

Recommendations on the protection of children and adolescents in environments with encryption in MERCOSUR



Recommendations on the protection of children and adolescents in environments with encryption in MERCOSUR

AUTHORSHIP

Luiza Correa de Magalhães Dutra
Paulo Rená da Silva Santarém
Wilson Guilherme Dias Pereira

REVISION

Ana Bárbara Gomes
Fernanda dos Santos Rodrigues Silva

TRANSLATION

Luiza Correa de Magalhães Dutra
Paulo Rená da Silva Santarém

GRAPHIC DESIGN, COVER, LAYOUT AND FINALIZATION

Felipe Duarte
Cover image Freepik

EDITORIAL PRODUCTION

IRIS - Institute for Research on Internet and Society

HOW TO CITE IN ABNT

DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson
Guilherme Dias; SANTARÉM, Paulo Rená da Silva.
**Recommendations on the protection of children
and adolescents in environments with encryption in
MERCOSUR**. Belo Horizonte: Internet and Society Reference
Institute, 2024. Available at: <https://bit.ly/4e0UaYj>. Accessed
at: dd mmm. aaaa



INSTITUTE
FOR RESEARCH
ON INTERNET
AND SOCIETY

DIRECTORS

Ana Bárbara Gomes

Paloma Rocillo

MEMBERS

Felipe Duarte | Head of Communication

Fernanda Rodrigues | Head of Research and Researcher

Glenda Dantas | Researcher

Júlia Caldeira | Researcher

Júlia Tereza Koole | Research trainee

Luisa Melo | Research trainee

Luiza Correa de Magalhães Dutra | Researcher

Paulo Rená da Silva Santarém | Researcher

Thais Moreira | Communication Analyst

Wilson Guilherme | Researcher

irisbh.com

SUMMARY

Presentation	<u>5</u>
A. Preconize the best interests of children and adolescents and respect integral protection in digital environments	<u>7</u>
B. Ensure that technology solutions maintain strong encryption and do not weaken technology security	<u>8</u>
C. Subject any government access to digital devices and systems to the principle of due process of law, the need for judicial authorization, and the protection of children's and youth's personal data	<u>9</u>
D. Respecting legality, proportionality, necessity, and multisectorial dialogue when formulating public safety policies and strategies regarding monitoring, surveillance, and access to instant messages and encrypted content is essential for the protection of children and adolescents	<u>11</u>
E. Consider scientific data, assess impact and promote social participation in the proposition of technological artifacts for the local context	<u>12</u>
F. Prohibiting or imposing strict parameters on the allowance of breaking or compromising encryption in criminal investigations and prosecutions	<u>13</u>
G. Regulate the role of digital platforms demanding transparency, accountability and shared responsibility in strategies to combat sexual violence against children and adolescents	<u>14</u>
H. Regulate the online protection of children and adolescents in a specific approach, taking into account the diversity of contexts, including regional differences	<u>16</u>
I. Promote national and regional debate rounds on the topic, with multisectoral participation and, preferably, incorporating the perspectives of children and adolescents affected by the policies	<u>17</u>
J. Promote public policies for meaningful connectivity and digital literacy for children and adolescents	<u>18</u>

Presentation

The Institute for Research on Internet & Society (IRIS) is an independent and interdisciplinary research center founded in 2015, dedicated to producing and communicating scientific knowledge on internet and society issues, as well as advocating for and promoting public policies that advance human rights in the digital realm. Our work aims to enrich and democratize discussions about the internet, society, and new technologies by providing scientific insights to internet users and various sectors of society: government, civil society, the private sector, and the technical and academic community.

Our project **Information Security and Children and Adolescents Protection: Narratives and Regulatory Proposals in MERCOSUR** focused on analyzing debates about the protection of children and adolescents in environments with encryption, from the perspective of the Global South, going beyond the polarization of technological security vs. protection of children and adolescents. At IRIS, we seek multisectorial dialogue on these two fields, based on scientific evidence and respect for human rights. From the insights gathered, our aim is to monitor and influence the legislative debate on this issue, offering recommendations to MERCOSUR states and digital technology companies operating in the region.

Previously, we listed in an Fact Sheet the normative artifacts regarding the protection of children and adolescents in encrypted digital environments in MERCOSUR.¹ We also contributed to the public agenda of related debates on the topic during two public hearings. First, on May 14, 2024, at the Senate's Communication and Digital Law Commission, we participated in the debate on Bill nº 2.628/2022 regarding online protection for children and adolescents.² Second, on June 11, 2024, we were at the Supreme Federal Court discussing *Arguição de Descumprimento de Preceito Fundamental* ("Claim of Non-compliance with Fundamental Precept") nº 1143, concerning the regulation of the use of secret monitoring tools for personal communication devices, such as mobile phones and tablets, by public agencies and officials.³

We also systematized the final results of our research in a report on the landscape of

1 See DUTRA, Luiza Correa de Magalhães; SANTARÉM, Paulo Rená da Silva; VIEIRA, Víctor Barbieri Rodrigues; PEREIRA, Wilson Guilherme Dias. **Fact Sheet: Normative artifacts on children and adolescents' rights in MERCOSUR digital environments**. Belo Horizonte: Internet and Society Reference Institute, 01 Aug. 2024. Available at <https://irisbh.com.br/en/publicacoes/fact-sheet-normative-artifacts-on-children-and-adolescents-rights-in-mercosur-digital-environments/>. Accessed on 20 Sep. 2024.

2 SANTARÉM, Paulo Rená da Silva; PEREIRA, Wilson Guilherme Dias; DUTRA, Luiza Correa de Magalhães. **Proteção de crianças e adolescentes online: panorama, efemérides e atualização**. Instituto de Referência em Internet e Sociedade, 20 May 2024. Available at <https://irisbh.com.br/protacao-de-criancas-e-adolescentes-online/>. Accessed on 15 Jul 2024.

3 FEDERAL SUPREME COURT. **STF encerra audiência pública com diversidade de visões sobre as ferramentas de monitoramento**. 11 Jun. 2024. Available at <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=547319&ori=1>. Accessed on 12 Jul. 2024.

MERCOSUR countries, based on a detailed analysis of normative⁴ and technological artifacts, mediated by a mosaic of expert discourses.⁵ The conclusions of this report support the recommendations presented here.

Now, as a proposal to advance the debate in favor of better online comprehensive protection for children and adolescents, we present ten recommendations aimed at contributing to the development of public policies in the fields of public safety and criminal justice, as well as to the actions of private companies operating with accessible digital platforms in MERCOSUR. This is a technical document directed at interested stakeholders, with a purpose that requires normative jargon, which we strive to mitigate as much as possible for a more accessible reading.

We hope that this publication will ignite an open dialogue with the various sectors involved in the topic, as well as integrate it into the agenda of multistakeholder debates on internet governance, especially in the MERCOSUR region, facilitating the creation of a joint political agenda.

4 During the period of our research, two important documents were issued in Brazil on the topic: the National Council for the Rights of Children issued Resolutions No. 245 and 246, dated April 5 and June 12, 2024, respectively, addressing the rights of children and adolescents in digital environments and establishing a Thematic Group to develop the corresponding National Policy. BRAZIL. Presidency of the Republic. Participa + Brasil. **Resoluções do Conanda**. At. Jun. 2024. Available at <https://www.gov.br/participamaisbrasil/https://www.gov.br/participamaisbrasil/blob-baixar-7359>. Accessed on 12 Jul. 2024.

5 See [CITE FINAL REPORT].

A. Preconize the best interests of children and adolescents and respect integral protection in digital environments

Integral protection and the best interests of children and adolescents, as outlined in the UN Convention on the Rights of the Child⁶ – ratified by all MERCOSUR countries⁷ – require prioritizing their protection in all contexts, by both private and public institutions (judicial, administrative, and legislative). Therefore, normative or technological proposals from these countries must articulate all child and adolescent rights to ensure that children and adolescents are not victims of any form of online violence, including hate speech, sexual violence, or even violations of their freedom of expression and social participation.

According to General Comment n° 25 of the Committee on the Rights of the Child, of 2021,⁸ the best interests of the child must be given special emphasis in the digital environment, particularly in design, management, and regulation, to ensure that the presence of children and adolescents online is safeguarded with the comprehensive protection of their rights. Furthermore, it should be recognized that privacy is a right of children and adolescents, including as a foundation for sexual democracy,⁹ guaranteed in light of its peculiar condition of development, always observing its progressive autonomy.

Therefore, **it is recommended** that MERCOSUR Member States, when developing digital policies, preconize the best interests of children and adolescents and their integral protection, in order to guarantee their privacy. This includes refraining from authorizing unlimited and permanent surveillance of this public, as well as assigning to digital platforms, particularly instant messaging services, the disproportionate duty of creating

6 UN – United Nations Organization. General Assembly. **Convenção sobre os Direitos da Criança. [A/RES/44/25]**. 20 Nov. 1989. Available at <https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca>. Accessed on 20 June 2024.

7 See DUTRA, Luiza Correa de Magalhães; SANTARÉM, Paulo Rená da Silva; VIEIRA, Víctor Barbieri Rodrigues; PEREIRA, Wilson Guilherme Dias. **Fact Sheet: Normative artifacts on children and adolescents' rights in MERCOSUR digital environments**. Belo Horizonte: Internet and Society Reference Institute, 01 Aug. 2024. Available at <https://irisbh.com.br/en/publicacoes/fact-sheet-normative-artifacts-on-children-and-adolescents-rights-in-mercosur-digital-environments/>. Accessed on 20 Sep. 2024.

8 UN – United Nations Organization. Committee on the Rights of the Child. **General Comment No. 25 (2021) on Children's Rights in relation to the digital environment**. Geneva: UN, 02 Mar. 2021. Available at <https://digitallibrary.un.org/record/3906061>. Accessed on 20 Jun. 2024. Unofficial translation by Instituto Alana from English to Portuguese (April/2021). Available at <https://criancaconsumo.org.br/wp-content/uploads/2022/01/comentario-geral-n-25-2021.pdf>. Accessed on 20 June 2024.

9 Sexual democracy can be understood in literature as “The idea permeates the opportunity to know and recognize one’s own body, desires, repulsions, guarantee the perception of the existence of different forms of manifestation of affection and desire, and combat the pathologization of consensual desires , in stages suitable for such consent” in PEREIRA, Wilson Guilherme Dias. **WHERE WERE YOU WHEN I NEEDED YOU? Perceptions of LGBTQIA+ victims of child and youth sexual violence about the Rights Guarantee System of Porto Velho – RO**. Porto Velho, 2023. Dissertation (Master’s). Interdisciplinary Professional Master’s Postgraduate Program in Human Rights and Justice Development. Federal University of Rondônia Foundation. Available at <https://dhjus.unir.br/pagina/exibir/22968>. Accessed on June 17th. 2024. p.46.

“backdoors”¹⁰ that allow surveillance of this group’s private habits.

It is recommended that companies, when developing digital services and products aimed at use by children and adolescents, respect their integral protection, establish effective internal mechanisms for reporting violence, and promote social projects for digital literacy aimed at this audience, in order to empower individuals to identify and report violence.

B. Ensure that technology solutions maintain strong encryption and do not weaken technology security

With the expansion of the use of digital information and communication technologies, the use of strong encryption is a concrete measure that supports the realization of the rights ensured by the Child and Adolescent Statute (CDC)¹¹, safeguarding navigation and communications in digital environments while ensuring respect for legal guarantees. To defend and enable the exercise of these rights in the information society, encryption plays a crucial role as a tool for ensuring digital security in general, protecting the content of communications and personal data, for example, against unauthorized access.¹²

The implementation of strong encryption has broad potential and ensures that personal data and private communications between young people and their families and friends remain inaccessible to malicious third parties, protecting them from various forms of exploitation and abuse. Technological tools with strong encryption make it more difficult for online abusers and exploiters to act, complicating the interception of communications or access to private information of children and adolescents.¹³ This reduces the risk of

10 SANTARÉM, Paulo Rená da Silva. **“Portas clandestinas”**: uma tradução mais precisa para debatermos **backdoors em criptografia**. Blog: Instituto de Referência em Internet e Sociedade. 17 Jan. 2022. Available at: <https://irisbh.com.br/portas-clandestinas-uma-traducao-mais-precisa-para-debatermos-backdoors-em-criptia/>. Accessed on: 10 Oct. 2022.

11 CRIN - Child Rights International Network; Defend Digital Me. **Privacy and Protection: a children’s rights approach to encryption**. 19 Jan. 2023. Available at <https://home.crin.org/readlistenwatch/stories/privacy-and-protection>. Accessed on 20 Jun. 2024.

12 LIGUORI, Carlos. **Law and Cryptography: fundamental rights, information security and the limits of legal regulation in technology**. São Paulo: SaraivaJur, 2022.

13 It is important to highlight the work “Encryption Policies: Between the Codification of Rights, Public Regulation and Cipher-Activism”, by André Barbosa Ramiro Costa, which explains that rights, such as the secrecy of communications, find in encryption a technological protection against state abuses associated with the growing culture of monitoring. See COSTA, André Barbosa Ramiro. **Políticas de encriptação: entre a codificação de direitos, regulação pública e o cipher-ativismo**. Dissertation (Master’s in Computer Science) - Universidade Federal de Pernambuco, Recife, 2021. Available at <https://repositorio.ufpe.br/handle/123456789/42872>. Accessed on 25 Mar. 2024.

grooming,¹⁴ leak of sexting,¹⁵ and other forms of digital sexual violence. Encryption serves as an additional barrier that protects young audiences from being easy targets for online criminals, aligning with existing protection efforts in the region.

In MERCOSUR, the recognition of this role of encryption is urgent, considering the lack of specific legal guarantee in these countries for its free use in these countries,¹⁶ with only limited mentions pertaining to the context of personal data protection. An explicit norm guaranteeing this right would confront normative and technological proposals that had the purpose of monitoring or criminal investigation involving the breaking of encryption or equivalent damage to its attributes, namely authenticity, integrity, confidentiality and non-repudiation.

It is recommended to MERCOSUR member states and companies that technological tools addressing online protection of children and adolescents, including those that deal with confronting sexual violence in digital environments, count on strong encryption as an ally in also safeguarding the rights of children and youth. The full exercise of these rights is enhanced by technological security mechanisms that are free from vulnerabilities.

C. Subject any government access to digital devices and systems to the principle of due process of law, the need for judicial authorization, and the protection of children’s and youth’s personal data

All MERCOSUR countries, in their constitutions and ordinary laws, guarantee due process from the outset of criminal investigations in light of human rights.¹⁷ In a democratic

14 “It is the gradual establishment of an emotional connection with the victim, manipulating their trust, affection and vulnerabilities in order to carry out (...)” sexual violence. In SANTARÉM, Paulo Rená da Silva; PEREIRA, Wilson Guilherme Dias; DUTRA, Luiza Correa de Magalhães. **Proteção de crianças e adolescentes online: panorama, efemérides e atualização**. Instituto de Referência em Internet e Sociedade, 20 May 2024. Available at <https://irisbh.com.br/protacao-de-criancas-e-adolescentes-online/>. Accessed on 15 Jul 2024.

15 “It is the sending of messages of a sexual nature, with text, audio, video or images” In SANTARÉM, Paulo Rená da Silva; PEREIRA, Wilson Guilherme Dias; DUTRA, Luiza Correa de Magalhães. **Proteção de crianças e adolescentes online: panorama, efemérides e atualização**. Instituto de Referência em Internet e Sociedade, 20 May 2024. Available at <https://irisbh.com.br/protacao-de-criancas-e-adolescentes-online/>. Accessed on 15 Jul. 2024.

16 DUTRA, Luiza Correa de Magalhães; SANTARÉM, Paulo Rená da Silva; VIEIRA, Víctor Barbieri Rodrigues; PEREIRA, Wilson Guilherme Dias. **Fact Sheet: Normative artifacts on children and adolescents’ rights in MERCOSUR digital environments**. Belo Horizonte: Internet and Society Reference Institute, 01 Aug. 2024. Available at <https://irisbh.com.br/en/publicacoes/fact-sheet-normative-artifacts-on-children-and-adolescents-rights-in-mercosur-digital-environments/>. Accessed on 20 Sep. 2024.

17 DUTRA, Luiza Correa de Magalhães; SANTARÉM, Paulo Rená da Silva; VIEIRA, Víctor Barbieri Rodrigue; PEREIRA, Wilson Guilherme Dias. **Fact Sheet: Normative artifacts on children and adolescents’ rights in MERCOSUR digital environments**. Belo Horizonte: Internet and Society Reference Institute, 01 Aug. 2024. Available at <https://irisbh.com.br/en/publicacoes/fact-sheet-normative-artifacts-on-children-and-adolescents-rights-in-mercosur-digital-environments/>. Accessed on 20 Sep. 2024.

State based on the rule of law, it is the duty of the public authority to avoid unrestricted data collection measures and to observe minimum legal safeguards, ensuring that the investigated or accused individual receives due process—which includes respect for personal data protection during criminal prosecution.

Therefore, it is necessary to recognize, among the elements of criminal prosecution, specific safeguards to guarantee the protection of personal data, especially sensitive ones involved in criminal investigations.¹⁸ In order to protect privacy and other rights, both direct violence against technological security by public security agents¹⁹ and the use of “backdoors”²⁰ for investigation through the breaking or manipulation of encryption must be prohibited.

All the investigative mechanisms must respect due legal process, with contradictory and broad defense, giving the person being investigated the right to question the need, proportionality and legality of the evidence to be produced. Thus, authorization to use mechanisms for breaking or manipulating encryption, in exceptional order, must be done under court order, ensuring the possibility of a concise and broad defense. These are the minimum bases of criminal procedural law in a democratic state of law.²¹

Such decisions should be based on an understanding of the risk exposure of children and adolescents, particularly among more vulnerable groups, such as the LGBTQIA+ community, both perceived and self-identified. Information that attests to their gender

18 In relation to the current precarious situation regarding the protection of personal data in the context of criminal proceedings in Brazil, see SANTARÉM, Paulo Rená da Silva. *Digital Constitucionalismo Digital na Relação entre Dados Pessoais e Direito Penal no Brasil: Diagnósticos, Perspectivas e um Chamado*. In CRUZ, Francisco Brito (ed.); SIMÃO, Bárbara (ed.). **Direitos Fundamentais e Processo Penal na Era Digital – Doutrina e Prática em debate, Vol. 6**. São Paulo: InternetLab, 2023. Pp. 114-127. Available at <https://congresso.internetlab.org.br/wp-content/uploads/2023/09/Direitos-Fundamentais-e-Processo-Penal-na-era-digital-Volume-6.pdf-.pdf>. Accessed on Aug. 27, 2024.

Regarding problematic issues in the treatment of biometric and genetic data in the routine of public security and criminal justice, see FRAGOSO, Nathalie; TAVARES, Clarice. *A Lei Anticrime e o processamento de dados genéticos biométricos pelo estado brasileiro: um projeto em expansão*. In CRUZ, Francisco Brito (ed.); FRAGOSO, Nathalie (ed.). **Direitos Fundamentais e Processo Penal na Era Digital – Doutrina e Prática em debate, Vol. 3**. São Paulo: InternetLab, 2020. Pp. 350-361. Available at https://congresso.internetlab.org.br/wp-content/uploads/2020/08/InternetLab_Volume-3_Pa%E2%95%A0%C3%BCg_Simples_Alta.pdf. Accessed on Aug. 27, 2024.

19 RODRIGUES, Gustavo Ramos. **Acesso policial a celulares no Brasil e a banalização da “criptoanálise de mangueira de borracha”**. IRIS - Instituto de Referência em Internet e Sociedade, 26 Oct. 2022. Available at <https://irisbh.com.br/acesso-policial-a-celulares-no-brasil-e-a-banalizacao-da-criptoanalise-de-mangueira-de-borracha/>. Accessed on 09 Jul 2024.

20 SANTARÉM, Paulo Rená da Silva. **“Portas clandestinas”: uma tradução mais precisa para debatermos backdoors em criptografia**. Blog: Instituto de Referência em Internet e Sociedade. 17 Jan. 2022. Available at: <https://irisbh.com.br/portas-clandestinas-uma-traducao-mais-precisa-para-debatermos-backdoors-em-criptia/>. Accessed on: 10 Oct. 2022.

21 PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. **Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Available at: <https://bit.ly/3kGTde3>. Accessed on 16 August. 2024.

identities and sexualities can expose them to new forms of violence, including from family members and guardians.

It is recommended that the MERCOSUR member states, from the outset of criminal investigations, respect the principles inherent to due process and only access digital devices and systems—especially when involving data of children and adolescents—through a duly substantiated court order, in light of the principles of purpose, necessity, legality, and proportionality. This ensures comprehensive protection through investigative means that do not compromise the attributes of encryption, such as the analysis of metadata.

D. Respecting legality, proportionality, necessity, and multisectorial dialogue when formulating public safety policies and strategies regarding monitoring, surveillance, and access to instant messages and encrypted content is essential for the protection of children and adolescents

The formulation of public security policies and strategies aimed at monitoring and accessing instant messages and encrypted content must respect fundamental rights. First, all measures must strictly comply with current legislation. Furthermore, they must be adequate and necessary to achieve the intended objectives, preventing abuse and excessive surveillance by state authorities. Finally, the implementation of policies and strategies should only occur if there are no less invasive alternatives available.

In specific cases regarding the protection of children and adolescents,²² it is imperative that these principles are strictly observed, especially in relation to this public, whose vulnerability demands integral protection against any undue access to their private life or personal data, for example. All fundamental rights of children and adolescents are universal, indivisible and interconnected, valid everywhere in the world, including MERCOSUR.²³

In this regard, public safety policies—defined as sets of principles, guidelines, and objectives that condition the plans and strategies to be implemented in an integrated and coordinated manner for the preservation of rights—should be constructed through

22 PEREIRA, Marcos César Martins; AMARAL, Pedro; CANTO, Mariana. **Discutir criptografia e a proteção de crianças e adolescentes é urgente.** ObCrypto, 2023. Available at: <https://obcrypto.org/discutir-criptografia-e-a-protecao-de-criancas-e-adolescentes-e-urgente/>. Accessed on 08/26/2024.

23 CRIN - Child Rights International Network; Defend Digital Me. **Privacy and Protection: a children's rights approach to encryption.** 19 Jan. 2023. Available at <https://home.crin.org/readlistenwatch/stories/privacy-and-protection>. Accessed on 20 Jun. 2024.

multidisciplinary debate. This includes holding public hearings open to contributions from specialists in various relevant fields. In this context, in addition to respecting existing regulations, the multiple perspectives of civil society, academia, the public sector, and the private sector must be taken into account.

It is recommended that States, especially at the legislative level, exercise caution and discretion in the use of surveillance and data access tools, always prioritizing the unrestricted defense of individuals' fundamental rights and respecting the principles of legality, proportionality and necessity. **It is also recommended** that impact assessments be conducted regarding the rights of children and adolescents in the formulation of public safety and criminal prosecution policies and strategies that involve monitoring, criminal investigation, and access to instant messages and encrypted documents for their protection.

Finally, **it is recommended** that the development of public policies include input from experts in digital technology, internet governance, data management, information security, and other professionals from various sectors of society and fields of knowledge dedicated to strengthening the rights of children and adolescents.

E. Consider scientific data, assess impact and promote social participation in the proposition of technological artifacts²⁴ for the local context

In Brazil, Argentina, Paraguay, Uruguay and Venezuela, digital infrastructure and internet access are constantly evolving, along with social, cultural and technological realities.²⁵ Legal or technological interventions must be flexible and sensitive to gradual changes, long-term constancies, and emerging threats. Therefore, the online protection of children and adolescents depends on updated and consistent data that reflect the reality of the conditions and challenges.

More than the collaboration of different sectors, including governments, the private sector, academia and civil society, considering empirical studies and trend analysis is an indispensable tool for identifying prevalent dangers and the most effective ways to address them. Public policies, corporate initiatives, research, and advocacy should not be guided solely by the individual impressions of decision-makers or simply reflect proposals imported from the Global North that do not address the challenges posed by the local contexts of MERCOSUR.²⁶

24 Technological artifacts are understood as private or public actions, carried out or proposed, to solve problems involving the themes of encryption and protection of children and adolescents in digital environments.

25 In [CITAR RELATÓRIO FINAL].

26 CARMO, Paloma; DUARTE, Felipe; GOMES, Ana Bárbara. **Digital Inclusion as Public Policy: Brazil and South America in perspective**. Reference Institute for Internet and Society: Belo Horizonte (MG), 25

Regarding adaptation to the local reality, for example, the existence of active helplines and support systems does not eliminate the need for prevention and digital education solutions. Additionally, legal provisions for parental control tools alone do not include explicit rules on how to ensure respect for strong encryption.

In summary, the online protection of children and adolescents requires approaches based on rigorous scientific research, updated data, and assessments of risks and opportunities.²⁷ It is, therefore, up to the public authorities not only to identify and promote but also to take on the production of scientific data – especially disaggregated data on social markers such as race, class and gender – that can inform both public and private decisions in the sector.

It is recommended that states and private companies base proposals for technological interventions regarding the protection of children and adolescents in digital environments on scientific research, updated data, and impact assessments, preferably incorporating input from experts across various fields of knowledge.

F. Prohibiting or imposing strict parameters on the allowance of breaking or compromising encryption in criminal investigations and prosecutions

Specifically observing digital investigation methods, the increasing use of intrusive tools exceeds the traditional legal rules for interception. This mismatch threatens fundamental human rights such as freedom of expression, privacy and free association,²⁸ and it also impacts due process, given the risk of manipulating digital evidence to the detriment of the integrity of proof. Even alternative mechanisms to breaking encryption for criminal investigation and surveillance – such as client-side scanning²⁹ and government hacking³⁰ – threaten the confidentiality of private communications and privacy, according to the report “*The right to privacy in the digital age*”, from the Office of the UN High Commissioner for Human Rights.³¹

May 2020. Available at <https://irisbh.com.br/publicacoes/inclusao-digital-como-politica-publica-brasil-e-america-do-sul-em-perspectiva/>. Accessed on 26 Aug. 2024.

27 CRIN - Child Rights International Network; Defend Digital Me. **Privacy and Protection: a children’s rights approach to encryption**. 19 Jan. 2023. Available at <https://home.crin.org/readlistenwatch/stories/privacy-and-protection>. Accessed on 20 Jun. 2024.

28 LIGUORI, Carlos. **Direito e Criptografia: direitos fundamentais, segurança da informação e os limites da regulação jurídica na tecnologia**. São Paulo: SaraivaJur, 2022.

29 Scanning mechanism performed on user devices in environments protected by encryption to identify when illicit materials are shared.

30 Procedure for exploiting vulnerabilities and flaws in systems, accessing personal data and private content on electronic devices and systems, by state institutions and authorities.

31 UN – United Nations Organization. **O direito à privacidade na era digital. Relatório do Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos (A/HRC/51/17)**. Trad. DUTRA, Luiza;

Public security and criminal prosecution institutions that support breaking encryption or alternative methods, even for the protection of children and adolescents, may ultimately undermine the defense of rights such as privacy through mass surveillance. Society would lack the means to monitor and measure the use of digital tools for this purpose in the handling of personal data, as well as their impact on vulnerable groups, especially under authoritarian and repressive states regarding race, gender, and sexuality. The protection of children and adolescents also benefits from encryption,³² as its prohibition would expose them to various forms of exploitation and abuse.

Such technologies exploit vulnerabilities, so their use by the State is not even based on strict legality.³³ Thus, ideally, they should not be used at all. From a more pragmatic perspective, given the current scenario, it would at least be necessary that if they are employed for intelligence activities, there should be a strict distinction between the allowance for intelligence operations and the restrictions that impose severe parameters for public security investigations. Therefore, at the normative level, legislative initiatives that could allow for their indiscriminate use should be rejected.

In conclusion, it is **recommended** the total ban on the use of mass surveillance tools for criminal prosecution and investigation by states. If used, it is **recommended** that their application be limited to intelligence activities, with appropriate regulation, conditions, and effective restrictive parameters, restricted exclusively to serious crimes and ensuring that the privacy of children and adolescents is not sidelined.

G. Regulate the role of digital platforms demanding transparency, accountability and shared responsibility in strategies to combat sexual violence against children and adolescents

The principle of shared responsibility³⁴ establishes that the responsibility for the protection of children and adolescents must be shared between the family, society and the State. Therefore, in the information society, it is up to digital platforms that offer online communication services to take an active and responsible role in preventing

SANTARÉM, Paulo Rená da Silva. Geneva: UN, 04 Aug. 2022. Original publication in <https://digitallibrary.un.org/record/3985679?ln=en>. Available at <https://irisbh.com.br/publicacoes/o-direito-a-privacidade-na-era-digital-traducao-do-relatorio-do-gabinete-do-alto-comissariado-das-nacoes-unidas-para-os-direitos-humanos>. Accessed on 16 Jul 2024.

32 SILVA, Isabela Inês Bernardino de Souza. **Criptografia é segurança para crianças e adolescentes: não está claro?** ObCrypto, 2020. Available at <https://obcrypto.org/criptografia-e-seguranca-para-criancas-e-adolescentes-nao-esta-claro/>. Accessed on Aug. 27, 2024.

33 PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. **Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Available at <https://bit.ly/3kGTde3>. Accessed on: 27 Aug. 2024.

34 INSTITUTO ALANA. Responsabilidade compartilhada. **Glossário do Instituto Alana**, 2024. Available at <https://alana.org.br/glossario/responsabilidade-compartilhada/>. Accessed on 22 Aug. 2024.

sexual violence against children and adolescents. A provision for specific legal rules for this responsibility of the platforms could enable the requirement for them to operate in a transparent and effective manner.

High levels of active and passive transparency in the practices of digital platforms would enhance the prevention of sexual violence through consistent and widespread knowledge of privacy policies, terms of service, and protection mechanisms in each online environment.³⁵ Understandable and accessible formats would help ensure that not only children and adolescents, but also their guardians, understand their rights and the responsibilities of companies, promoting a safer digital environment.

This transparency would enable more effective accountability. Society would be able to monitor companies' actions, recognizing any challenges faced, but primarily holding them accountable for omissions in developing and applying strategies to combat sexual violence against children and adolescents.

In turn, the predictability and proportionality of this accountability depends on a previous legal definition of the extent and depth of responsibility required from companies. Clear legislation should impose requirements and criteria for performance, such as content moderation that violates the rights of children and adolescents, and age verification for access to inappropriate digital environments. It should also establish deadlines for the required actions and mechanisms for collaboration with the competent authorities.³⁶

Furthermore, public policies must be formulated taking into account the role of the private sector. For example, encouraging investment in research, development and sharing of new technologies in the area could improve performance in detecting content to be moderated.

It is recommended that there be specific regulation regarding the role of digital platforms in the protection of children and adolescents, in light of the shared responsibilities inherent in the doctrine of integral protection. This should require the promotion of high levels of transparency in companies' practices for preventing sexual violence against this population, including the dissemination of terms of service in understandable and accessible formats.

35 KURTZ, Lahis Pasquali; CARMO, Paloma Rocillo Rolim do; VIEIRA, Victor Barbieri Rodrigues. **Transparência na moderação de conteúdo: tendências regulatórias nacionais**. Instituto de Referência em Internet e Sociedade, 05 Jul. 2021. Available at <https://irisbh.com.br/publicacoes/transparencia-na-moderacao-de-conteudo-tendencias-regulatorias-nacionais/>. Accessed on Aug. 27, 2024.

36 CRIN - Child Rights International Network; Defend Digital Me. **Privacy and Protection: a children's rights approach to encryption**. 19 Jan. 2023. Available at <https://home.crin.org/readlistenwatch/stories/privacy-and-protection>. Accessed on 20 Jun. 2024.

H. Regulate the online protection of children and adolescents in a specific approach, taking into account the diversity of contexts, including regional differences

Platform self-regulation has proven insufficient,³⁷ especially on topics related to ensuring the safety of citizens.³⁸ Understanding that the digital space is a potential environment for violence, it is essential to recognize the role of states in formulating policies aimed at prevention, promotion, and accountability of individuals involved in sexual violence against children and adolescents in online settings.³⁹

All MERCOSUR countries have in their legal frameworks aimed at combating the spread of online sexual violence content against children and adolescents.⁴⁰ However, the digital space has been used as a pathway to access the youth population or as a means for the commercialization of violence, creating a profitable market not only for those directly involved in the acts of violence but also for the platforms that benefit, to some extent, from the increase and frequency of users.

In light of this scenario, countries need to advance toward building regulatory policies that ensure the sexual and digital rights of children and adolescents in online environments. Specific risks should be considered, such as the potential use of Global South countries as facilitating routes for the commercialization of child sexual abuse material.⁴¹

It is recommended that MERCOSUR member states establish specialized regulations for the protection of children and adolescents in the digital context, taking into account the risks and opportunities of the online environment, as well as the ongoing connection between the “offline” and “online” worlds, so that the asymmetries and violence present in one are directly mirrored in the other.

It is also recommended that the specific political, economic, social, and cultural contexts

37 TIBURTINO, Glauber. **Por que regular a internet é preciso?** Radis, 01 Oct. 2023. Available at <https://radis.ensp.fiocruz.br/reportagem/direito-a-comunicacao/por-que-regular-a-internet-e-preciso/>. Accessed on 27 Oct. 2024.

38 DUTRA, Luiza Correa de Magalhães. **Tecnologias e Segurança Pública: debates sobre policiamento, privacidade, vigilância e controle social.** Instituto de Referência em Internet e Sociedade, 09 Jan. 2023. Available at <https://irisbh.com.br/tecnologias-e-seguranca-publica-debates-sobre-policiamento-privacidade-vigilancia-e-controle-social/>. Accessed on Aug. 27, 2024.

39 CRIN - Child Rights International Network; Defend Digital Me. **Privacy and Protection: a children’s rights approach to encryption.** 19 Jan. 2023. Available at <https://home.crin.org/readlistenwatch/stories/privacy-and-protection>. Accessed on 20 Jun. 2024. p. 9-10.

40 See DUTRA, Luiza Correa de Magalhães; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues; PEREIRA, Wilson Guilherme Dias. **Fact Sheet: Normative artifacts on children and adolescents’ rights in MERCOSUR digital environments.** Belo Horizonte: Internet and Society Reference Institute, 01 Aug. 2024. Available at <https://irisbh.com.br/en/publicacoes/fact-sheet-normative-artifacts-on-children-and-adolescents-rights-in-mercosur-digital-environments/>. Accessed on 20 Sep. 2024.

41 Ver [CITAR RELATÓRIO FINAL].

in which children and adolescents are situated be taken into account. Furthermore, the establishment of regional cooperation policies within MERCOSUR to create minimum standards among countries is advised, recognizing privacy as a fundamental and progressive element for children and adolescents. Finally, such regulations should consider parameters for prevention, promotion, and accountability, avoiding the formulation of norms that are solely criminal in nature, as these alone are insufficient to dismantle all illegal trade in child and adolescent sexual violence content.

I. Promote national and regional debate rounds on the topic, with multisectoral participation and, preferably, incorporating the perspectives of children and adolescents affected by the policies

It is vital to recognize the role of MERCOSUR in the construction of economic and social policies in the regional scenario, especially in South America.⁴² Cooperation policies among countries have laid the foundation for the development of member states, even sparking the interest of other countries, such as Bolivia, that were not previously part of the regional cooperation to join.⁴³

Member countries of this bloc have demonstrated significant influence over regional and international politics. Therefore, building a national and regional debate agenda on the topics of information security and the protection of children and adolescents in the digital context could gain prominence on the common agenda of these countries.

This prominence could transform the current landscape of legislative and technological scarcity⁴⁴ highlighting the ongoing challenges in the realm of youth public safety, while facilitating the comprehensive protection of children and adolescents through digital security. should transcend the common bilateral method in international relations and involve experts from various sectors: civil society, governments, companies, technical

42 The Southern Common Market (MERCOSUR) is a regional integration initiative initially formed by Argentina, Brazil, Paraguay and Uruguay, and later joined by Venezuela and Bolivia, currently in the accession process. The official languages are Spanish and Portuguese, with Guarani also incorporated since 2006. MERCOSUR's main objective is to create a common space that promotes commercial and investment opportunities through the integration of national economies into the international market. He signed several agreements with countries or groups of countries, granting them Associated State status in some cases, as is the case with South American countries. Furthermore, MERCOSUR has signed commercial, political and cooperation agreements with several nations and organizations around the world. In MERCOSUR. **Quem somos em poucas palavras.** Available at: <https://www.mercosur.int/pt-br/quem-somos/em-poucas-palavras/>. Accessed on: 19 June. 2024.

43 **MERCOSUL.** Bolívia ingressa no MERCOSUL. Available at <https://www.mercosur.int/pt-br/bolivia-ingressa-no-mercosul/>. Accessed on 20 Aug. 2024.

44 DUTRA, Luiza Correa de Magalhães; SANTARÉM, Paulo Rená da Silva; VIEIRA, Víctor Barbieri Rodrigues; PEREIRA, Wilson Guilherme Dias. **Fact Sheet: Normative artifacts on children and adolescents' rights in MERCOSUR digital environments.** Belo Horizonte: Internet and Society Reference Institute, 01 Aug. 2024. Available at <https://irisbh.com.br/en/publicacoes/fact-sheet-normative-artifacts-on-children-and-adolescents-rights-in-mercosur-digital-environments/>. Accessed on 20 Sep. 2024.

and scientific sectors, as well as international organizations, such as UNICEF, ITU, UNESCO, etc. In disciplinary terms, specialists in digital security, child psychology, law, education and other relevant fields should be consulted⁴⁵ to gather insights for a mosaic of consistent technical and practical perspectives, incorporating local cultural and political traits.

Finally, it is imperative that this process recognizes the voice of children and adolescents through active listening during the development of public policies aimed at their protection. Understanding the unique experiences and perceptions of these individuals reveals needs and challenges that may not be fully considered by adults. This understanding enables the creation of normative and technological artifacts that are genuinely useful and suited to the demands of this age group.

Thus, it is **recommended** that MERCOSUR member states adopt policies and actions that involve rounds of debate, multisectoral forums, workshops and other instruments that can provide opportunities for the socialization of experiences between countries and their different social actors involved with the highlighted themes. Attention should be given to the different perspectives presented, producing documents that can support the formulation of regional and national policies on the subject.

J. Promote public policies for meaningful connectivity and digital literacy for children and adolescents

The unequal reality of access to digital technologies in MERCOSUR countries⁴⁶ raise the demand for public policies for digital inclusion guided by the concept of meaningful connectivity,⁴⁷ with efforts aimed at offering connection infrastructure, people's access to electronic devices, availability of fast connections and the capacity for technological appropriation.⁴⁸ Otherwise, the risks of the information society may manifest themselves in an increasingly serious manner, heightened by the precariousness of digital literacy, especially for children and adolescents, due to their peculiar condition as developing people.

45 CRIN - Child Rights International Network; Defend Digital Me. **Privacy and Protection: a children's rights approach to encryption.** 19 Jan. 2023. Available at <https://home.crin.org/readlistenwatch/stories/privacy-and-protection>. Accessed on 20 Jun. 2024. p. 9-10.

46 CARMO, Paloma; DUARTE, Felipe; GOMES, Ana Bárbara. **Inclusão Digital como Política Pública: Brasil e América do Sul em perspectiva.** Instituto de Referência em Internet e Sociedade: Belo Horizonte (MG), 25 May. 2020. <https://irisbh.com.br/publicacoes/inclusao-digital-como-politica-publica-brasil-e-america-do-sul-em-perspectiva/>. Accessed on: 21 Aug. 2023.

47 GOMES, Ana Bárbara; GERTRUDES, Júlia; ROCILLO, Paloma. **Conectividade Significativa em Comunidades Brasileiras.** Relatório. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2022. 35 p. Available at <https://bit.ly/3e8lWsK>. Accessed on: August 21, 2024.

48 GOMES, Ana Bárbara; GERTRUDES, Júlia Maria Caldeira; SILVA, Lucas Samuel da; SANTARÉM, Paulo Rená da Silva. **Apropriação tecnológica no Brasil: uma perspectiva do Sul Global sobre inclusão digital e empoderamento de comunidades.** Instituto de Referência em Internet e Sociedade, 10 Sep. 2023. Available at <https://bit.ly/3RINQgt>. Accessed on Aug. 27, 2024.

The current equal exercise of citizenship depends on the public authorities providing quality internet connectivity and access to appropriate technological devices, regardless of socioeconomic status. However, this task is only the first step. States must ensure a set of measures and tools, as a standard, for training, guidance, and protection throughout these digital inclusion processes, so as not to perpetuate the fallacy that individuals are “digital natives”—naturally equipped to be and interact online. This includes concerns about screen time and other challenges faced by many families, who need to rely on resources and support programs to establish healthy and safe practices for themselves and for children and adolescents.

It is essential to ensure access to educational programs that teach digital skills, online safety, and internet ethics. This is crucial for empowering children and adolescents to navigate and interact safely and consciously in digital environments, as well as to recognize the importance of technological security, including strong encryption and how to use it for their protection. An adequate level of knowledge allows for dialogue, partnership, and transparency in the home regarding the use of technological tools for protection and parental mediation on the devices and platforms used by children and adolescents, respecting their progressive autonomy in adopting content filters, monitoring activities, and being alerted to online risks.

It is the responsibility of the state, through a multisectoral and multidisciplinary approach, to establish guidelines and best practice parameters for online protection, taking on the shared commitment to coordinate and complement efforts in regulation and the implementation of public policies. This scenario requires normative harmony to avoid any overlap of work and, above all, to effectively reach all individuals in their various uses of the internet while strengthening rights.

It is recommended that the MERCOSUR states develop public policies for meaningful connectivity that, by providing quality internet access, promote a safe and educationally enriching digital environment for children and adolescents, with their active participation, in coordinated collaboration with the state, families, and society, including digital platforms.

It is also recommended that the MERCOSUR states and companies operating in the region adopt public policies and private initiatives that promote digital literacy for children and adolescents as part of a digital inclusion initiative. This aims to ensure not only access to meaningful connectivity and appropriate devices but also training in digital skills, technological safety, and ethical conduct, preventing risks that could violate the rights of this population.

iris

INSTITUTE
FOR RESEARCH
ON INTERNET
AND SOCIETY