalidades de vigilancia masiva desplegada por los Estado: casos relevantes en América Latina (Social Media Profiling and Cyber Patrolling as New Modes of Mass Surveillance deployed by the State: Relevant Cases in Latin America)*. (2024) Available at: https://www.derechosdigitales.org/wp-content/uploads/Informe-RELE-vigilancia-masiva_cerrado.pdf

100 Available at: https://silpy.congreso.gov.py/web/ley/146014

101 See Díaz, M., *Retención de datos y registro de teléfonos móviles: Chile en el contexto Latinoamericano (Data retention and mobile phones record: Chile in the Latin American Context)*. (Derechos Digitales, 2017). Available at: https://www.derechosdigitales.org/wp-content/uploads/informe-marianne-retencion-de-datos.pdf

102 "Ley de protección contra el Grooming: Cuidar a los niños, niñas y adolescentes, sin vulnerar los derechos digitales" (Grooming Protection Act: Caring for children and adolescents, without violating digital rights), *TEDIC*. October 29, 2025. Available at: https://www.tedic.org/ley-de-proteccion-contra-el-grooming-cuidar-a-los-ninos-ninas-y-adolescentes-sin-vulnerar-los-derechos-digitales/

103 Available at: https://www.isoc.org.br/uploads/download/260

emphasized that the difficulty in identifying the perpetrator does not in itself amount to a greater injury or risk to the victim. Using security tools as a basis for aggravation can stigmatize their use and discourage necessary protective practices for children and adolescents, journalists, human rights defenders and victims of violence. It may also lead to similar measures in other contexts.

The severity of the crimes under investigation does not exempt States from justifying the need and proportionality of the measures taken. This requires demonstrating their contribution to the objective pursued, examining less intrusive alternatives and assessing their impact on the rights of the people concerned, including the children and adolescents themselves. Protection of this group shall not be used as an automatic justification to broaden access to personal data, to standardize mass monitoring or to weaken ciphering or anonymity. Every interference must be clearly provided, must be limited to what is strictly necessary, and must count with independent oversight and effective means to challenge abuses. Privacy and digital security are protective conditions, also for those who need to seek help, report violence or communicate confidentially.

The expansion of the criminal response must also be considered in the context of the structural problems that characterize the criminal justice and prison systems of the region. The Inter-American Commission on Human Rights (IACHR) has repeatedly pointed to problems such as the excessive use of pretrial detention, overcrowding, poor conditions of detention, high levels of violence, and insufficient basic services. All of these, added to the limitations to ensure adequate conditions of social reintegration[104].

These conditions do not constitute an argument to stop investigating and punishing serious forms of violence against children and adolescents. They do raise the need to critically consider responses that increasingly focus protection policies on the expansion of crime types and prison sentences, without necessarily strengthening, with such measures, the institutional capacities to prevent these forms of violence, investigate them properly and protect victims.

Therefore, the criminal response and the powers to investigate should be integrated in a protection policy that includes accessible reporting channels, psychological and social care, assistance to victims and their families, prevention, education and guarantees to avoid revictimization. The effectiveness of this policy cannot be measured solely by the

104 Inter-American Commission on Human Rights. *Annual Report 2025*. (Washington, 2025). Available at: https://www.oas.org/es/cidh/docs/anual/2025/IA2025_SPA.pdf; Inter-American Commission on Human Rights. *Argentina: Uso de la prisión preventiva en la provincia de Córdoba (Argentina: Use of pretrial detention in the province of Córdoba)*. July 25, 2025. Available at: https://www.oas.org/es/cidh/sesiones/audiencia.asp?Hearing=3845.

severity of the sentences or the amount of information available to the authorities, but by its ability to reduce violence, care for those who suffer it and guarantee their rights without causing further violations.

3.2. Age Restrictions and the Expansion of Age Determination

Another particularly visible trend is the proliferation of proposals that seek to establish minimum ages to access social media. Although none of the access ban initiatives identified in the region had been passed as law at the close of the period under review, this model has quickly gained space on Latin American legislative agendas.

With different formulations, such proposals were identified in Argentina, Brazil, Chile, Colombia, Ecuador, Panama, Paraguay and Uruguay. Thresholds are not uniform: The initiatives analyzed set limits ranging from 13 to 16 and, in some cases, combine minimum ages with parental authorization for certain age groups. In Brazil, although there have not been access ban initiatives, Digital ECA requires accounts of children under 16 to be linked to the account of a legally responsible person.

As for ban initiatives, the speed with which they circulate between countries contrasts with the still limited evidence on their implications, particularly in Latin American contexts. Evaluating these measures requires considering both their ability to reduce exposure to certain risks and the specific ways in which children and adolescents access the Internet in the region. Socioeconomic conditions, territorial inequalities, availability of devices and possibilities for family support affect the ways of accessing and using technologies. Regional evidence further reinforces that problematic uses result from multiple factors, including time and intensity of use, early access, well-being, family dynamics and socialization contexts[105]. Therefore, models developed in other contexts should not simply be reproduced without evidence of their potential different effects in Latin America.

Age restrictions also introduce a second regulatory issue: In order to prevent a person of a certain age from using a service, it is necessary to establish some mechanism to determine their age. Therefore, proposals for prohibition or restriction are generally accompanied by obligations to verify or estimate age. However, the relationship between age restrictions and age determination obligations is not uniform.

105 Matías Dodel, Ariel Tófalo, Rolando Pérez, David Torres and Jazmín Mazó Torrico. *Usos problemáticos de dispositivos digitales en la infancia y adolescencia en América Latina: desigualdad, bienestar y apoyo familia (Problematic uses of digital devices in childhood and adolescence in Latin America: Inequality, well-being and family support)*. ECLAC. (Santiago, 2026). Available at: https://www.cepal.org/es/publicaciones/90361-usos-problematicos-dispositivos-digitales-la-infancia-adolescencia-america

Age determination includes different procedures used to verify or estimate a person's age or age range. Verification uses official documents or other accredited sources to verify age, without necessarily revealing the full identity to the service. Estimating, on the other hand, infers a likely age by analyzing physical characteristics, such as facial appearance, or behavioral signals, such as device interactions, usage patterns, and activity on a platform[106]. This distinction is relevant because the methods require different data and present different margins of error and risks to rights.

The mechanisms available to determine the age of users range from the presentation or verification of identity documents to age estimation systems based on biometrics or use patterns. The initiatives analyzed do not always determine which technology should be used to meet determination obligations. Some, however, incorporate specific safeguards to reduce the amount of personal data shared. Argentine Bill No. 2.733-D-2026[107], for instance, also provides for a State technology that would inform platforms only if the person meets the applicable age threshold, without transferring data such as ID number, address, biometric image or exact date of birth.

Regardless of the method used, age determination is a clear example of how a regulation aimed at the protection of children and adolescents can alter the infrastructure and conditions of Internet access for all people. This is because, in order to distinguish who meets an age threshold, it is necessary to collect information also from adults who are not subject to the legislation. As a result, access to digital services, which nowadays are not necessarily mediated by age or identity accreditation, is subject to requirements that have critical implications for digital participation, privacy, freedom of expression and access to information. It is worth mentioning that the violation of these rights also affects the children they seek to protect. Thus, the measure can weaken the very purpose of the protection policy.

The problem is not the loss of absolute anonymity that may now be guaranteed. Most connections and devices already generate identifiers and logs that can allow tracking activities and, under certain conditions, associate them with a person. However, leaving traces does not amount to having to identify themselves, nor is true that every activity is

106 OECD: "AGE ASSURANCE PRACTICES OF 50 ONLINE SERVICES USED BY CHILDREN". (Paris. June, 2025). Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/age-assurance-practices-of-50-online-services-used-by-children_3fbe5e92/a19853ab-en.pdf

107 Available at: https://www.hcdn.gob.ar/comisiones/permanentes/ceducacion/proyecto.html?exp=2733-D-2026

directly linked to a credited identity. Access to identifying information must be subject to safeguards and, as a general rule, judicial authorization. In addition, identification must be given in specific cases and in the form determined by law, when strictly necessary for the purposes sought and proportionately. Generalized age testing reverses the logic of identification as an exceptional measure. A generalization of age checks as a daily condition of access to the Internet is not acceptable.

Not all age determination systems produce this association in the same way. A credential that only certifies compliance with a threshold can reduce the information received by the platform. However, limiting shared data does not alone resolve who knows the identity when issuing the credential, whether checks can be linked between services or if there are records that allow reconstructing where and when it was used. Safeguards should therefore examine the functioning of the entire system and ensure that age checks do not become a navigation tracking infrastructure.

Within this transformation, each method poses certain specific risks[108]. Document-based procedures may exclude those who do not have the supported documentation or are unable to complete the verification, for example. Those that analyze facial images require processing sensitive data, while behavioral-based estimation can foster more intensive analysis of digital activity. These methods also pose difficulties when several people use the same device, a relevant practice in contexts of inequality of access in places such as Latin America. If the estimation is based on the activity of the device or a shared account, you may combine usage patterns of different family members and attribute to one person the age inferred from the behavior of another. This can both unjustifiably restrict adult access and prevent child protection from being activated. On top of this, the results of the estimate are probabilistic. Technical evaluations of facial estimation systems have found differences in performance according to age, sex, region of origin and image quality. These errors can result in unjustified exclusions or the need for more intrusive additional checks.

The incorporation of specialized providers to perform these services also introduces new actors and data flows. Without safeguards, the information obtained may be retained, combined with other records or reused for profiling, advertising and other commercial or surveillance purposes. This exploitation constitutes an additional risk, but the central problem persists even when the data is not marketed. Guarantees of minimization, separation of purposes and deletion of data are essential, but must be accompanied by a prior assessment of whether the requirement is necessary and proportionate for each service.

108 Marina Meira. "Por que aplicar a verificação de idade na internet é tão difícil" (Why is implementing age verification online so difficult?), *UOL Tilt*. October 7, 2025. Available at: https://www.uol.com.br/tilt/analises/ultimas-noticias/2025/10/07/por-que-aplicar-a-verificacao-de-idade-na-internet-e-tao-dificil.htm

The consideration of these risks is not uniform in the legal initiatives analyzed. Some include specific safeguards, such as Argentine Bill No. 2733-D-2026[109], which limits the information communicated to platforms to the fulfillment of the age threshold, or the Peruvian Bill No. 00498/2026-2031-CD[110], which requires an alternative to official documents and restricts the use and retention of the data obtained. Others establish age-determination obligations without sufficiently specifying the limits of data processing or the guarantees required of the providers involved[111]. The scope of the requirement also varies. In Brazil, the Act and its regulatory decree[112] contemplate differentiated obligations according to the characteristics of the services and contents, rather than indiscriminately requiring the determination of age to access any digital space. These differences are relevant, although both the delimitation of the services subject to verification and the data safeguards should be assessed in the light of the necessity and proportionality of the measure and its effects on rights.

These problems are not unique to Latin America, although regional conditions may intensify them. Inequalities in access to digital documents, devices and services can make checks difficult and exacerbate their exclusive effects. In addition, the articulation of these mechanisms with State and private identification infrastructures requires particular attention to controls over access, linking, and reuse of data. The regional assessment should consider both these conditions and the broader change in making age determination a standard requirement for information, communication, and participation on the Internet.

3.3. From Restricting Access to Regulating Digital Services

At the same time, the mapping shows another regulatory trend: The adoption or discussion of broader frameworks that assign part of the responsibility to the companies that design and operate digital products and services. Examples in the region include the Brazilian and Colombian case, to different extents, and the projects discussed in Argentina, Chile, Mexico, Panama and Peru.

109 Available at: https://www.hcdn.gob.ar/comisiones/permanentes/ceducacion/proyecto.html?exp=2733-D-2026

110 Available at: https://img.lpderecho.pe/wp-content/uploads/2026/10/PL-00498-2026-2031-CD-LP-Derecho.pdf

111 For example, Brazilian Bill No. 2387/2025, and the original version of Peruvian Bill No. 10880/2024-CR.

112 Available at: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm; https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm

These initiatives broaden the scope of regulation. In addition to the conditions of access of children and adolescents to certain services, they incorporate issues such as privacy and security by design, protective configurations by default, recommendation systems, dark patterns, design aimed at maximizing the time spent, behavioral advertising, profiling and processing of personal data. This approach recognizes that certain risks depend not only on user behavior, but also on product characteristics and the business models that underpin them. It allows, therefore, to guide intervention toward corporate decisions that generate or intensify these risks, and to broaden the debate beyond the opposition between allowing or prohibiting access to social media. Both approaches can coexist, as shown by the Brazilian Digital ECA, which combines obligations on the functioning of services with limitations on the creation of individual accounts by children under the age of 16.

At the same time, the experiences analyzed show tensions that generated questions from civil society organizations regarding excessively broad obligations of monitoring, moderation, identification of users or removal of content, which can affect privacy, freedom of expression, access to information and security of communications[113].

The challenge of these models is, therefore, to move towards companies' responsibilities over the conditions of the digital environments they design and run, without transforming the protection of children and adolescents into a general authorization to broaden mechanisms of surveillance, content control and data collection. The regulation of design and business models opens an important agenda for the region, but requires that obligations be specific, proportionate to the risks and accompanied by clear safeguards for the rights of children and adolescents, as well as other users.

Its implementation also requires building and strengthening an institution capable of overseeing compliance with these obligations. It is not enough to assign new powers to the authorities if they lack independence from political and business interests, expertise, and adequate financial and human resources. Oversight shall have the power to obtain information from companies, evaluate their practices and demand

113 "ISOC Chile presents Internet impact assessment on Bill for the protection of children and adolescents in digital environments", *ISOC CHILE.* August 31, 2026. Available at: https://www.isoc.cl/?p=5946; "Proteger a niños, niñas y adolescentes sin sacrificar derechos: lo que preocupa del decreto que reglamenta la Ley 2489 de 2025", *Fundación Karisma*. May 19, 2026. Available at: https://blog.karisma.org.co/proteger-a-ninos-ninas-y-adolescentes-sin-sacrificar-derechos-lo-que-preocupa-del-decreto-que-reglamenta-la-ley-2489-de-2025/; Rubiela Gaspar. "Hacia una Internet Segura: regular sin censurar a infancias y adolescencias" (Towards a Safe Internet: Regulate without censoring childhood and adolescence), *Hiperderecho*. Available at: https://hiperderecho.org/2025/06/hacia-una-internet-segura-regular-sin-censurar-a-infancias-y-adolescencias/

corrective actions, along with coordination mechanisms among authorities in charge of data protection, consumption and rights of children and adolescents. Transparency, accountability and the participation of civil society and children and adolescents themselves must accompany this institution-building, so that protection does not depend exclusively on the evaluations and decisions of regulated companies.

3.4. Two Emerging Agendas: Participation in Digital Economic Activities and Artificial Intelligence

Beyond the trends mentioned above, we have identified two agendas that are gaining more specific ground in the region. The first concerns the participation of children and adolescents in digital economic activities. The second relates to the implications of Artificial Intelligence on their rights. Although both relate to previous problems, they raise new questions about the responsibilities of companies, families and authorities.

The involvement of children and adolescents as digital content creators raises specific questions about the commercial exploitation of their image and voice, production conditions, revenue management and the responsibilities of families, platforms and advertisers. During the period analyzed, this issue received regulatory attention in Brazil, where regulatory decree of the ECA Digital[114] requires prior judicial authorization for certain forms of habitual exploitation of the image or routine of children in monetized or promoted content; in Ecuador, where a project presented in 2026 proposes patrimonial safeguards and due diligence mechanisms against economic exploitation and over-exposure of children and adolescents[115]; and in Colombia, where Bill No. 394/2025C[116] combines the protection of children and adolescents in digital environments with the regulation of content creators.

Although incipient in the region, this agenda has an international background. France, for example, adopted in 2020 specific legislation on the commercial exploitation of the image of persons under 16 on online platforms[117], extending protections traditionally associated with child labor in audiovisual sectors to certain activities carried out on digital platforms and establishing specific rules for income generation and content dissemination.

114 Available at: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm

115 Available at: https://www.asambleanacional.gob.ec/es/noticia/118087-luigi-garcia-impulsa-ley-para-proteger-ninas-ninos-y

116 Available at: https://leyes.senado.gov.co/p-ley/2024-2025/PL%20394-25%20CONTENIDO%20DIGITAL.pdf

117 Available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042439054

The emergence of these initiatives suggests a further expansion of the digital protection agenda. Children and adolescents participate in the platforms as users exposed to content and interactions, but also as content producers and actors in a digital economy capable of generating value from their image, activity, and data. The challenge is to ensure that this participation respects their rights, including the conditions of production, the protection of their income, privacy, and ability to decide on the exposure of their image.

The second emerging agenda concerns Artificial Intelligence. So far, much of the responses identified focus on their use to facilitate forms of sexual violence. Brazil, through Act No.15,487/2026[118], and Peru, through Act No. 32,314/2025[119], expressly incorporated content produced or manipulated with AI into their provisions on child sexual abuse material. In Mexico[120] and Ecuador[121], projects aimed at punishing sexual representations generated through these technologies or their use to facilitate deception and contact with children for sexual purposes were also identified. These initiatives show the adaptation of criminal frameworks to new forms of production and circulation of content and interaction with victims.

However, the AI and the children and adolescent rights agenda goes beyond the criminal response. In Ecuador, the draft Organic Law on Digital Use and Artificial Intelligence for Children and Adolescents[122] proposes a specific framework that includes transparency, accountability, data protection, security and equitable access. Its inclusion in the mapping allows to identify a line of discussion that also covers the conditions of design, development and use of AI systems that may affect children and adolescents.

This expansion is relevant because the impacts of AI on children and adolescents exceed the generation of sexual content. They also need to examine how these systems interfere in learning, access to information, interactions, and decisions that affect them, as well as the risks of discrimination, profiling, and commercial exploitation of

118 Available at: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15487.htm

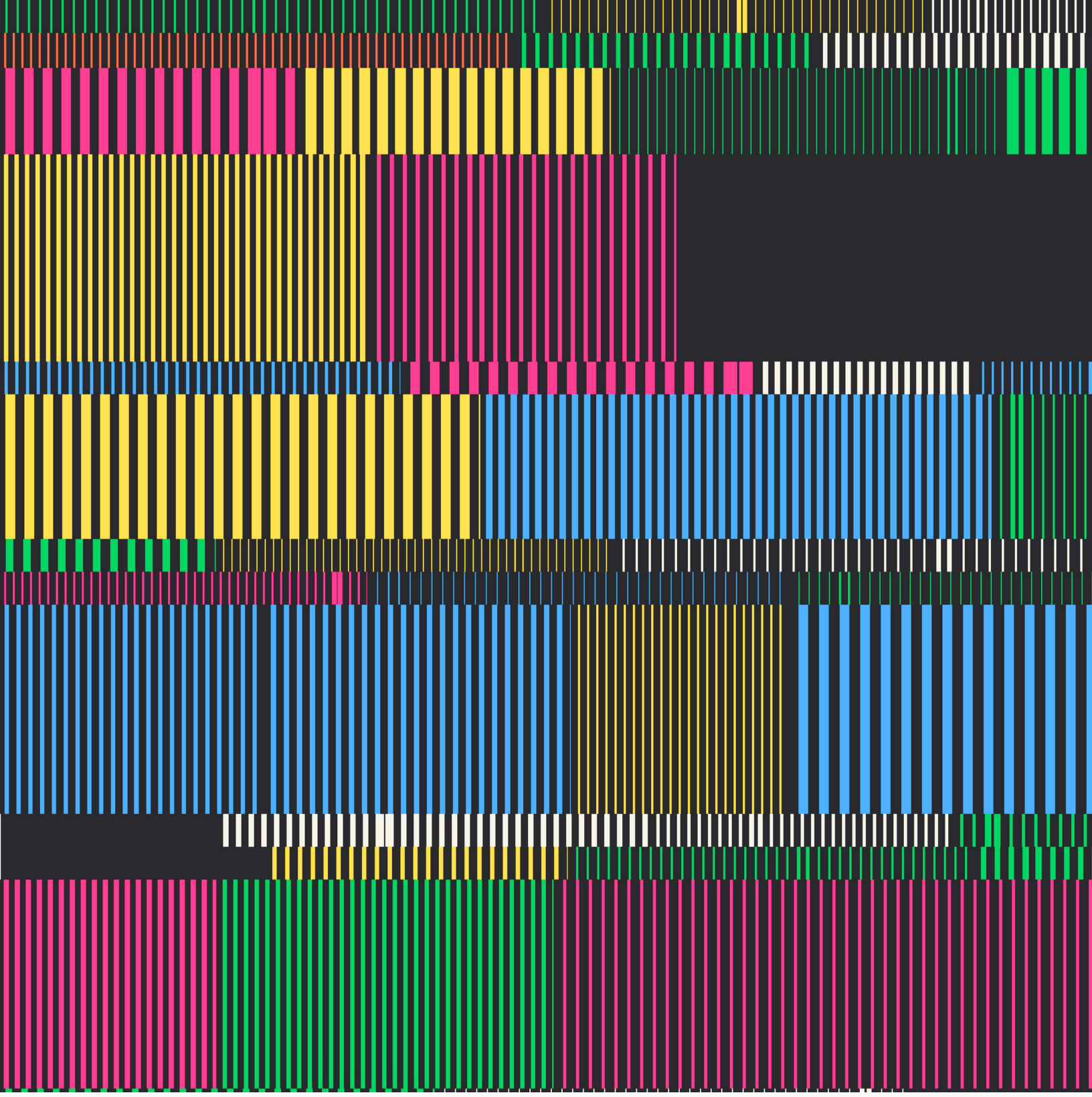
119 Available at: https://img.lpderecho.pe/wp-content/uploads/2025/04/Ley-32314-LPDerecho.pdf

120 Initiative that modifies and adds various provisions of the Federal Criminal Code, the General Education Law and the General Law on the Rights of Children and Adolescents, in the area of digital protection and sexual induction through deception. Available at: https://gaceta.diputados.gob.mx/PDF/66/2026/mar/20260318-II-3.pdf

121 Available at: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/115385-proyecto-de-ley-organica-reformatoria

122 Available at: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/101492-proyecto-de-ley-organica-de

their data. A comprehensive protection agenda should address these dimensions and establish responsibilities throughout the development and use of the systems, with guarantees of transparency, oversight, and participation of children and adolescents. Otherwise, attention to the most visible manifestations of violence may leave out of the debate other effects on their rights.



04

FINAL CONSIDERATIONS

04

4. FINAL CONSIDERATIONS

The analysis carried out in this report evidences the growing prominence of the protection of children and adolescents in digital environments in the regulatory agendas of Latin America. In a relatively short period of time, several countries passed new Acts, amended existing frameworks or started to discuss initiatives specifically focused on the relationship between children and adolescents and digital technologies. Although these responses are based on legitimate concerns about risks and forms of violence that require public attention, the mapping also shows considerable diversity in the problems identified and, in the solutions, proposed.

At the same time, this agenda has implications that go beyond the protection of children and adolescents. Some of the measures analyzed directly intervene on the way in which digital services are designed and run, the conditions for accessing them, the data to be collected from users and the rules applicable to the circulation and moderation of content. In this sense, regulatory decisions taken in the name of the protection of children and adolescents are, as have historically been, part of broader debates on Internet governance[123] and can have an impact on the exercise of human rights by the whole population.

The protection of children and adolescents cannot be considered in isolation from other rights recognized by the Convention on the Rights of the Child. Children and adolescents have, among others, the right to privacy, to seek and receive information, to express themselves, to participate and to associate, and to exercise increasing levels of autonomy in accordance with the development of their abilities. The Committee on the Rights of the Child has precisely stressed that these rights continue to apply in digital environments. Regulatory measures must therefore protect against harm and preserve the conditions for the exercise of those rights.

However, human rights analysis also does not end in the rights of children and adolescents. Several of the measures identified in this report require technical or regulatory modifications that would reach all Internet users. Age determination provides a particularly clear example: an obligation created to distinguish who can access a particular service may lead to the introduction of age verification or estimation mechanisms on a much larger scale. It may even change the conditions of access also for adults. Similarly, obligations related to content detection and moderation may affect freedom of expression and access to information of other users, while measures that

123 Jovan Kurbalija. *An Introduction to Internet Governance*. (DiploFoundation, 2016). Available at: https://dspace.diplomacy.edu/items/be5449e5-a1c3-4e42-bf53-2ce6c1b0cc49

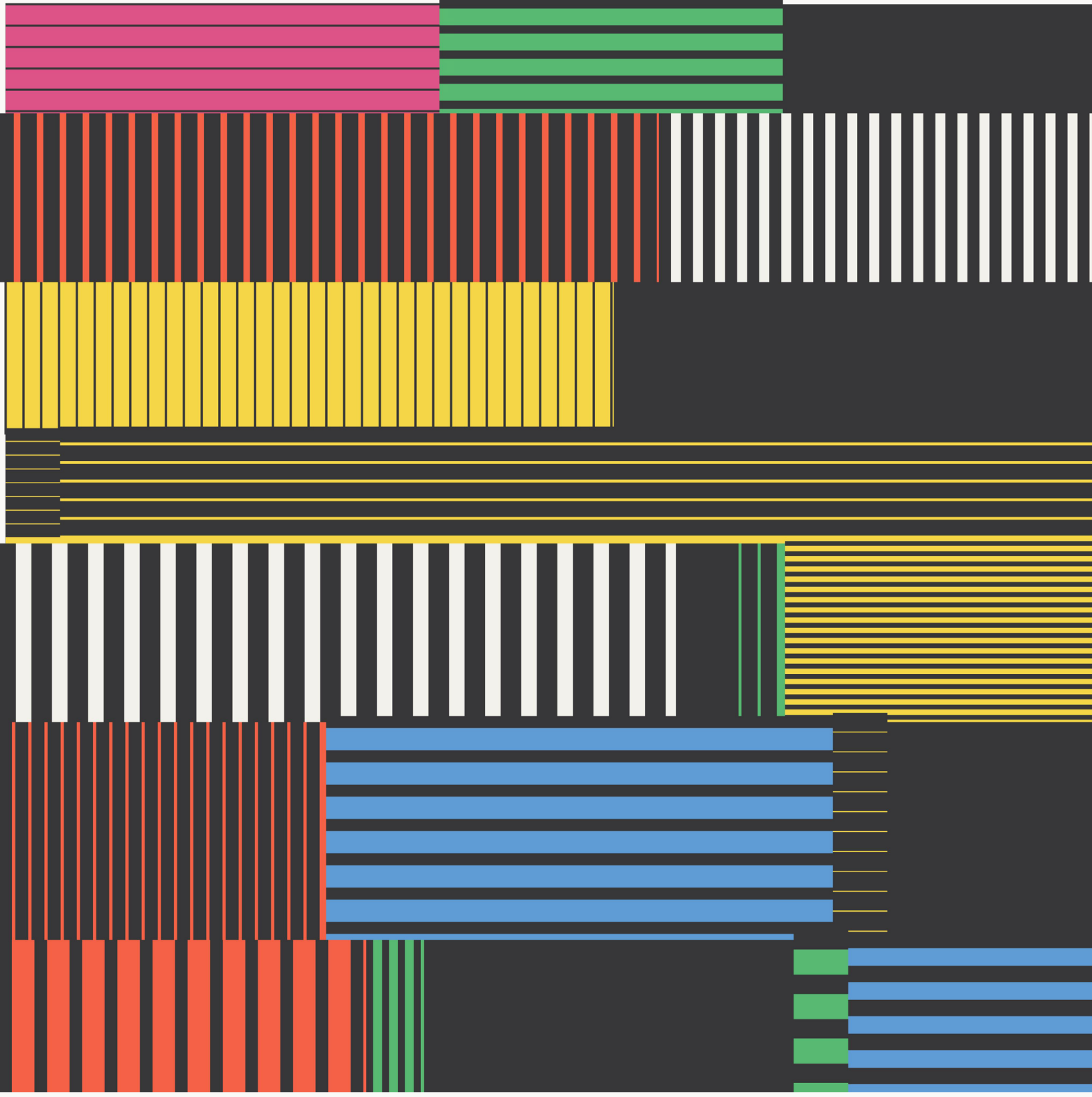
involve communications monitoring or weakening of security mechanisms can generate consequences for the privacy and security of communications of the entire population.

This shows the importance of assessing these measures not only in terms of the legitimacy of the protective objectives they pursue, but also their proportionality, their foreseeable impacts on several rights and the availability of less restrictive alternatives. The scope of an obligation, the mechanisms used to implement it, the categories of services to which it applies and the safeguards incorporated can have very different impacts on human rights. This evaluation should be accompanied by institutional capacities to monitor its implementation and participation mechanisms that incorporate the experiences and perspectives of children and adolescents.

Children and adolescent protection and digital rights should not be seen as conflicting goals. Human rights provide both the basis for protection and the parameters for determining how it is enforced, as well as the limits of the measures taken. This requires looking at children and adolescents' rights from a holistic perspective and assessing the impact of transformations on infrastructure, design and governance of services on the Internet as a space to exercise rights.

A Latin American agenda must also take advantage of lessons learned from international experiences without automatically replicating its solutions. European approaches to corporate responsibilities and the Australian age restriction model already influence the region, but adoption itself does not solve the institutional, social and economic conditions needed to implement them. The production of regional evidence is essential to assess its effects in contexts of inequality of access and diverse regulatory capacities. Power asymmetries among countries and vis-á-vis transnational corporations must also be taken into consideration, as these companies leverage their economic power and lobbying structures to influence public decision-making and limit the obligations imposed on them. This requires transparency on such influence and guarantees against the capture of regulatory processes.

Strengthening regional cooperation can help reduce these asymmetries by sharing evidence, coordinating authorities, and building joint capacities to monitor services operating beyond national borders. Such coordination should be supported by independent institutions, adequate resources and effective participation of civil society as well as children and adolescents themselves. A truly Latin American agenda requires that the experiences, needs and inequalities of the region guide the responses, and that the responsibility for protection be shared without placing the burden on families or leaving it to the discretion of companies. Its outcome should be assessed by measuring the reduction of violence and the expansion of the conditions necessary to exercise rights.



Derechos Digitales
AMÉRICA LATINA