Child Online Protection in Latin America

Risks, Frameworks, and Policy Responses

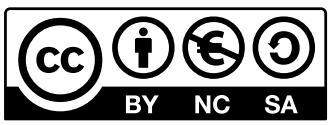
DIGI AMERICAS

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks Google

kriptos LUMU netskope paloalto NETWORKS Resecurity Schneider Electric SISAP Sistemas Aplicativos SOPHOS

TANIUM tenable Trellix TrendAI whalemate zscaler



Executive Summary

Child online protection (COP) has become a central digital governance challenge for Latin America. As children spend more of their lives online, the region must expand meaningful connectivity while ensuring that digital environments are safe, secure, privacy-protective, and age-appropriate. Online risks, including grooming, child sexual exploitation and abuse, harmful content, privacy violations, disinformation, cyberbullying, and algorithmically amplified harms are growing in scale and complexity, particularly as artificial intelligence and other emerging technologies reshape the digital ecosystem.

Latin American countries are not starting from zero. Many have adopted data protection laws, cybersecurity strategies, digital literacy programs, reporting mechanisms, and child safety initiatives. Several countries have already begun to demonstrate important progress, with approaches ranging from rights-based data protection and education campaigns to more comprehensive platform accountability and cybersecurity frameworks. However, implementation remains uneven, and fragmented national approaches limit the region's ability to respond effectively to harms that are inherently cross-border.

The report identifies several persistent gaps: inconsistent legal definitions, divergent platform obligations, limited child-specific cybersecurity strategies, uneven enforcement capacity, slow cross-border cooperation, and the difficulty of implementing age assurance and content moderation in ways that protect privacy and freedom of expression. These challenges place an unrealistic burden on families, educators, and communities to manage risks that require coordinated legal, technical, institutional, and private-sector responses.

International frameworks from UNICEF, ITU, OHCHR, ECLAC, and others provide a strong foundation for regional action. They emphasize child rights, safety- and privacy-by-design, multi-stakeholder governance, digital literacy, victim support, and coordinated enforcement. Global policy examples from Australia, the European Union, the United Kingdom, and India, as well as from countries in Latin America also illustrate different models for operationalizing platform accountability, age-appropriate design, age assurance, and regulatory oversight.

The central takeaway is that Latin America does not need a single uniform model for protecting children online, but it does need greater harmonization. Countries should preserve flexibility to reflect domestic legal systems and cultural contexts while aligning around interoperable principles, shared technical standards, and coordinated enforcement mechanisms. Priority actions include developing a model framework, harmonizing key definitions and safeguards, creating regional reporting and evidence-exchange standards, promoting privacy-preserving age assurance, strengthening mutual legal assistance processes, establishing online safety focal points, investing in shared technical labs and training, and embedding multi-stakeholder governance and human rights impact assessments into policymaking.

Protecting children online is not a one-time regulatory exercise. It is an ongoing governance commitment that requires governments, industry, civil society, educators, parents, and regional institutions to work together. By combining legal interoperability, cybersecurity best practices, privacy safeguards, child participation, and regional cooperation, Latin America can build a more coherent and sustainable approach that protects children from harm while enabling them to benefit fully from the opportunities of the digital age.

Table of Contents

Introduction

The world is becoming increasingly interconnected, with internet access now underpinning economic development, education, and social participation. In Latin America, rapid digital adoption among young populations has expanded opportunities for learning, communication, and inclusion, while also exposing children to a growing range of online risks, including harmful social media use, privacy and data misuse, online grooming, sexual exploitation, exposure to disinformation, and algorithmically amplified content that can negatively affect mental health and development. Despite the recognized importance of connectivity, an estimated two-thirds of the world's school-aged children still lack internet access at home, highlighting persistent inequalities that are also reflected across the region.[1]

While digital connectivity delivers significant social and economic benefits, its implications for children's mental and physical health, privacy, education, and overall well-being remain uneven and context-dependent.[2] Over the past decade, the policy debate on child online protection has evolved from a narrow focus on access and digital literacy to a broader emphasis on platform accountability, data protection, cybersecurity, and age-appropriate design—driven in large part by growing evidence of the dangers of increased online usage and the long-term, adverse societal impacts. Governments across Latin America have begun to respond through a range of approaches, including strengthening data protection frameworks for minors, updating cybersecurity strategies, introducing platform obligations, and expanding child protection and digital literacy initiatives. However, these efforts remain fragmented, with significant variation in legal definitions, enforcement capacity, and institutional coordination.

Artificial intelligence (AI) and other emerging technologies are likely to amplify both opportunities and risks, potentially widening existing gaps if not addressed proactively.[3] In Latin America, where legal frameworks, digital governance approaches, and cultural contexts vary widely, these challenges are particularly complex and increasingly cross-border in nature.

---

[1] https://www.unicef.org/innocenti/reports/childhood-digital-world
[2] https://www.unicef.org/innocenti/reports/childhood-digital-world
[3] https://www.cgdev.org/blog/three-reasons-why-ai-may-widen-global-inequality

This paper examines how countries across the region are addressing child online protection at the intersection of digital governance and cybersecurity by highlighting common challenges, policy gaps, and areas of divergence. It also analyzes the role of international frameworks and regional cooperation, and proposes practical pathways toward greater harmonization, including interoperable standards, cross-border enforcement mechanisms, and capacity-building initiatives. Addressing these issues will require coordinated action across governments, industry, and civil society to ensure that children can participate in the digital environment safely, securely, and equitably.

Key Gaps & Tensions Impeding Effective COP in Latin America

The digital environment is becoming increasingly central to nearly all aspects of children's lives, including education, social interaction, access to government services, and participation in civic life.[4] Across Latin America, efforts to expand connectivity have been a central policy priority, reflecting the widely recognized link between internet access and economic growth, innovation, and social inclusion.[5] Telecommunications operators and internet service providers (ISPs) have played a foundational role in extending this connectivity, investing in infrastructure and enabling broader participation in the digital economy.[6] [7] Indeed, reliable internet connectivity is increasingly understood as a key indicator of development, enabling access to information, markets, and public services.[8] [9]

However, this rapid expansion of digital access is not always matched by equally robust systems to protect children online. While connectivity generates significant economic and societal benefits, it also introduces a parallel set of risks that disproportionately affect younger users.[10] Increased exposure to social media has been associated with negative mental health outcomes , while online environments have facilitated new forms of harm, including sexual exploitation and grooming, the spread of disinformation and misinformation, privacy and data misuse, and algorithmically amplified content that can influence behavior and development.[11], [12] These risks are compounded by the scale, speed, and cross-border nature of digital platforms.

---

[4] https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

[5] https://openknowledge.worldbank.org/entities/publication/483cab21-85be-544f-93c6-302e094b2dfe

[6] https://publications.iadb.org/en/strategies-and-business-models-improving-broadband-connectivity-latin-america-and-caribbean

[7] https://2017-2021.state.gov/u-s-support-for-digital-transformation-in-latin-america-and-the-caribbean/

[8] https://www.cepal.org/en/publications/45835-childhood-and-adolescence-digital-age-comparative-report-kids-online-surveys

[9] https://blogs.worldbank.org/en/digital-development/can-internet-access-lead-improved-economic-outcomes

[10] https://www.unicef.org/documents/keeping-children-safe-online

[11] https://law.stanford.edu/2024/05/20/social-media-addiction-and-mental-health-the-growing-concern-for-youth-well-being/

[12] https://www.hopkinsmedicine.org/health/wellness-and-prevention/social-media-and-mental-health-in-children-and-teens

In many cases, policy and regulatory frameworks across the region have struggled to keep pace with these evolving challenges. Fragmented and underdeveloped approaches to child online protection have often left families, educators, and communities to manage complex risks with limited support. The expectation to handle this situation alone is unrealistic given the technical and institutional sophistication required to address them effectively. As a result, significant gaps and tensions continue to impede a coherent regional response.

One of the most persistent challenges is the fragmentation of legal definitions and regulatory obligations across countries, particularly related to age restriction definitions, what constitutes harmful content, and what responsibility platforms and device manufacturers have. This lack of alignment creates uncertainty for both regulators and industry actors, complicating enforcement and weakening accountability. Similarly, divergent data protection and privacy regimes and limited enforcement capacity limit the ability of authorities to safeguard children's personal information and respond effectively to violations in some cases.

Cross-border cooperation remains another critical weakness. Harmful online activity frequently transcends national boundaries, yet mechanisms for mutual legal assistance, evidence sharing, and coordinated takedown or traceback efforts are often slow, inconsistent, or underutilized. For network operators and service providers, this fragmentation creates operational challenges in responding to lawful requests and implementing safety measures across jurisdictions. This is further complicated by technical challenges, including the need to implement age verification or age assurance systems that do not rely on intrusive data collection, as well as the difficulty of moderating content at scale across multiple languages, dialects, and cultural contexts present in the region.

At the same time, efforts to strengthen child online protection must carefully balance competing rights and policy objectives. Overly broad or poorly designed regulations risk undermining freedom of expression, restricting access to information, or incentivizing platforms to adopt blunt enforcement measures such as over-removal or blanket content blocking. These tensions highlight the need for nuanced, rights-respecting approaches that can effectively mitigate harm without creating unintended consequences.

Taken together, these challenges point to the need for greater regional coordination and policy interoperability. More harmonized legal frameworks, aligned technical standards, and structured public–private collaboration mechanisms can help reduce fragmentation, improve enforcement outcomes, and provide clearer expectations for industry actors operating across multiple jurisdictions.

Cybersecurity and Operational Challenges in COP

As digital connectivity becomes a defining feature of modern life, the protection of children online is increasingly shaped not only by social and regulatory considerations, but also by the underlying security of digital systems and infrastructures. Cybersecurity and child online protection are deeply interconnected. Vulnerabilities in platforms, devices, and networks can be exploited to facilitate harms such as grooming, sexual exploitation, data breaches involving minors, and the manipulation of children through malicious or algorithmically amplified content. The proliferation of connected devices like smartphones, gaming platforms, and internet-enabled toys has further expanded the potential attack surface, introducing new risks where weak security standards can expose children to surveillance, exploitation, or unauthorized data collection. In this context, safeguarding children online requires not only content moderation and regulatory oversight, but also robust cybersecurity practices embedded across the digital ecosystem.

Despite this clear intersection, national approaches across Latin America vary significantly in the extent to which cybersecurity strategies explicitly address child-specific risks. While some countries have begun to incorporate elements of child protection into broader cybersecurity frameworks, many strategies remain focused on critical infrastructure, economic security, and general cybercrime, with limited attention to the unique vulnerabilities of children. At an operational level, gaps persist in key areas such as secure and accessible reporting mechanisms, effective evidence preservation, and coordinated incident response systems that integrate law enforcement, cybersecurity agencies, and child protection services. Strengthening protection for children in this domain will require closer collaboration between governments and the private sector, alongside improved information sharing and clearer protocols for cross-sector response. Developing these capabilities is essential to ensuring that cybersecurity efforts meaningfully contribute to safer digital environments for children across the region.

Global Frameworks & International Norms

Efforts to address child online safety are increasingly shaped by a combination of international frameworks and national policy responses. Global frameworks, including those developed by organizations such as the United Nations Children's Fund (UNICEF) and the International Telecommunication Union (ITU), have established guiding principles for protecting children in digital environments, emphasizing rights-based approaches, multi-stakeholder governance, and child participation.[13] These frameworks provide an important foundation for countries seeking to balance the benefits of connectivity with the need to mitigate harm.

At the same time, governments across the world and in Latin America are translating these principles into domestic policy through a range of legal and regulatory measures, including child-specific data protection provisions, platform obligations, age restrictions, and digital literacy initiatives. However, the interpretation and implementation of these norms vary significantly across jurisdictions, reflecting differences in legal systems, institutional capacity, and societal priorities.

This evolving landscape highlights both opportunities and tensions. While international frameworks promote greater alignment and shared standards, national approaches often diverge in how they balance competing objectives such as privacy versus effective age assurance, or freedom of expression versus content moderation and child safety. Understanding how these global norms influence, and are adapted within, national contexts is critical to identifying pathways toward more coherent and effective child online protection across the region.

International Frameworks

UNICEF and ITU Guidelines for Industry on Child Online Protection[14]

The UNICEF and ITU Guidelines for Industry on Child Online Protection provide a globally recognized, non-binding framework for how private sector actors—including telecommunications operators, internet service providers, and digital platforms—should respect and support children's rights in the digital environment. Developed

[13] https://www.unicef.org/documents/guidelines-industry-child-online-protection
[14] https://www.unicef.org/media/66616/file/industry-guidelines-for-online-childprotection.pdf

through a multi-stakeholder process, the guidelines emphasize a rights-based approach aligned with the UN Convention on the Rights of the Child and the UN Guiding Principles on Business and Human Rights.

The framework outlines five core areas for industry action: integrating child rights into corporate policies and governance; implementing processes to detect and address child sexual abuse material; designing safer, age-appropriate digital environments; promoting digital literacy and responsible use among children and caregivers; and leveraging technology to support children's participation and civic engagement.[15]

Importantly, the guidelines recognize the shared responsibility of industry actors to both mitigate harm and enable positive online experiences, encouraging companies to embed child protection into product design, operational practices, and cross-sector collaboration. They also provide sector-specific recommendations for different parts of the ICT ecosystem, including ISPs, mobile operators, content providers, and platforms, reflecting the diverse roles these actors play in the digital value chain. Overall, the guidelines serve as a flexible global reference point, helping align industry practices with international child rights standards while allowing for adaptation across different regulatory and regional contexts.

OHCHR General Comment No. 25 (2021) on children's rights in relation to the digital environment[16]

The Office of the United Nations High Commissioner for Human Rights (OHCHR) General Comment No. 25 (2021) on children's rights in relation to the digital environment provides authoritative guidance on how the UN Convention on the Rights of the Child (UNCRC) applies in digital contexts. It affirms that children's rights apply fully online, including rights to privacy, protection from harm, access to information, education, and participation. The framework emphasizes that states have an obligation to protect children from online risks such as exploitation, abuse, and harmful content, while also ensuring that measures do not unduly restrict access to information or freedom of expression.

The General Comment calls for a holistic, rights-based approach to digital governance, including child-centered data protection regimes, age-appropriate design standards, and

[15] https://merlin.obs.coe.int/download/7025/pdf

[16] https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

accountability mechanisms for digital service providers. It also underscores the importance of business responsibility, requiring companies to conduct due diligence to identify, prevent, and mitigate risks to children. Importantly, it highlights the need for inclusive access, digital literacy, and the meaningful participation of children in policymaking processes that affect them. Overall, the document serves as a foundational global reference, guiding governments in balancing protection, empowerment, and rights in the digital environment.

ECLAC Childhood and adolescence in the digital age[17]

The Economic Commission for Latin America and the Caribbean (ECLAC) highlights that the region's digital transformation presents both significant opportunities for inclusion and persistent structural challenges, particularly for children and vulnerable populations. While internet access has expanded considerably, deep inequalities remain in connectivity, quality of access, and digital skills, limiting the ability of many children to fully benefit from the digital environment. The report underscores that digital inclusion must go beyond access to encompass affordability, meaningful use, and the development of digital capabilities, especially in education.

At the same time, ECLAC emphasizes the need for stronger digital governance frameworks to address emerging risks, including data protection, cybersecurity, and the safe use of digital platforms. It calls for coordinated public policy approaches, investment in infrastructure, and regional cooperation to close gaps and ensure that digital transformation supports sustainable and inclusive development. The analysis also points to the importance of aligning national strategies with broader regional and international frameworks, while adapting policies to local contexts.

Overall, the report reinforces that achieving equitable and safe digital inclusion in Latin America requires integrated policies that balance access, protection, and capacity-building, with particular attention to children and other at-risk groups.

[17] https://repositorio.cepal.org/server/api/core/bitstreams/51f4dc9b-9bde-4358-bd68-98275f64583d/content

WeProtect Model National Response to end child sexual exploitation and abuse online[18]

The WeProtect Global Alliance Model National Response framework provides a structured approach for governments to prevent and respond to online child sexual exploitation and abuse (CSEA). It outlines a comprehensive, system-wide model built on six key domains: policy and governance, criminal justice, victim support, industry engagement, society and prevention, and coordination and cooperation. The framework emphasizes that effective child online protection requires integrated action across institutions, including law enforcement, child protection services, regulators, and private sector actors.

A central feature of the model is its focus on multi-stakeholder collaboration and clearly defined roles and responsibilities, ensuring that governments, industry, and civil society work in a coordinated manner. It also highlights the importance of capacity-building, data sharing, and operational readiness, including mechanisms for reporting, investigation, and victim support.

The framework includes a maturity model that allows countries to assess their current capabilities and identify gaps, supporting a phased approach to strengthening national responses. Overall, it serves as a practical implementation tool, helping countries translate international principles into coordinated, actionable systems for addressing online child exploitation and abuse.

National Policy Examples

While international frameworks establish a shared set of principles and expectations for child online protection, their effectiveness ultimately depends on how they are translated into national laws, regulations, and operational practices. Across the globe, governments are adapting these international norms into domestic policy responses that reflect local legal systems, institutional capacities, and societal priorities. This process has resulted in a diverse landscape of approaches to protecting children online, offering valuable insights into both emerging best practices and ongoing gaps in implementation.

Australia: Online Safety Act 2021[19]

Australia's Online Safety Act 2021 establishes a comprehensive regulatory framework to address a wide range of online harms, with a strong focus on protecting children and vulnerable

[18] https://www.weprotect.org/resources/frameworks/model-national-response/

[19] https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/current-legislation

users. The legislation grants enhanced powers to the eSafety Commissioner[20] to compel the rapid removal of harmful content, including cyberbullying material targeting children, image-based abuse, and illegal or seriously harmful content. It introduces enforceable online safety standards for platforms and service providers, requiring them to take proactive steps to reduce exposure to harmful material and improve reporting and response mechanisms.

The Act also includes a Basic Online Safety Expectations (BOSE) framework, setting baseline requirements for digital service providers around user safety, transparency, and accountability. Importantly, it creates pathways to address emerging harms such as online grooming, sexual exploitation, and the non-consensual sharing of intimate images, while also supporting victims through complaint and redress mechanisms. The legislation reflects a risk-based, systems-level approach, combining regulatory oversight, industry obligations, and user protections to mitigate harms while maintaining access to digital services.

Overall, the Act is widely regarded as a practical and enforceable model for operationalizing child online protection, demonstrating how governments can translate high-level principles into concrete regulatory tools and institutional authority.

European Union: European Parliament Resolution 2693/2026[21]

The European Parliament has called for stronger EU-wide action to combat cyberbullying, particularly to better protect children and young people online. The initiative emphasizes the need for clearer legal frameworks, stronger platform accountability, and improved reporting and support mechanisms for victims. It targets harms such as online harassment, psychological abuse, and the spread of harmful content, while encouraging coordinated action across member states. The proposal also highlights the importance of prevention measures, digital literacy, and cross-border cooperation, reflecting a more proactive and harmonized approach to addressing cyberbullying in the EU.

[20] https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/esafety-commissioner

[21] https://www.europarl.europa.eu/news/en/press-room/20260423IPR41845/parliament-wants-stronger-action-against-cyberbullying-in-the-eu

European Union: EU-wide Age Verification Technologies[22]

The European Commission's common approach to EU-wide age verification technologies outlines a coordinated framework to protect minors from accessing age-inappropriate content online, particularly under the Digital Services Act (DSA). The initiative promotes the development and deployment of privacy-preserving age assurance solutions, aiming to verify whether a user is above or below a certain age without requiring excessive collection of personal data. This approach seeks to mitigate harms such as exposure to harmful or inappropriate content, online grooming, and exploitation, while addressing concerns around data protection and user privacy.

The framework emphasizes interoperability and standardization across the EU, encouraging the use of trusted digital identity systems and reusable credentials to ensure consistency across platforms and services. It also reflects a risk-based and proportionate approach, requiring platforms to implement appropriate safeguards based on the nature of their services and the risks posed to minors. Importantly, the initiative balances child protection objectives with fundamental rights, particularly privacy and data minimization, by promoting technologies that minimize tracking and profiling.

The EU's approach demonstrates how governments can advance scalable, technically feasible solutions to age assurance that align with broader regulatory frameworks, offering a model for integrating child protection into digital identity and platform governance systems.

United Kingdom Online Safety Act 2023[23]

The United Kingdom's Online Safety Act 2023 establishes a comprehensive regulatory regime aimed at reducing online harms, with a strong emphasis on protecting children. The legislation places statutory duties of care on online platforms, requiring them to proactively assess and mitigate risks associated with harmful content, particularly for minors. Platforms must implement age-appropriate safety measures, including stronger content moderation, default safety settings for children, and mechanisms to prevent exposure to harmful material such as pornography, self-harm content, and online abuse.

The Act empowers the communications regulator, Ofcom, with significant

[22] https://digital-strategy.ec.europa.eu/en/library/commission-sets-out-common-approach-eu-wide-age-verification-technologies
[23] https://www.legislation.gov.uk/ukpga/2023/50

oversight and enforcement authority, including the ability to set safety standards, require transparency reporting, and impose substantial fines for non-compliance. It also introduces requirements for platforms to address illegal content and priority harms, including child sexual exploitation and abuse, grooming, and cyberbullying, while improving user reporting and redress mechanisms.

Importantly, the legislation adopts a risk-based and proportionate approach, requiring companies to tailor protections based on the scale and nature of their services. At the same time, it seeks to balance child protection with freedom of expression and privacy considerations, embedding safeguards to prevent overreach. Overall, the Act represents a robust operational model for translating child online protection principles into enforceable platform obligations and regulatory oversight.

India: The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Updated 2023)[24]

India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (amended 2023) establish a regulatory framework governing online intermediaries, with provisions that address harms affecting children and vulnerable users. The rules impose due diligence obligations on platforms, requiring them to remove unlawful content within specified timeframes, including material related to child sexual abuse, exploitation, and other harmful content. Intermediaries must also implement grievance redress mechanisms, appoint compliance officers, and enable users to report harmful content efficiently.

The framework introduces additional obligations for larger platforms, including proactive monitoring measures and traceability requirements for certain types of content, aimed at addressing issues such as online abuse, misinformation, and exploitation. It also includes provisions to restrict access to age-inappropriate content and strengthen accountability for digital media publishers through a code of ethics and oversight structure.

While the rules aim to mitigate harms such as online exploitation, harmful content dissemination, and abuse, they have also raised important debates around privacy, encryption, and freedom of expression, particularly in relation to traceability requirements. Overall, the framework represents a compliance-driven model that emphasizes platform accountability, rapid content removal, and government oversight as key tools for addressing online harms.

[24] https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf

Regional Landscape: How Countries in Latin America Approach COP

The aforementioned international frameworks and national examples demonstrate a growing convergence around core principles such as rights-based governance, multi-stakeholder coordination, safety-by-design, and platform accountability. Their implementation, however, varies significantly across regions. In Latin America, countries are at different stages of policy and institutional maturity, reflecting disparities in legal frameworks, regulatory capacity, digital infrastructure, and resource availability. As a result, approaches to child online protection across the region remain uneven, with some countries advancing comprehensive strategies while others are still developing foundational policies. Despite these differences, there is a clear opportunity, and need, for all countries to align with these shared global principles, adapting them to local contexts while working toward more consistent, effective, and interoperable approaches to protecting children online. The following countries are among those that have begun to tackle these issues.

Argentina

Argentina's approach to child online protection is anchored in its established data protection framework and complemented by targeted criminal law, public awareness initiatives, and emerging cybersecurity strategy. Law No. 25.326 on Personal Data Protection provides the core legal baseline, establishing principles such as consent, purpose limitation, and data security, which apply to minors' data but do not create a fully distinct child-specific regime.[25] [26] The national data protection authority (AAIP) has sought to fill this gap through soft-law guidance and public-facing initiatives, most notably its "Nuestro Mundo Digital" program, which promotes digital literacy, privacy awareness, and practical safeguards for children, families, and educators.[27] The AAIP has also issued statements on age assurance and child privacy that emphasize proportionality, data minimization, and alignment with regional and international standards, reflecting a cautious, rights-based approach to implementing technical safeguards.[28]

On the criminal law and prevention side, Law No. 27.590 (the "Mica Ortega Law") plays a central role by mandating education and awareness programs on online grooming, signaling a policy emphasis on prevention through schools and public campaigns rather than platform-centric regulation.[29] From a cybersecurity perspective, Argentina's capabilities are structured around CERT.ar, which provides national incident response, threat monitoring, and coordination across sectors, forming the operational backbone for addressing digital risks, including those affecting minors.[30] These efforts are further contextualized by the federal cybercrime prevention and strategic cybersecurity management plan for 2025–2027, which integrates cyber risk management, institutional coordination, and capacity building, though without a strong child-specific focus.[31]

Overall, Argentina's posture is characterized by a rights-based data protection foundation, supplemented by education- and awareness-driven child safety measures and general cybersecurity infrastructure. Compared

---

[25] https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790
[26] https://termly.io/resources/articles/argentinas-personal-data-protection-act/
[27] https://www.argentina.gob.ar/aaip/nuestro-mundo-digital-guia-pedagogica-y-guia-para-adolescentes
[28] https://iapp.org/news/a/argentinas-appi-creates-ai-transparency-and-protection-of-personal-data-program
[29] https://www.argentina.gob.ar/normativa/nacional/ley-27590-345231/texto
[30] https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar
[31] https://www.boletinoficial.gob.ar/detalleAviso/primera/319722/20250116

to more prescriptive models, it relies more heavily on guidance, public policy initiatives, and criminal law tools, with less emphasis on binding platform obligations or comprehensive child-specific regulatory frameworks.

Brazil

Brazil has adopted an increasingly comprehensive and integrated approach to child online protection, combining statutory obligations, regulatory guidance, and national cybersecurity strategy. At the core is Law No. 15.211/2025 ("Digital ECA"), which establishes a rights-based framework grounded in the best interests of the child and imposes affirmative duties on digital service providers to ensure safety- and privacy-by-design.[32] The law requires platforms to implement measures such as age-appropriate design, default high privacy settings, parental controls, and continuous risk assessment of features that may expose minors to harm, including algorithmic systems.[33] These obligations are operationalized through Decree No. 12.880/2026, which creates a coordinated federal enforcement and reporting architecture, clarifies institutional responsibilities, and embeds child online protection within a broader national policy structure led by the Ministry of Justice.[34] [35] Government-facing materials, including the Ministry's "ECA Digital" initiative, emphasize a preventive, systemic model that combines regulation, public awareness, and cross-sector cooperation.[36]

On the data governance side, Brazil leverages its existing data protection regime under the General Personal Data Protection Act (LGPD)[37], with the National Data Protection Agency (ANPD)[38], recently upgraded from an authority to a federal agency,[39] issuing detailed guidance on the processing of children's and adolescents' personal data. This includes requirements for lawful basis, purpose limitation, and heightened safeguards, alongside a clear expectation of privacy-by-default and restrictions on profiling and behavioral advertising.[40] Complementing this, ANPD's 2026 preliminary guidance on reliable age assurance highlights a technical

[32] https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm
[33] https://www.hrw.org/news/2025/09/17/brazil-passes-landmark-law-to-protect-children-online
[34] https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm
[35] https://www.dataguidance.com/news/brazil-president-signs-two-decrees-regulating-digital
[36] https://www.dataguidance.com/news/brazil-president-signs-two-decrees-regulating-digital
[37] https://lgpd-brazil.info/
[38] https://www.gov.br/anpd/pt-br
[39] https://iapp.org/news/a/anpd-becomes-regulatory-agency-a-turning-point-for-brazilian-data-protection-compliance
[40] https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/noticias/2025/09/lula-sanciona-lei-que-protege-criancas-na-internet-e-anuncia-medidas-para-ampliar-concorrencia-e-infraestrutura-digital

approach that balances effectiveness with proportionality and privacy preservation, encouraging risk-based methods and discouraging excessive data collection. At the cybersecurity level, Brazil's National Cybersecurity Strategy (E-Ciber 2025) reinforces the protection of vulnerable populations, including children, by promoting secure digital infrastructure, incident response capacity, and coordination across public and private actors.[41] [42] Finally, implementation is supported in practice by civil society partnerships such as SaferNet Brasil, which provides widely used reporting channels, helplines, and educational resources, illustrating how Brazil combines legal mandates with operational mechanisms for reporting, victim support, and digital literacy.[43] Together, these elements reflect a layered posture that integrates policy, technical safeguards, and institutional coordination to address risks to children in digital environments.

Chile

Chile's approach to child online protection is shaped by a mature cybersecurity framework alongside a significant transition in its data protection regime. The National Cybersecurity Policy 2023–2028, led by the National Cybersecurity Agency (ANCI), establishes a coordinated, risk-based strategy focused on critical infrastructure protection, incident response, and cross-sector collaboration.[44] Operationally, the national CSIRT provides national-level incident response, threat monitoring, and public guidance, forming the technical backbone for managing digital risks, including those affecting minors. While these instruments are not child-specific, they contribute to a secure digital environment that underpins broader online safety.[45]

Chile's data protection framework is currently governed by Law No. 19.628, which provides a general baseline for personal data processing but offers limited child-specific provisions.[46] This is set to change with Law No. 21.719, entering into force in December 2026, which establishes a modernized data protection regime and creates a dedicated supervisory authority.[47] The new law is expected to strengthen safeguards, accountability, and oversight, with clearer implications for

[41] https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-ciberseguranca-eciber
[42] https://depp.oecd.org/policies/BRA2214
[43] https://new.safernet.org.br/denuncie
[44] https://anci.gob.cl/pncs-2023-2028/
[45] https://csirt.gob.cl/
[46] https://www.bcn.cl/leychile/navegar?idNorma=141599
[47] https://www.bcn.cl/leychile/navegar?i=1209272

children's data and digital services.[48] On the policy and social side, initiatives such as Kids Online Chile 2022 and the Ministry of Education's Digital Citizenry program highlight risks faced by children online and promote digital literacy, responsible use, and awareness among students, educators, and families.[49] [50]

Overall, Chile's posture combines strong cybersecurity institutions with an evolving data protection framework and education-focused child safety initiatives. Its model emphasizes institutional capacity and public policy development, with the forthcoming data protection reform likely to play a key role in advancing more robust, child-sensitive digital governance.

Mexico

Mexico's approach to child online protection reflects a growing convergence between cybersecurity planning, telecommunications governance, and child-rights policy. At the strategic level, the National Cybersecurity Plan 2025–2030[51], supported by the Digital Transformation and Telecommunications Agency (ATDT)[52], frames cybersecurity as a matter of national resilience and public safety, with implicit relevance for protecting vulnerable populations, including minors.[53] Operationally, CERT-MX provides incident response capabilities, threat monitoring, and coordination across public and private sectors, forming the backbone of Mexico's technical cybersecurity infrastructure. While these instruments are not child-specific, they contribute to a broader environment of digital risk mitigation that underpins online safety.[54]

Child-focused protections are more explicitly developed through institutional and policy channels. SIPINNA (the National System for the Protection of Children and Adolescents) leads federal efforts on child online safety, issuing guidance on safe internet use, digital literacy, and risk prevention, often in collaboration with international partners such as UNICEF Mexico, which emphasizes a rights-based and educational approach.[55] In parallel, Mexico's telecommunications framework plays

[48] https://resguard-solutions.com/blog/es/chile-data-protection-law-21719-guide/
[49] https://www.unicef.org/chile/informes/kids-online-chile-2022
[50] https://ciudadaniadigital.mineduc.cl/
[51] https://mexicobusiness.news/cybersecurity/news/mexico-unveils-national-cybersecurity-plan-2025-2030
[52] https://www.gob.mx/atdt/
[53] https://www.gob.mx/atdt/comunicacion/liderara-mexico-ciberresiliencia-en-la-region-con-plan-nacional-de-ciberseguridad
[54] https://www.gob.mx/gncertmx
[55] https://www.gob.mx/sipinna/articulos/ciberseguridad-para-ninas-ninos-y-adolescentes-en-el-ecosistema-digital?idiom=es

a role in shaping platform and network-level responsibilities, particularly around access, content, and user protections.[56] Data protection is governed by federal laws applicable to both public and private sectors, which establish principles such as consent, purpose limitation, and security safeguards, including heightened considerations for minors' data.

Overall, Mexico's posture combines cybersecurity infrastructure, telecom regulation, and child-rights policy, but remains less centralized and prescriptive than other countries. Its strength lies in institutional coordination and public education efforts, while its evolving data governance structure and reliance on general-purpose cybersecurity tools highlight ongoing challenges in developing a cohesive, child-specific digital safety regime.

Peru

Peru's approach to child online protection is anchored in a dedicated legal framework specifically addressing the safe and responsible use of ICTs by children and adolescents, complemented by general data protection law and national cybersecurity structures. Law No. 30254, as amended by Law No. 31664 and implemented through Supreme Decree No. 093–2019–PCM, establishes obligations to promote safe digital environments, prevent online risks such as grooming and exploitation, and encourage coordination among government, private sector, and civil society actors.[57] The framework places particular emphasis on awareness, education, and shared responsibility, rather than imposing extensive direct obligations on digital platforms, and is operationalized through national policies and interinstitutional initiatives.

Peru's data protection regime, under Law No. 29733, provides the baseline for privacy and personal data governance, including principles such as consent, purpose limitation, and security safeguards applicable to minors' data. While not child-specific, it supports broader online safety efforts by regulating how personal data is collected and processed. On the cybersecurity side, the Centro Nacional de Seguridad Digital and related CSIRT functions provide national coordination for incident response, risk monitoring, and digital security policy, contributing to a safer digital ecosystem overall.

Child-focused protection is reinforced through government-led public education and coordination efforts, including official guidance for families on safe internet use and initiatives such as the Alianza Nacional por una Internet Segura, which brings together public

[56] https://www.gob.mx/crt/es/que-hacemos
[57] https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/292146–30254

institutions and private stakeholders to promote awareness and preventive practices. Overall, Peru's posture emphasizes education, interinstitutional coordination, and targeted legal protections for minors, supported by general privacy and cybersecurity frameworks, but with a comparatively lighter emphasis on binding platform-level obligations.

Uruguay

Uruguay's approach to child online protection is grounded in a strong data protection framework, supported by coordinated cybersecurity governance and a notable emphasis on digital literacy and prevention. Law No. 18.331 on Personal Data Protection establishes the core legal regime, incorporating principles such as consent, purpose limitation, and data security, and is overseen by the data protection authority (URCDP), which provides institutional oversight and guidance.[58] While the law is not exclusively child-specific, it applies to minors' data and is complemented by regulatory engagement and public guidance that reinforce privacy protections in digital environments.

On the cybersecurity side, Uruguay has developed a coherent governance structure led by Agesic, which coordinates national cybersecurity strategy, risk management, and interagency collaboration.[59] Operationally, CERTuy serves as the national incident response team, offering threat monitoring, reporting channels, and response procedures that are accessible to both institutions and the public.[60] Its defined incident reporting rules and processes contribute to a structured and transparent approach to handling digital threats, including those that may impact children.

Child-focused protection is particularly visible in Uruguay's prevention-oriented policies. The Ceibal digital citizenship strategy integrates online safety, responsible technology use, and digital skills into the education system, targeting students, teachers, and families.[61] This is reinforced by empirical insights from Kids Online Uruguay 2022, which documents children's online behaviors, risks, and coping strategies, informing evidence-based policy and educational interventions.[62] Overall, Uruguay's posture reflects a balanced model that combines data protection,

[58] https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/uruguayan-law-protection-personal-data-and-habeas-data-action-ldpd-2024-09-25_en
[59] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/
[60] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/tramites-y-servicios/servicios/certuy
[61] https://ceibal.edu.uy/institucional/articulos/lanzamiento-nueva-estrategia-nacional-de-ciudadania-digital-2024-2028/
[62] https://www.unicef.org/uruguay/informes/informe-kids-online-uruguay-2022

institutional cybersecurity capacity, and strong education-driven prevention efforts, with a particular strength in integrating child online safety into its national digital inclusion and education agenda.

Regional Takeaway

Taken together, these country examples illustrate both meaningful progress and room for improvement across the region. While there is clear alignment with global principles, particularly around rights-based governance, prevention, and institutional coordination, implementation pathways differ based on legal traditions, institutional capacity, and policy priorities. This diversity is not unique to Latin America; countries across other regions are similarly experimenting with different regulatory mixes, institutional arrangements, and technical approaches to child online protection. No single model has emerged as definitively "correct," and attempts to impose a uniform solution risk overlooking the contextual factors that shape both risks and feasible interventions.

Accordingly, the most effective path forward lies not in convergence toward a single blueprint, but in thoughtful harmonization. National approaches should continue to draw from international frameworks and shared standards, ensuring interoperability, cross-border cooperation, and baseline protections for children in an inherently global digital environment. At the same time, these approaches must remain adaptable to local contexts, reflecting domestic legal systems, cultural considerations, and resource realities. Balancing global alignment with contextual relevance will be critical to building resilient, coherent, and effective child online protection regimes both within Latin America and as part of a broader, evolving international landscape.

Practical Policy, Technical, and Governance Solutions for Regional Harmonization

Advancing child online protection across Latin America requires moving from high-level alignment on principles to practical mechanisms that enable coordination, interoperability, and shared accountability. Building on existing international frameworks and the diverse national approaches outlined above, this section proposes actionable, regionally adaptable solutions. These recommendations are designed to be modular, allowing countries to adopt common building blocks while tailoring them to domestic legal systems, institutional capacity, and risk environments.

Legal and regulatory harmonization

A foundational step toward regional coherence is the development of a model COP framework or reference law that establishes core minimum standards. Rather than prescribing identical legislation, this model should define key baseline elements: harmonized definitions (including "child," "adolescent," and age of digital consent), minimum data protection safeguards for minors, mandatory reporting obligations for severe online harms (such as child sexual exploitation and grooming), and safe-harbor provisions for platforms conditioned on compliance with due process and transparency requirements. Drafting should align with established international guidance, including ITU and UNICEF frameworks, as well as widely accepted privacy and human rights principles.

Crucially, countries should be encouraged to adopt interoperable principles rather than identical statutory language. This approach enables legal compatibility across borders, facilitating cooperation and enforcement while preserving flexibility for national adaptation. Regional bodies or forums can support this process by issuing interpretive guidance, model clauses, and periodic updates that reflect evolving risks and technologies.

Technical interoperability and standards

Legal alignment must be complemented by technical interoperability to ensure that systems designed to detect, report, and respond to harms can function seamlessly across jurisdictions. A priority area is the development of a regional reporting standard: a shared data schema for documenting incidents such as child sexual exploitation, grooming, and other high-risk harms. This would enable consistent reporting by platforms, streamlined intake by authorities, and more efficient cross-border case handling. Paired with this, secure protocols for evidence exchange (incorporating encryption, chain-of-custody safeguards, and privacy protections) are essential for timely and lawful cross-border investigations.

In parallel, Latin America would benefit from common technical standards for age-appropriate design and privacy-preserving age assurance. Rather than relying on intrusive or inconsistent verification methods, countries can promote approaches based on data minimization, such as cryptographic proofs or minimal-attribute attestations that confirm age ranges without exposing full identity. Standardized expectations for platform transparency, supported by shared APIs or reporting tools, can further enhance accountability, enabling regulators and researchers to access comparable data on content moderation, abuse reporting, and risk mitigation outcomes.

Cross-border enforcement and cooperation

Given the inherently transnational nature of online harms, strengthening cross-border enforcement mechanisms is critical. The development of standardized Mutual Legal Assistance (MLA) templates tailored to COP cases can significantly reduce delays and procedural friction. These should include expedited channels for urgent child safety matters, with clear timelines and escalation pathways. Establishing designated COP focal points within law enforcement agencies, data protection authorities, and judicial networks can further streamline communication and coordination.

Capacity-building and shared services

Disparities in institutional capacity remain a significant barrier to effective implementation. Addressing this requires sustained investment in regional capacity-building initiatives. A standardized training curriculum covering legal, technical, and operational aspects of COP could be developed for prosecutors, judges, law enforcement, CERT teams, and

child protection organizations. Delivery through regional training centers or online platforms would ensure scalability and accessibility.

Shared services offer an efficient way to extend capabilities to less-resourced countries. Regional technical labs could provide advanced forensic analysis, digital evidence processing, and victim support services.

Multistakeholder governance and accountability

Effective COP frameworks depend on inclusive governance structures that bring together regulators, industry, civil society, and child rights advocates. Countries should consider establishing multi-stakeholder oversight bodies at both national and regional levels, tasked with monitoring platform compliance, reviewing policy effectiveness, and advising on emerging risks. These bodies can enhance transparency, build public trust, and ensure that diverse perspectives are reflected in decision-making.

At the regional level, such mechanisms can facilitate peer learning and benchmarking, enabling countries to compare progress, identify gaps, and coordinate responses. Regular reporting and public accountability processes should be embedded into these structures to maintain momentum and credibility.

Privacy-protecting safeguards and human rights considerations

Finally, all harmonization efforts must be grounded in strong safeguards to protect fundamental rights. Mandatory human rights impact assessments (HRIAs) should be required for COP-related interventions, particularly those involving sensitive technologies such as age verification, content filtering, or surveillance tools. These assessments should evaluate proportionality, necessity, and potential unintended consequences, ensuring that measures designed to protect children do not undermine broader rights to privacy, expression, and access to information.

Equally important is the inclusion of children's voices in policy design and evaluation. Mechanisms for meaningful child participation such as youth advisory panels, consultations, and participatory research can provide valuable insights into lived experiences and emerging risks. Embedding these perspectives not only strengthens policy relevance but also reinforces the rights-based foundation of COP efforts.

Conclusion

Child online protection is no longer a peripheral digital policy issue; it is a core component of digital governance, cybersecurity, child rights, and inclusive development. As children across Latin America spend more of their lives online, the region faces a dual responsibility: expanding meaningful connectivity while ensuring that digital environments are safe, secure, rights-respecting, and age-appropriate. The challenge is not simply to reduce harm after it occurs, but to build systems that prevent abuse, protect privacy, strengthen resilience, and enable children to participate fully in the digital world.

This paper shows that Latin American countries are not starting from zero. Across the region, governments have developed data protection laws, cybersecurity strategies, public education initiatives, reporting mechanisms, and emerging platform accountability frameworks. International models and global frameworks also provide a strong foundation. Yet progress remains uneven, and fragmented approaches limit the effectiveness of national efforts against risks that are inherently cross-border. The region now needs to move from isolated initiatives toward practical harmonization, shared principles, interoperable standards, coordinated enforcement, stronger institutions, and sustained capacity-building. This includes advancing interoperable legal frameworks grounded in common baseline principles, developing regional technical standards for reporting and evidence exchange, promoting privacy-preserving age assurance approaches, strengthening cross-border cooperation mechanisms, investing in shared regional services and training, and establishing multi-stakeholder governance structures that support transparency and accountability.

There is no single “right” model for child online protection. Each country must adapt solutions to its legal system, institutional capacity, culture, and digital ecosystem. But national flexibility should not mean regional fragmentation. A more coherent approach grounded in international human rights standards, privacy safeguards, cybersecurity best practices, and meaningful child participation can help countries protect children while preserving openness, innovation, and access to information. Regional harmonization efforts should therefore prioritize interoperable principles rather than identical laws, enabling countries to align around shared objectives while maintaining domestic flexibility. At the same time, safeguards such as human rights impact assessments and participatory mechanisms that incorporate children’s voices must remain central to policy development and implementation.

Governments should modernize legal frameworks and strengthen enforcement capacity. Industry should embed safety- and privacy-by-design into products and services used by children. Platforms should also support standardized transparency reporting and implement age-appropriate design measures that minimize unnecessary data collection and protect children's privacy. Civil society, educators, parents, and child protection organizations should be resourced as essential partners, not left to manage risks alone. Regional institutions and partners should support shared tools, training, evidence exchange, and technical standards that make cooperation faster and more effective.

Protecting children online is not a one-time regulatory project, it is an ongoing governance commitment. The digital environment will continue to evolve, and so will the risks. Latin America has an opportunity to shape a regional approach that is practical, interoperable, and rights-respecting—one that protects children from harm while empowering them to benefit from the opportunities of the digital age. By combining legal interoperability, technical coordination, cross-border cooperation, inclusive governance, and strong privacy and human rights safeguards, the region can move toward a more effective and sustainable model for child online protection that reflects both regional realities and global best practices.


DIGI
AMERICAS