

Information Security and Children and Adolescents Protection

Narratives and Regulatory
Proposals in MERCOSUR



Information Security and Children and Adolescents Protection

Narratives and Regulatory Proposals in MERCOSUR

AUTHORSHIP

Luiza Correa de Magalhães Dutra
Paulo Rená da Silva Santarém
Victor Barbieri Rodrigues Vieira
Wilson Guilherme Dias Pereira

REVISION

Ana Bárbara Gomes Pereira
Fernanda dos Santos Rodrigues Silva

EXTERNAL REVIEW

Emanuella Ribeiro Halfeld Maciel
Veridiana Alimonti

TRANSLATION

Luiza Correa de Magalhães Dutra
Paulo Rená da Silva Santarém

GRAPHIC DESIGN, COVER, LAYOUT AND FINALIZATION

Felipe Duarte

EDITORIAL PRODUCTION

Internet and Society Reference Institute

HOW TO CITE IN ABNT

DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson
Guilherme Dias; SANTARÉM, Paulo Rená da Silva; VIEIRA,
Victor Barbieri Rodrigues. **Information Security and
Children and Adolescents Protection: Narratives and
Regulatory Proposals in MERCOSUR**. Belo Horizonte:
Institute dor Research on Internet and Society, 2024.
Available at: <https://bit.ly/3ZpjZNY>. Accessed at: dd mmm.
YYYY.





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	5
EXECUTIVE SUMMARY	8
1. INTRODUCTION	9
2. METHODOLOGY	12
2.1. Procedures and methodological paths	13
2.2. Theoretical framework	16
2.3. Research limitations	19
3. RESULTS	19
3.1. Common Normative Artifact: Convention on the Rights of the Child	20
3.2. Argentina	21
Interviews	21
Normative artifacts	23
3.3. Brazil	25
Interviews	25
Normative artifacts	30
3.4. Paraguay	34
Interviews	34
Normative artifacts	37
3.5. Uruguay	39
Interviews	39
Normative artifacts	41
3.6. Venezuela	42
Interviews	42
Normative artifacts	44
3.7. MERCOSUR	48
3.7.1. Specific debate on the intersection of the topics	48
3.7.2. Normative and technological artifacts	52
4. FINAL CONSIDERATIONS	55
5. REFERENCES	57
6. APPENDIX 1 - INTERVIEW SCRIPT	70
7. APPENDIX 2 - ATLAS.TI ANALYSIS CODES	72

Presentation

The Internet and Society Reference Institute (IRIS) is an independent and interdisciplinary research center, founded in 2015, dedicated to producing and communicating scientific knowledge on Internet and society issues, and to defending and promoting public policies that advance human rights in the digital realm. Our work seeks to qualify and democratize debates about the Internet, society, and new technologies by providing scientific input to Internet users and the various sectors that make up society: government, civil society, the private sector, and the technical and academic community.



In this context, our project **Information Security and Children and Adolescents Protection: Narratives and Regulatory Proposals in MERCOSUR¹** aimed to analyze the existing political debates on the protection of children and adolescents in environments with encryption, going beyond the common polarization between the two fields, and understanding which strategies are being discussed for the online safety of children and adolescents, particularly regarding the fight against sexual violence in the digital context. We intend to understand whether it is possible to combine personal data protection with the safety of children and adolescents, without compromising privacy and without resorting to mass surveillance practices. Specifically, we aim to: 1) understand the normative and technological artifacts related to the protection of children and adolescents in encrypted digital environments in MERCOSUR;² 2) systematize and analyze the narratives of experts in these two fields of knowledge; and 3) produce recommendations for the development of public security policies focused on the protection of children and adolescents in digital environments.

1 This project is financed by META. All IRIS projects are carried out independently, in accordance with research ethics parameters such as replicability, scientificity and those described in the Institute's statute. All results are published and available freely and without any intervention or, under any circumstances, prior approval from the funding institution.

2 The first consolidated results to this end have been published in DUTRA, Luiza Correa de Magalhães; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues; PEREIRA, Wilson Guilherme Dias. **Facht Sheet: Normative Artifacts on children and adolescents' rights in MERCOSUR Digital environments.** Belo Horizonte: Internet and Society Reference Institute, 2024. Available at: <https://bit.ly/3VsxQzz>. Accessed on: 15 Jul. 2024.

In this scientific report, we present the final result of our reflections and analysis on how MERCOSUR countries have been developing tools to deal with sexual violence against children and adolescents in digital environments.

The preliminary results of this study were released in four key moments: the first three involved the publication of three blog posts aimed at disseminating the partial results of the research using simplified language that could connect with the target audience of the report, creating a process of familiarization with the contents worked on, especially given the technical production gap in MERCOSUR. The published texts covered: (1) the theoretical framework of sexual violence against children and adolescents;³ (2) the National Day to Combat Sexual Violence against Children and Adolescents in Brazil, May 18, and our participation in the Public Hearing on Bill 2628/2022 in the Brazilian Senate;⁴ and (3) the methodological paths followed in the construction of the theoretical encryption framework.⁵ The fourth moment of dissemination of preliminary results was the publication of the *Fact Sheet: Normative artifacts on children and adolescents' rights in MERCOSUR digital environments*, which systematized legislation and bills related to the topic in MERCOSUR countries.⁶

In the course of this process, we have already had the opportunity to share our thoughts at two public hearings. First, on May 14, 2024, in the Senate's Communication and Digital Law Committee, we took part in the debate on Bill 2628/2022 on the online protection of children and adolescents.⁷ Second, on June 11, 2024, we were at the Federal Supreme Court, debating the *Arguição de Descumprimento de Preceito Fundamental* ("Claim of Non-compliance with Fundamental Precept", in english) nº 1143, on the regulation for the use of secret monitoring tools for personal communication devices, such as cell phones and tablets, by agencies and public agents.⁸

The steps that preceded this report were aimed at disseminating the partial findings with the intention of intervening in the public agenda and bringing the rights of children and adolescents to the center

3 PEREIRA, Wilson Guilherme Dias; VIEIRA, Victor Barbieri Rodrigues. **Violência Sexual Online e Criptografia**. *Instituto de Referência em Internet e Sociedade*, 05 Mar. 2024. Available at <https://irisbh.com.br/violencia-sexual-online-e-criptografia/>. Accessed on 15 Jul. 2024.

4 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.

5 SANTARÉM, Paulo Rená da Silva; PEREIRA, Wilson Guilherme Dias. **Caminhos da pesquisa: nossos marcos teóricos para criptografia**. *Instituto de Referência em Internet e Sociedade*, 01 Jul. 2024. Available at <https://irisbh.com.br/marcos-teoricos-para-criptografia/>. Accessed on 15 Jul. 2024.

6 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, 2024. Available at: <https://bit.ly/3VsxQzz>. Accessed on: 15 Jul. 2024.

7 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.

8 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.

of the debate on encryption. These steps were essential to present and contextualize the importance of this research to the target audience. In this final phase, we intend to present a comprehensive compilation of the findings as well as a more in-depth analysis.

From the conclusion of this research, we at the Internet and Society Reference Institute - IRIS propose dialogues with different sectors in order to build understandings on these two fields of analysis and research that have gained notoriety in recent years, always guided by scientific evidence and respect for human rights. Finally, our project also includes monitoring and contributing to the legislative debate on the subject.

Executive summary

- In the political and legal field, the protection of children and adolescents in digital environments tends to be placed in opposition to the defense of technological security through encryption. However, while encryption can complicate criminal investigations, it can also protect children and adolescents from violence, protect them from threats, and guarantee their human rights to privacy, freedom of expression, education, and personality development. This ambivalence affects several aspects of guaranteeing their rights and of their online interaction.
- This project sought to analyze and explore how this dispute occurs and the development of legislation and technology to protect children and adolescents in digital environments with encryption in MERCOSUR countries. We considered encryption and sexual violence against children and adolescents as key concepts for analysis. Our object of analysis included semi-structured interviews with experts, normative artifacts—legal norms and bills that help understand how each of the central themes, or their intertwining, is regulated by the state or legislatively debated—and technological artifacts—digital mechanisms in online environments, which affect encryption, aimed at combating digital sexual violence against children and adolescents—in the region. The methodology included bibliographic and documentary analysis and interviews with experts from the bloc’s countries;
- We conclude that MERCOSUR countries face significant gaps in the normative and technological protection of the rights of children and adolescents in digital environments with encryption, especially against online sexual violence. Legislative debates are rare and incipient at this intersection, with little direct public participation from this public, reflecting challenges in guaranteeing rights and in fully recognizing these individuals as active subjects of law, capable of influencing public policies.
- In the general legal context, countries follow the international legislation established by the United Nations (UN) Convention on the Rights of the Child, but the practical implementation of these rights varies, with Brazil as a center for more robust debates in this area.
- During the research, no specific technological artifacts were found for tackling sexual violence against children and adolescents in the digital environment with encryption, but only mechanisms unrelated to the functioning of encryption on digital platforms and an unimplemented legal provision.

1. Introduction

From the end of the 20th century there has been intense debate in the world about the public availability of strong encryption to protect private communications, with proposals for mechanisms for exceptional access by state investigation and criminal prosecution agencies.⁹ Such proposals have generated significant controversies due to their legal, political and economic impacts, called “crypto wars”,¹⁰ and faced resistance from the technical community, the private sector, activists, and digital human rights researchers.

The increasing use of digital technologies by Public Security institutions is becoming a priority on political agendas, especially with regard to the legitimate protection of children and adolescents against violence through digital means. But the proposals of these public bodies – including weakening encryption¹¹ and carry out mass surveillance and social control – reflect the political disputes surrounding the technological tools that can be used and the laws to be formulated, putting fundamental rights such as freedom of expression, access to information and protection of personal data at risk, particularly harming vulnerable groups, including children and adolescents.

In this sense, in the Private Communications, Investigations and Rights project, of the Internet and Society Reference Institute - IRIS, between 2022 and 2023, we seek to offer subsidies and recommendations for this political and legal debate, matching security in information and communication technology (ICT) with the protection of human rights. In systematic bibliography reviews, we evaluated impacts and risks of three mechanisms for investigating private communications that circumvent attributes of encryption: traceability of instant messages,¹² hacking governmental¹³ and client-side scanning.¹⁴

9 Exceptional access refers to the digital mechanisms used by state investigation and prosecution agencies to obtain data from environments protected by encryption, through doors that are intended to be inaccessible to other people. Among them, the following are central in academic debates: i) traceability of instant messages; b) client-side scanning; c) government hacking.

10 LIGUORI, Carlos. **Direito e Criptografia: direitos fundamentais, segurança da informação e os limites da regulação jurídica na tecnologia**. São Paulo: SaraivaJur, 2022. Pp. 109-150.

11 The United Nations - UN has been consolidating a history of positions on the subject of encryption, ranging from the Report by David Kaye, UN Special Rapporteur on rights of assembly and association, in 2015, to the most recent document, from 2022, written by the UN Office of the High Commissioner for Human Rights, which recalls previous considerations on encryption and presents new perspectives on the right to privacy in the context of information and communication technologies. Check it out at: UN – United Nations Organization. **The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/51/17)**. Geneva: UN, 04 Aug. 2022. Available at <https://digitallibrary.un.org/record/3985679?ln=en>. Accessed on 16 Jul. 2024.

12 RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. **Comunicações privadas, investigações e direitos: rastreabilidade de mensagens instantâneas**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, May 2022. Available at <https://irisbh.com.br/publicacoes/comunicacoes-privadas-investigacoes-e-direitos-rastreabilidade-de-mensagens-instantaneas/>. Accessed on 30 Nov. 2022.

13 DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. **Hacking Governamental: uma revisão sistemática**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, Feb. 2023. Available at <https://bit.ly/3YdVcIL>. Accessed on 26 June 2024.

14 PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Rená da Silva;

In this research, we saw narrative disputes between ICT security, privacy and protection of children and adolescents in digital environments. In some works, tools supposedly alternative to breaking encryption were defended in narratives and political actions for the online protection of this public.¹⁵ On the other hand, these same alternatives were considered violators of guarantees such as the presumption of innocence and secrecy of communications, especially of human rights defenders and political actors. The question of how to protect children and adolescents in digital environments with encryption has arisen – a question that led to the creation of this research, called **Information Security and Protection of Children and Adolescents: Narratives and Regulatory Proposals in MERCOSUR**.

In today's world, proposals for online safety of children and teenagers are controversial. For example, the United States has been discussing the "Children and Teens' Online Privacy Protection Act 2.0" (COPPA 2.0), the "Kids Online Safety Act" (KOSA) and the "Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment" (STOP CSAM Act), in order to expand parental control and the responsibility of platforms for the safety of children and adolescents.¹⁶ But the bills have been criticized by civil and academic organizations,¹⁷ as they increase data collection from children and adolescents, and categorize materials with the LGBTQIAPN+ theme as risky content. These issues also emerge in Brazil, around Bill N° 2.630, of 2020, which regulates platforms, and Bill 2628/2022, on the integral protection of children and adolescents in the digital environment.

On this topic, in the report "*Privacy and Protection: A children's rights approach to encryption*",¹⁸ Child

VIEIRA, Victor Barbieri Rodrigues. **Varredura pelo lado do cliente: uma revisão sistemática**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, Nov. 2022. Available at <https://irisbh.com.br/publicacoes/comunicacoes-privadas-investigacoes-e-direitos-varredura-pelo-lado-do-cliente/>. Accessed on: 30 Nov. 2022. p.5.

15 When we use the terms "online protection" or "online environment" we are aware of the possibility that violence suffered online reverberates offline and vice versa. We understand that the idea of a supposed separation between the virtual and "real" world has a symbolic charge that hides the reality, in which these barriers are not so clear, and both "worlds" can be equally affected in an action of violence. However, we have adopted the term "online" in the text because we understand the need to specify the focus of our investigation, which is on encrypted digital environments that may be involved in the practice of violence both online and offline.

16 FIGUEIREDO, Ana Luiza. Congresso dos EUA avança com medidas de proteção infantil na Internet. **Olhar Digital**. 27 Jul. 2023. Available at <https://olhardigital.com.br/2023/07/27/seguranca/congresso-dos-eua-avanca-com-medidas-de-protecao-infantil-na-Internet/>. Accessed on 20 Jun. 2024. Regarding criticisms of the STOP CSAM Act project, see COPE, Sophia; CROCKER, Andrew; TRUJILLO, Mario. **The STOP CSAM Act Would Put Security and Free Speech at Risk**. Electronic Frontier Foundation, 21 Apr. 2023. Available at <https://www.eff.org/pt-br/deeplinks/2023/04/stop-csam-act-would-put-security-and-free-speech-risk>. Accessed on Aug. 9, 2024.

17 A group of civil society organizations opposed the US bill called KOSA (*Kids Online Safety Act*) due to the harm to LGBTQIAP+ youth. See FIGHT FOR THE FUTURE. **Letter: Civil rights groups reaffirm opposition to KOSA, emphasize continued threat to LGBTQ youth**. 29 Jun. 2023. Available at <https://www.fightforthefuture.org/news/2023-06-29-letter-civil-rights-groups-reaffirm-opposition-to-kosa-emphasize-continued-threat-to-lgbtq-youth>. Accessed on 27 Mar. 2024. The Electronic Frontier Foundation critically analyzed the project based on a constitutional law analysis. See MACKAY, Aaron; KELLEY, Jason. **Analyzing KOSA's Constitutional Problems In Depth**. Electronic Frontier Foundation, 15 Mar. 2024. Available at <https://www.eff.org/deeplinks/2024/03/analyzing-kosas-constitutional-problems-depth>. Accessed on 2 Aug. 2024.

18 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.

Rights International Network (CRIN) and *Defend Digital Me* reveal results of their research, carried out through literature review, interviews, questionnaires and conversations with organizations and experts in child protection, children's rights, digital rights, privacy and data protection, internet regulation and the technology sector. They concluded: a) encryption has uses beyond confidentiality, from anonymity to authentication, and affects children's lives in several areas, such as health, education and leisure; b) the duality of "privacy versus protection" does not hold up, as encryption can also protect children; c) interventions in the digital environment must consider, including assessment of impacts, all children's rights, such as protection against violence, privacy and freedom of expression; d) experts and affected communities, as survivors of child abuse, people or groups that are disproportionately affected by intrusive practices, must be heard in public policy discussions about encryption and ICTs; and e) encryption regulation must be sensitive to different political, economic, social and cultural contexts, and ensure access to justice for children against all violations of their rights online.

Taking a step further, we note the importance of bringing these discussions to the context of the Global South, as the aforementioned report has a European and US-centric vision for the discussion. The field of social and institutional relations specific to Latin America needs to be looked at, especially the MERCOSUR,¹⁹ as a **geographic cutout** from the Global South, objective of this study. By investigating normative and technological artifacts, as well as the perceptions of experts from each country in the bloc, we seek to reflect and analyze how instruments are being developed to deal with the challenges offered by digital platforms, and what are the discursive disputes in the relationship between defense the free use of encryption and strategies for online protection of children and adolescents.

In order to make up for this absence, the **core questions** that guided our project were: a) what are the normative and technological proposals for monitoring encrypted online environments in MERCOSUR in policies to confront violence against children and adolescents?; b) in what social contexts are investigation techniques supposedly alternative to breaking encryption being used?; c) what are the institutional objectives and discourses present in these proposals?; and d) what normative strategies dominate this debate?

Reflecting the political weight and legal parameters of the debate, in this document, we present the results of our investigation, first around each country, and then in a synthesis for the MERCOSUR region, having as central axes the search for normative and technological artifacts, and the perceptions of experts we interviewed, analyzed from the perspective of our theoretical framework.

19 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, this one 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. Several agreements were signed 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 Jun. 2024.

2. Methodology

We aim to identify and understand the MERCOSUR regional scenario to map the relationship between encryption and protection of children and adolescents, analyzing the perceptions of experts in each country: Argentina, Brazil, Paraguay, Uruguay and Venezuela.²⁰ In addition, we seek to identify in national legal frameworks the legal status of encryption and the human rights of children and adolescents; and the existence of technological artifacts, i.e., digital actions or tools for the practical confrontation or investigation of sexual violence against children and adolescents in encrypted environments.

As justification, CRIN; Defend Digital Me detected that, in USA and Europe, the number of regulatory proposals on the digital environment that affect encryption has increased, often motivated by the issue of protecting children and adolescents against online violence. At the same time, they noted the invisibility of this issue in the Global South.²¹

Thus, our specific selection of MERCOSUR for analysis is justified by its historical significance as a strategic space for discussions on data protection in Latin America. We emphasize that Argentina and Uruguay were pioneering countries in the region in aligning themselves with the personal data protection rules defined by the European Union.²² Therefore, it is essential to carry out detailed research on how this topic is addressed in public debate, in legal regulations²³ and the technology applied in the bloc.

20 The study does not address Bolivia, whose incorporation into MERCOSUR is still ongoing, with Brazil being the last country to approve the Accession Protocol, in December 2023. On the other hand, even though it has been suspended since 2016, Venezuela is part of our objective of analysis.

21 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. 93 and 62-63.

22 In 2018, the Council of Europe updated the *Convention 108 for the Protection of Natural Persons with regard to the Automated Processing of Personal Data*, from 1981. The so-called Convention 108+ sought to adapt the provisions of the treaty to new digital technologies and strengthen mechanisms for monitoring compliance with the General Regulation for the Protection of Personal Data. Argentina and Uruguay are part of the short list of non-European countries that have both ratified the original norm (COUNCIL OF EUROPE. **Chart of signatures and ratifications of Treaty 108. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – ETS n° 108.** Available at <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatyenum=108>. Accessed on 20 Aug. 2024) and the updated norm (COUNCIL OF EUROPE. **Chart of signatures and ratifications of Treaty 223. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - CETS n°. 223.** Available at <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatyenum=223>. Accessed on 20 Aug. 2024). On the importance of the updated norm, see FUKU FACHINETTI, Aline; CAMARGO, Guilherme. **Convenção 108+: o tratado de proteção de dados e a relevância do tema para o Brasil.** Revista Consultor Jurídico, 04 Jul. 2021. Available at <https://www.conjur.com.br/2021-jul-04/opiniao-convencao-108-relevancia-protacao-dados/>. Accessed on Aug. 20, 2024.

23 MARQUES, Cláudia Lima; LIMA, Cíntia Rosa Pereira de; PEROLI, Kelvin. **T A proteção de dados pessoais nos Estados-membros do MERCOSUL.** Revista Eletrônica CNJ, Brasília, v. 7, n. 1, p. 45-56, jan./jun. 2023. Available at <https://bdjur.stj.jus.br/jspui/handle/2011/177398>. Accessed on 03 Jul 2024.

2.1. Procedures and methodological paths

We followed three different and intersecting methodological paths: bibliographical research, interviews, and law review. First, we analyzed works to **define the research theoretical framework** and the analysis of the academic debates, in terms of MERCOSUR, that are taking place. After the initial reading of CRIN report – as already explained, we defined the theoretical framework that would support the analysis of our two main conceptual fields: encryption and sexual violence against children and adolescents (for more details, see the next subtopic).

In the second path, we carry out **semi-structured interviews with experts** in the areas of encryption and protection of children and adolescents in the 5 MERCOSUR countries. The interview guide (available in Appendix 1) sought information regarding the existence of a debate on the protection of children and adolescents in digital environments and encryption in the country of the person interviewed. We began our search for interlocutors based on our knowledge of institutions that worked on the topic. At the end of each interview, we ask for recommendations for new people to interview, using the snowball method. Our interview target was 20 people, 4 from each Mercosur country. In total, we contacted 60 institutions and experts and received 17 responses, the total number of interviews carried out. The names of the interviewees presented during our report are pseudonyms, in order to guarantee confidentiality, but without losing sight of the fact that they are real human people, with an identity and distinct voices.

The interviews were transcribed and coded using the Atlas.ti qualitative data analysis software. The codes were divided into seven large blocks for content analysis, corresponding to the following themes: a) whether there are debates about encryption and violence against CA in your country, or whether there are debates about just one of these two topics; b) whether there are notable cases involving the issues; c) whether there are legal norms involving both themes or involving only one of the themes; d) whether there are documents from different sectors of society that deal with the topics; e) whether there are proposed or imposed technological artifacts; f) position of the institution that the person interviewed represents in relation to the topic; g) risks highlighted regarding government measures adopted to protect children and adolescents in encrypted environments. After the interviews, we mapped the legal norms mentioned during the interviews, and paid attention to a more accurate criticality regarding the risks and problems related to information security involving the rights of children and adolescents.

Finally, in the third way, we seek to identify the **normative artifacts** pertinent to each country: any legal norm, in force or under discussion, that allows understanding how each of the central themes, or their intertwining, is regulated by the State or debated legislatively. After our initial search and selection of normative artifacts found, we also added the legal norms and bills mentioned in the interviews (in addition to contributions from external reviewers). In all, We analyzed, through our reading sheet, 39 normative artifacts. In the analyses, we sought to identify the provisions that addressed the main themes and analyze how each theme was addressed. From this perspective, we categorize legislation based on its greatest inclination: when the legislation has legal provisions aimed at children's rights, the norm was highlighted with a thematic focus on *children and adolescents*; When the regulations had a greater correlation with rights to privacy, information security and encryption, their thematic

focus was marked as *encryption*. We also sought to verify whether any existing or proposed regulations would be expected to focus on the intersection of the two themes, presenting any legal provision that would address the intersection of the two themes.

The search for normative artifacts followed three paths. First, in the CRIN **website** we checked the information available on the rights of children and adolescents in MERCOSUR countries. This repository dedicates pages to national Argentina (with data from 2011),²⁴ Brazil (2012),²⁵ Paraguay (2011)²⁶ and Uruguay (2013).²⁷ As there was no content for Venezuela on the site, we used the page with references of the UN Universal Periodic Review (2016).²⁸ It is important to reiterate that, after this initial research, the team interviewed local experts, which made it possible to confirm the relevance of some normative artifacts, but also brought new findings.

From this first trail, and with contributions from semi-structured interviews, we followed a second path of **specific searches on the Google search engine**. Through searching in Portuguese and Spanish and based on the number of each standard (or name, in the case of Venezuela), associated with the name of the country, we sought to verify the status of each of the artifacts found, whether current, updated, regulated, replaced or revoked. We prioritize results in the official language of the respective country: Portuguese for Brazil and Spanish for the others.

So, in the third way, we seek to define one **database as the default source** of normative artifacts from each country, which would guarantee uniformity in citations and the current validity of the norms. Thus, for Argentina, the *Sistema Argentino de Información Jurídica* (SAIJ),²⁹ maintained by *Ministerio de Justicia de la Nación*; for Brazil, the *Portal da Legislação*,³⁰ of the *Presidência da República*; for Paraguay, the *Biblioteca Y Archivo del Congreso Nacional*,³¹ for Uruguay, the *Electronic Banco Electrónico de Datos Jurídicos Normativos*³² of the *Dirección Nacional de Impresiones y*

24 CRIN – Child Rights International Network. **Argentina: National Laws**. 7 Jul. 2011. Available at <https://archive.crin.org/en/library/publications/argentina-national-laws.html>. Accessed on 25 Mar. 2024.

25 CRIN – Child Rights International Network. **Brazil: National Laws**. 6 Jun. 2012. Available at <https://archive.crin.org/en/library/publications/brazil-national-laws.html>. Accessed on 25 Mar. 2024.

26 CRIN – Child Rights International Network. **Paraguay: National Laws**. 8 Dec. 2011. Available at <https://archive.crin.org/en/library/publications/paraguay-national-laws.html>. Accessed on 25 Mar. 2024.

27 CRIN – Child Rights International Network. **Uruguay: National Laws**. 26 Jul. 2013. Available at <https://archive.crin.org/en/library/publications/uruguay-national-laws.html>. Accessed on 25 Mar. 2024.

28 CRIN – Child Rights International Network. **Venezuela: Children’s Rights References In The Universal Periodic Review**. 25 May. 2017. Available at <https://archive.crin.org/en/library/publications/venezuela-childrens-rights-references-universal-periodic-review.html>. Accessed on 25 Mar. 2024.

29 ARGENTINA. Ministerio de Justicia de La Nación. **Sistema Argentino de Información Jurídica**. Available at <http://www.saij.gob.ar/>. Accessed on 25 Mar. 2024.

30 BRAZIL. Presidência da República. **Portal da Legislação**. Available at <https://www4.planalto.gov.br/legislacao>. Accessed on 25 Mar. 2024.

31 PARAGUAY. **Biblioteca y Archivo Central del Congreso de La Nación**. Available at <https://www.bacn.gov.py/>. Accessed on 25 Mar. 2024.

32 URUGUAY. IMPO – Dirección Nacional de Impresiones y Publicaciones Oficiales. **Normativa y Avisos Legales del Uruguay**. Available at <https://www.impo.com.uy/cgi-bin/bases/consultaBasesBS.cgi?tipoServicio=3>. Accessed on 25 Mar. 2024.

Publicaciones Oficiales (IMPO); and, for Venezuela, the *Leyes Vigentes*³³ of the *Asamblea Nacional*. As a backup resource, in case the content of a law is not available, or even if the repository is temporarily inaccessible, we count additionally with the *Sistema de Informações de Tendências Educacionais na América Latina* (SITEAL)³⁴ by UNESCO.

Among the normative artifacts found, we selected those that contained elements about children and adolescents; about encryption; or on both topics. In the tabulation, we observe: a) the name/number of the law; b) the country to which the law refers; c) summary of the document; and d) provisions on the protection of children and adolescents or on encryption, depending on which of the topics the law referred to.

Furthermore, it is worth noting that we chose to highlight the laws that are distinctive to each country. In this section, it was found that all five countries under analysis have both a constitutional provision on the rights of children and adolescents, and a national law that internalizes the UN Convention on the Rights of the Child. Therefore, these laws are not highlighted on the specific pages for each country, and are only listed at the end of this Guide, in the table of normative artifacts that summarizes the list of laws we found.

As for the **technological artifacts**, we consider as such the digital mechanisms in online environments, which affect encryption, aimed at combating digital sexual violence against children and adolescents. Even though we made an effort to search for its existence, including asking questions about the topic during interviews with experts, we did not obtain any results from a mechanism implemented in accordance with our definition. We found only one legal provision relating to a possible artifact, but which has not yet been implemented in practice, which prevented our analysis of this point of view; and reporting measures that do not interfere with the functioning of encryption, which goes beyond our objective. This is not proof that such technological artifacts do not exist in MERCOSUR, but rather that our field of research and our methodology did not allow us to recognize them.

In terminology, we occasionally refer synthetically, just to encryption or digital security, on the one hand, and to the rights of children and adolescents or sexual violence, on the other. However, we emphasize that our research focus is at the intersection between the preservation of strong end-to-end encryption in harmony with the integral protection of children and adolescents against online sexual violence.

Conceptually, in relation to normative references to encryption, we do not only consider the legal norms that expressly deal with this technology, but also take into account mentions of the attributes of authenticity, integrity, confidentiality and non-repudiation. But we restricted ourselves to provisions that could directly affect the field of online sexual violence against children and adolescents, in hypothetical situations of criminal investigations, disregarding issues linked to the broader field of personal data protection.

33 VENEZUELA, Bolivarian Republic of. *Asamblea Nacional*. **Leyes Vigentes**. Available at <https://www.asambleanacional.gob.ve/leyes/vigentes>. Accessed on 25 Mar. 2024.

34 UNESCO – United Nations Educational, Scientific and Cultural Organization. Office for Latin America and the Caribbean. IIEP – Instituto Internacional de Planejamento Educacional. **Políticas e regulamentações**. SITEAL – Sistema de Informação de Tendências Educacionais na América Latina. Available at <https://siteal.iiep.unesco.org/pt/politicas>. Accessed on 09 Aug. 2024.

2.2. Theoretical framework

The theoretical framework of our project, as already mentioned, intertwines two macro-concepts: encryption, seen not only as a technique, but also in its principled proposal for digital security and privacy; and online sexual violence against children and adolescents. At this point, we will outline a brief synthesis, in order to present these works and correlate them with the object of the research. Throughout this report, they will be used as our analysis instruments.

The catalyzing spark of this project of ours, to intertwine **encryption and the rights of children and adolescents**, was a research developed by the Child's Rights International Network (CRIN) and by Defend Digital Me, entitled "Privacy and Protection: a children's rights approach to encryption". Released in 2023, the report addresses the interrelationship between encryption and human rights of children and adolescents in the digital sphere with the aim of overcoming a supposed polarization between the logic of privacy and the demand for child and youth protection.³⁵ It presents the results of an investigation with interviews with agents who work both in the technology scenario and in the rights of children and adolescents.³⁶ In the end, it points out a series of recommendations in terms of building a path to compatibility and recognition of privacy and digital security as a human right for children and adolescents. However, it is recognized the analytical perspectives are centered on the Anglo-Saxon and Eurocentric world.³⁷

In this sense, the report served us as an investigative starting point, a model of scientific analysis that we intend to expand by using similar methodological strategies. However, our proposal was to fill the gap in the lack of analyzes guided by and for the Global South, in particular, with a focus on countries in the MERCOSUR.

As a second reference, specifically focused on the context of **encryption**, the book "*Direito e Criptografia: direitos fundamentais, segurança da informação e os limites da regulação jurídica na tecnologia*",³⁸ of Carlos Liguori, served as a foundation for the historicity of the political-legal nature of the debate on encryption and privacy. The main aspect for our research object is the systematization of the contemporary global context of debates surrounding the limits of legality of the free use of encryption.

As the author explains, although cryptographic techniques have existed for thousands of years, the recent popularization of the civilian use of digital information and communication technologies, especially the Internet, has boosted the development of sophisticated cryptographic algorithms. Within what the law can contribute to the issue, Liguori identifies strong encryption as a technical

35 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.

36 CRIN; Defend Digital Me. *Op. cit.* P. 8.

37 CRIN; Defend Digital Me. *Op. cit.* p. 13

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

solution for a multifactorial demand from the information society – which seeks authenticity, confidentiality, availability and non-repudiation of the myriad of data that travel online – but which encounters political resistance expressed in legal terms, demanding a legal solution.

And looking at what technology can contribute, our third theoretical basis was “*Políticas De Encriptação: Entre a Codificação de Direitos, Regulação Pública e o Cipher-Ativismo*”,³⁹ by André Barbosa Ramiro Costa. The technological limits to the realization of rights, given the expansion of government surveillance and the abusive trade in personal data, are seen as contours of the duality between information security systems – aimed at individual privacy and informational self-determination – and criminal investigations – capable of intercepting and accessing private devices and communications. As a contribution to our research, we align ourselves with Costa in the assessment that rights such as communications secrecy find in the technique of encryption technological shelter against state abuses inherent to the growing culture of society monitoring.

Furthermore, Costa analyzes the range of arguments in favor of weakening digital security techniques, and even a complete ban on the use of strong encryption. At the point of “child exploitation networks”, core to our analysis, he points out how the narrative of confronting sexual violence against children and adolescents is used to defend the creation or maintenance of weaknesses in technological security. And precisely with the support of a UNICEF study, in a reflection aligned with our research, Costa points out that technological and organizational security measures prevent leaks and fraud, to the benefit of the entire community, including the most vulnerable people. Therefore, where children and adolescents’ data travel, the most modern and current technological protection should always be installed.

In addition to the basic theoretical conceptual overview of modern encryption (ciphers and keys; symmetry and asymmetry; data in transit and stored; end to end; homomorphic encryption, etc.) and its everyday applications, this trio of works reveals regulatory conflicts, from the 1970s to the present day, and explains their formation and how civil society mobilized in favor of the use of strong encryption. Especially for our research, they share the perception that there must be caution in criminal investigations that seek to defend human rights, as the information society is closer to a “golden age of surveillance” – never before has so much data been produced – than from the supposed erasure of data by technological security techniques – as suggested by the term “going dark”.

To these analysis instruments, we add four other key points from these works. First, the joint expansion of public state surveillance programs and the private market for personal data. Second, the criminal and rights-restrictive nature of arguments in favor of weakening strong encryption. Third, the diffuse social interest in technological security, including in particular the integral protection of children and adolescents; and, finally, the urgent need for legal harmonization between technological security and human rights protection in the legal regulation of digital environments.

39 COSTA, André Barbosa Ramiro. **Políticas de encriptação: entre a codificação de direitos, regulação pública e o cipher-ativismo**. 2021. Dissertation (Master’s in Computer Science) - FUniversidade Federal de Pernambuco, Recife, 2021. Available at <https://repositorio.ufpe.br/handle/123456789/42872>. Accessed on 25 Mar. 2024.

At the other central theme of our theoretical framework, namely, the **human rights of children and adolescents**, especially in the face of confronting online sexual violence and the new frontiers of digital rights, we chose two more works as references, in addition to the contributions on the topic in the aforementioned CRIN and Defend Digital Me report.

The research “*ONDE ESTAVAM VOCÊS QUANDO EU PRECISEI? Percepções de vítimas de violência sexual infantojuvenil LGBTQIA+ sobre o Sistema de Garantia de Direitos de Porto Velho – RO*”, developed by Wilson Guilherme Dias Pereira,⁴⁰ supports the reflections built in this investigation by offering a consolidation of the different concepts involved in the theme of sexual violence against children and adolescents. This analysis is especially conceptual, aiming to overcome existing obstacles to importing terms without due problematization in accordance with local public policies.

For example, the research developed by CRIN makes strong use of the term “sexual abuse” as a category that, at times, is even presented as a synonym for “sexual exploitation”. However, according to Pereira, in the logic of the Convention on the Rights of the Child, and consequently Latin America, especially Brazil, the terms have different loads of sensitivity, responsibility and action. While “sexual abuse” refers to acts of violation of the sexual intimacy of children and adolescents, which can be carried out without the intention of economic or financial gain, “sexual exploitation” has as its main purpose a certain compensation, whether for the victim or for her “aggressor-groomer”.⁴¹

Furthermore, as a recent work, the dissertation allows us to invoke reflections on children and youth groups that are even more vulnerable, such as LGBTQIA+, black people, indigenous people, among others, apoint also highlighted by CRIN report. But it must be recognized that its interrelationship with digital rights issues is scarce, especially with regard to the issue of online sexual violence against children and adolescents.

For this reason, the doctoral thesis “*Violência Sexual Contra Crianças e Adolescentes Mediada Pela Tecnologia da Informação e Comunicação: elementos para a prevenção vitimal*”, by Maria Emilia Accioli Nobre Bretan, is also used as a theoretical framework for this investigation.⁴² The research is one of the few developed in Brazil that focuses on sexual violence against children and adolescents mediated by ICTs and builds an analysis from the point of view of victims’ safety, recognizing the need to strengthen children’s digital literacy in the country, back in 2012. As a limitation to your contribution to our work, we highlight the temporal context, as other risks and opportunities are observed in the expansion of communication channels, the changing of usage habits and of access to certain platforms, and the development of new emerging technologies.

40 PEREIRA, Wilson Guilherme Dias. **ONDE ESTAVAM VOCÊS QUANDO EU PRECISEI? Percepções de vítimas de violência sexual infantojuvenil LGBTQIA+ sobre o Sistema de Garantia de Direitos de Porto Velho – RO**. Porto Velho, 2023. Dissertation (Master’s). Interdisciplinary Professional Master’s Postgraduate Program in Human Rights and Justice Development. Universidade Federal de Rondônia. Available at <https://dhjus.unir.br/pagina/exibir/22968>. Accessed on June 17th. 2024.

41 PEREIRA, Wilson Guilherme Dias. *Op cit.*

42 BRETAN, Maria Emilia Accioli Nobre. **VIOLÊNCIA SEXUAL CONTRA CRIANÇAS E ADOLESCENTES MEDIADA PELA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO: elementos para a prevenção vitimal**. 2012. 326 p. Thesis (PhD) - Faculdade de Direito da Universidade de São Paulo, [S. l.], 2012. Available at <https://doi.org/10.11606/T.2.2012.tde-22042013-111456>. Accessed on 4 Mar. 2024.

Thus, to understand the concept of sexual violence, we approach the reflections constituted by Pereira⁴³ and Bretan,⁴⁴ and we take online sexual violence against children and adolescents as a macro concept that encompasses all types of offenses against the sexual rights of a population under priority legal protection due to their peculiar development condition, including abuse and exploitation.

2.3. Research limitations

The methodological choice for interviews provides important inputs for we think about the context and create hypotheses about the scenario studied, including encouraging new future research, but it does not allow us to make generalizations based on the perceptions of experts in the field, considering our search for scientific rigor.

Geographically, we chose to limit our focus to MERCOSUR, which reduces the representativeness of the research in relation to Latin America and the Global South, but makes a first research effort viable. Future studies that address other regions or specific contexts within the theme can serve as a comparison for a broader and more complete understanding. Still in this aspect, we admit the limitations of our own nationality. All the people on the team are from Brazil. Despite our mastery of other languages and our efforts to contact institutions from other countries, the fact that we are not in continuous incidence in Argentina, Paraguay, Uruguay and Venezuela impacts our range of experts, as well as our knowledge of the nuances in the local normative and technological contexts.

3. Results

The results of our investigation, carried out through bibliographical research, interviews, and review of normative artifacts, allow us to visualize the specific situation of each country, which will be presented below in alphabetical order.

Before specific national portraits, we begin by analyzing the Convention on the Rights of the Child, as it is a normative artifact common to the entire MERCOSUR.

Then, for each nation, we systematized the findings in the narratives of experts we interviewed around seven themes (see item 2.1, in the methodology): 1) existence of debate in the country; 2) notorious cases mentioned in the interviews; 3) existence of normative artifacts in the country; 4) existence of documents from different institutions in the country; 5) existence of technological artifacts in the countries; 6) positioning of the institution of which the person interviewed is a member; and 7) risks mentioned in the interviews in relation to disputes between encryption and the protection of children and adolescents and the paths taken by the national government. Then, considering our perceptions about each social context, we will describe and analyze the normative artifacts of each country.

43 PEREIRA, Wilson Guilherme Dias. *Op cit.* Pp. 49-60. And for a reading with simpler language, in the nature of scientific dissemination, see: PEREIRA, Wilson Guilherme Dias Pereira; VIEIRA, Victor. **Violência sexual online e criptografia: o papel das tecnologias na proteção das vítimas.** IRIS, 05 Mar. 2024. Available at <https://irisbh.com.br/violencia-sexual-online-e-criptografia/>. Accessed on 07 Aug. 2024.

44 BRETAN, Maria Emilia Accioli Nobre. *Op cit.*

In the end, we consolidated the contributions and addressed the central problem of our research in the regional context of MERCOSUR. We analyze possible convergences and divergences between discourses, as well as viable approaches for joint reflection on encryption and the rights of children and adolescents.

3.1. Common Normative Artifact: Convention on the Rights of the Child

The **Convention on the Rights of the Child**, with the exclusive exception of the United States of America, is ratified by all countries of the world. It was approved by the UN General Assembly Resolution of November 20, 1989, and entered into force on September 2 of the following year. In Argentina, it was internalized by **Act nº 23,849/1990**;⁴⁵ in Brazil, by **Decree nº 99.710/1990**;⁴⁶ in Paraguay, by **Act nº 57/1990**;⁴⁷ in Uruguay, by **Act nº 16.137/1990**;⁴⁸ and in Venezuela, by **Act nº 1/1990**.⁴⁹

In line with the doctrine of integral protection, the Convention imposes on States the commitment to meet, with absolute priority, the best interests of “every human being under 18 years of age”, recognized as subjects with full rights. Among its 54 articles, we highlight articles 3, 4, 13, 19, 34, 35 and 36, that touch or explicitly oblige signatory countries to prevent exploitation, in particular sexual, of people between 0 and 18 years of age.

When preconizing consideration of the “best interests of the child”,⁵⁰ Article 3 demands that the State adopts all appropriate legislative and administrative measures to ensure the protection and care necessary for their well-being. In the same direction, article 4 imposes the obligation to adopt all necessary measures to guarantee the implementation of children’s rights, using the maximum available resources and collaborating internationally. Regarding online communication, Article 13 deals with children’s right to freedom of expression, including access to information and ideas without

45 ARGENTINA. **Ley nº 23.849. Apruébase la Convención sobre los Derechos del Niño.** Boletín Oficial, 22 Oct. 1990. Available at <https://www.argentina.gob.ar/normativa/nacional/ley-23849-249/texto>. Accessed on 20 Jun. 2024.

46 BRAZIL. **Decreto nº 99.710, de 21 de novembro de 1990. Promulga a Convenção sobre os Direitos da Criança.** Presidência da República. Available at https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm. Accessed on 20 Jun. 2024.

47 PARAGUAY. **Ley nº 57/1990. Que aprueba y ratifica la Convención de Las Naciones Unidas sobre los derechos del Niño.** Corte Suprema de Justicia. Available at <http://www.csj.gov.py/cache/lederes/P-0-20121990-L-57-1.pdf>. Accessed on 20 Jun. 2024.

48 URUGUAY. **Ley nº 16.137/1990. Aprobación de la Convención sobre los derechos del niño.** IMPO. Available at <https://www.impo.com.uy/bases/leyes/16137-1990>. Accessed on 20 Jun. 2024.

49 VENEZUELA, Bolivarian Republic of. **Ley nº 1/1990. Ley aprobatoria de la Convención Sobre los Derechos del Niño. 23 Ago. 1990.** 23 Aug. 1990. SITEAL – Educational Trends Information System in Latin America. Available at <https://siteal.iiep.unesco.org/bdnp/873/ley-11990-ley-aprobatoria-convencion-derechos-nino>. Accessed on 20 June 2024.

50 In MERCOSUR countries, legislation distinguishes between children (between 0 and 12 years of age) and adolescents (between 12 and 18 years of age). However, the Convention refers to children without distinction. In this section, we respect the nomenclature of the legislation under analysis.

borders, by various means, which can also be understood as a guarantee of Internet access.

In the field of sexual violence, article 19 requires States to take all protective measures against all forms of violence, offenses and physical or mental abuse, neglect, carelessness, ill-treatment and exploitation, even in the custody of those responsible for the child. More specifically, the Article 34 provides a commitment to protecting children against all forms of sexual exploitation and abuse, including the duty to prevent encouragement or coercion of any sexual practices of economic exploitation⁵¹ or illegal practices, and also shows or materials that sexualize them. Finally, articles 35 and 36 require protection against kidnapping, sale or any type of exploitation harmful to their well-being.

3.2. Argentina

Interviews

We interviewed four experts from different institutions in Argentina. Adrielle Keys⁵² and Amanda Soledad are dedicated to the rights of children and adolescents; Adrian Tavaréz, to early childhood education; and Ana Ivanz, to technology topics.

A consensus was identified about the absence and need for a **specific debate on the intersection of themes** – protection of children and adolescents and digital security, with a focus on encryption. For Ana Ivanz and Adrian Tavaréz this intersection does not seem to be prominent in the country, where debates are more focused on the protection of children youth or in the sphere of personal data protection, with the work of various civil society organizations, such as *Chicos.net*, *Digital Strike* and *The Other Voices Foundation*.

Adrielle Chaves also highlighted that, regarding children and adolescents, themes orbit the limitation of the use of technologies, sexting, cyberbullying and online betting. For her, there is special emphasis in the country on the issue of online gaming and betting, and how to protect this group in these environments.

None of the people interviewed, however, deepened the debate on encryption.

The **notorious cases** presented by the interviewees elucidate the important points highlighted

51 The Convention, as well as other MERCOSUR legislation, uses the term “child prostitution” to describe commercial sexual exploitation practices. However, we chose to avoid using the term, based on the First World Congress to Combat the Sexual Exploitation of Children and Adolescents, in 1996, in Stockholm, Sweden, where the participating countries decided to no longer use the term, as it refers to violence in which a child or adolescent is used as a “marketable good” for the profit and pleasure of those involved. For more information see: CHILDHOOD BRASIL. **Exploração sexual de crianças e adolescentes não é prostituição**. Childhood Brazil. Available at <https://www.childhood.org.br/exploracao-sexual-de-criancas-e-adolescentes-nao-e-prostituicao/#:~:text=Desde%20o%20Primeiro%20Congresso%20Mundial,em%20que%20um%20ou%20mais>. Accessed on 07 Aug. 2024.

52 The names here mentioned are pseudonyms, as an effort of the research team to protect the identity of the people interviewed, in order to prevent any attribution of responsibility or even their personal or institutional connection to any positions.

previously, such as the need for a specific debate on the topics in question, as well as discussions on grooming and on the cases that led to the creation of laws, such as the case of Mica Ortega.

In Argentina we had the case of a person well known for having participated in these reality shows, who ended up getting involved in adult situations with minors, through a pedophile network, which used a digital platform to exchange images of minors. (Adrian Tavarez)⁵³

The case of Mica Ortega, which was what generated the Mica Ortega law, was a very resonant case because she was a girl who first came into contact with a case of grooming and then ended up murdered, she had coexistence with other crimes, a very resonant case, which led to the creation of the Mica Ortega law. (Amanda Soledad)

About **normative artifacts**, according to the people interviewed, there would be no legal provision regarding encryption, only protocols for decrypting devices, conversations and accessing information, in the context of legal proceedings.

I think there is a lot missing, there is a very strong communication gap with children to try to protect them. That's where the biggest problem is and to reinforce that. Security policies, encryption policies, encryption, or whatever strategy that ends up being most effective in protecting children. (Ana Ivanz)

Between the identified **documents**, were presented the *Elige Tu Forma*, a campaign with videos and an educational guide to point out ways to establish dialogues with children and adolescents on various topics such as: screen time, grooming, hate speech, dangers in online games, sexting, among other topics.⁵⁴ The material is based on the preventive debate to raise awareness of children and adolescents to make better use of the networks. Another campaign we highlight is *My First Device*.⁵⁵

When asked about documents, Adrian Tavarez highlighted another civil society document.

[...] a publication called Sistema de Educação Digital published by Axel Rivas at CPEC with whom we worked together that I can research and share with you, where somehow his public policy proposal to create a digital educational system had incorporated the data protection recommendation as an important issue to be considered. (Adrian Tavarez)

As for the **technological artifacts**, no artifacts existing in Argentina were presented. In other words,

53 In this report, we present all the statements collected during the interviews – which were conducted in Spanish or Portuguese – translated by us into English.

54 CHICOS.NET. **#Elige Tu Forma**. Available at <https://www.eligetuforma.org/home>. Accessed on 03 Jul. 2024.

55 CHICOS.NET. **Mi primer dispositivo**. Available at <https://www.chicos.net/programa/mi-primer-dispositivo>. Accessed on 03 Jul 2024.

the people interviewed did not identify government or private sector actions by digital platforms that sought to analyze and manage the issue of protecting children and adolescents in encrypted environments.

As for the **positioning** of people interviewed about whether weakening or breaking encryption would be the way to protect children and adolescents in encrypted environments, only one person took an explicit stance in defense of encryption, despite also considering it urgent and important to create safe digital environments for them. In other words, it considered that ensuring encryption and privacy is central, but did not eliminate the relevance of the debate on children and adolescents. On the other hand, we assessed that two people interviewed presented positions more focused on the rights of children and adolescents, as their narratives exposed greater concern with the issue of their protection, and less attention or attachment to debates about encryption. Furthermore, one interviewee did not present any position on the matter.

About potential **risks and concerns** in the context of protecting children and adolescents in digital environments, with a focus on encrypted environments, according to the people interviewed, there are: a) the possibility of mistakes and inappropriate requests for information made by third parties, highlighting the difficulty of children and adolescents in discerning these situations and dealing with them appropriately; b) significant communication gap between adults and children/adolescents, making it difficult to protect these groups; c) excessive exposure from children and adolescents to inappropriate content, especially in online environments, without adequate security and regulation policies; d) early adolescence associated with excessive and problematic technology consumption, including online betting, which lack of regulation in the country and present serious risks of dependence and psychological harm; e) themes of intolerance, gender violence and access to inappropriate content are also highlighted concerns; and f) challenge in creating public security policies that protect children and adolescents through the establishment of open and emancipatory, who understand these individuals as subjects of the promotion of safe spaces.

Normative artifacts

To understand which rules of the Argentine legal system are related to our object of study, we found the following normative artifacts:

THEMATIC FOCUS	NORMATIVE ARTIFACT	SUMMARY
Children and Adolescents	Argentine Constitution of 1853	Legal norm that underpins the country's legal system.
Children and Adolescents	Act n° 23.849/1990	Ratifies the Convention on the Rights of the Child
Children and Adolescents	Act n° 26.061/2005	Law for the Comprehensive Protection of the Rights of Children and Adolescents

Children and Adolescents	Act n° 26.904/2013	Amends the Penal Code to include crimes against the sexual integrity of children and adolescents in online environments in the normative list.
Children and Adolescents	Act n° 27.436/2018	Amends the Penal Code to hold people accountable for acts of child pornography.
Children and Adolescents	Act n° 27.590/2020	Commonly titled Law Mica Ortega, the law establishes the National Program for Prevention and Awareness of online harassment against children and adolescents.

As observed, Argentina does not have legislation that jointly addresses the central themes of this research. Six pieces of legislation were identified and selected because they address the protection of children and adolescents, to some extent also in online media. Regarding encryption specifically, nothing was found, neither from prior research carried out by the research team, nor from the interviews.

The **Constitution of Argentina** of 1853, in its current wording, establishes in article 75 the powers of the National Congress. Section 22 mentions the approval of human rights treaties and agreements on a suprallegal basis, highlighting the Convention on the Rights of the Child, which means that these rights are subordinate only to the Constitution, being superior to infra-constitutional legislation. Section 23 gives Congress the power to legislate on measures that promote equality and the full exercise of human rights, including children among vulnerable groups.

In turn, **Act n° 26.061 of 2005** adheres to the doctrine of integral protection of the rights of children and adolescents, in a set of provisions that safeguard their full development. We highlight that it provides for the right to life, personal integrity, private life, free association, discrimination, freedom, among other guarantees that may be threatened in online sexual violence against people under 18 years of age. Furthermore, we see art. 9, which guarantees personal integrity and dignity, prohibiting violent, discriminatory, humiliating, intimidating treatment, or any practice of sexual violence against this group, in addition to the duty to report any subject who has information about the practice of violence against children and adolescents; and the art. 22, which prohibits any humiliating exposure to your dignity, image or reputation, thus having a direct correlation with the production or circulation of online sexual violence content.

Act n° 27.436 of 2018 inserted into the Penal Code criminal punishment for the production and circulation of sexual content with children and adolescents, including the exposure of their genitals for sexual purposes. The art. 128 has come to criminalize producing, financing, offering, marketing, publishing, facilitating, disseminating or distributing this type of material, with more serious punishment if there is a violation of rights of people under the age of thirteen.

In the same sense, **Act n° 26.904 lei of 2013** also changed the Penal Code to punish online sexual harassment against children and adolescents. Art. 131 has made it a crime to use electronic media,

telecommunications or any other transmission technology to contact children and adolescents in order to commit an offense against their sexual integrity, which directly includes messaging applications that may contain encryption.

Finally, the **Mica Ortega Act (27.590/2020)** created the National Program for the Prevention and Awareness of Online Harassment against Children and Adolescents. We highlight its arts. 2nd, 3rd, 4th, 5th and 6th, which determine the purpose of the program to prevent and raise awareness about grooming and online harassment, with a conceptual definition of these two forms of violence: “*actions in which a person, through electronic communications, telecommunications or any other data transmission technology, contacts a minor with the purpose of committing any offense against their sexual integrity*”. Furthermore, the law provides guidance on the online exposure of children and adolescents, and ways to make the Internet safer, in a language that is educational and sensitizing. It is important to mention that such legislation has a particularly educational character, diverging to a certain extent from the punitive logic present in sexual violence regulations, and exploring a layer of social awareness and empowerment of children and adolescents to identify and reporting violence.

3.3. Brazil

Interviews

For Brazil, four experts from different institutions were interviewed; they all shared some specialized knowledge in digital law, but with different trajectories. Bernardo Ivans, coming from digital technology with deep experience in Internet governance; Barbara Lins, specialist in digital law; Bianca Diela, specialist in digital law with experience in children and adolescents’ law; and Bruna Amaral, specialist in children and adolescents’ law.

It was possible to identify among the people interviewed a reasonable consensus regarding the local absence of a **specific debate on the intersection of project themes**, although there is debate about the protection of children and adolescents in digital environments and a brief debate about encryption, with variation about the breadth, maturity and importance of these themes. The issues appear in different contexts, such as legislative, executive, judicial, technological and academic, but when they deepen and become more sophisticated, they are increasingly restricted to specialists, so the debate still needs to mature considerably and expand.

We still don’t have such a robust debate about commercial child exploitation. We talk more about whether or not to expose children on social media, but what about when that child is exposed on social media, is there a kind of child labor, in the logic of the child influencer? We don’t argue, we don’t have such a robust public debate. (Bianca Diela)

In relation to **notorious cases**, there were mentions of delicate situations involving children and adolescents and the use of technology, such as situations of sexual abuse, online revictimization and violence in schools, including fatal victims. The reports involved the use of social networks to

coordinate and disseminate worrying events, such as threats of attacks on schools,⁵⁶ with emphasis on the interviewees' perception that there was a closer collaboration between companies and authorities to facilitate the investigation of crimes and criminal prosecution.

On another note, regarding the use or plans to adopt investigative technology by security forces, the blocking of applications such as WhatsApp⁵⁷ and Telegram⁵⁸ was mentioned. In particular, Discord was mentioned as an example of a relevant platform that would fall outside the proposed regulation in the last text of the **Bill 2.630/2020**, a legislative proposal in Brazil with the purpose of regulating platforms, depending on the number of users, generating a failure in the online protection of children and adolescents.

Within these limits, a consensus was identified that the cases do not directly involve encryption in situations of online violence against children and adolescents, but rather challenges in the legal regulation of digital platforms, which can indirectly be related to technologies for protecting privacy and the secrecy of communications.

As for **normative artifacts**, the interviews showed that there was **current legal legislation** with some approach to the intersection between themes, but in an incipient way. Were cited art. 14 of the General Data Protection Law (LGPD),⁵⁹ with best interests as a legal parameter in the processing of personal data, in line with the UN Convention on the Rights of the Child,⁶⁰ General Comment N° 25 of the UN Committee on the Rights of the Child,⁶¹ which addresses encryption as a tool capable of

56 At the beginning of 2023, Brazil faced a wave of violent attacks on schools, marked by physical attacks and murders, often perpetrated by young people influenced by extremist ideologies and hate speech on social media. There were 36 attacks between 2002 and 2023, with 164 victims, 49 deaths and 115 injured people. See CARA, Daniel (rap.). **Ataque às escolas no Brasil: análise do fenômeno e recomendações para a ação governamental**. Relatório do Grupo de Trabalho Interministerial de Prevenção e Enfrentamento da Violência nas Escolas. Brasília: Ministério da Educação, 03 Nov. 2023. Available at <https://www.gov.br/mec/pt-br/aceso-a-informacao/participacao-social/grupos-de-trabalho/prevencao-e-enfrentamento-da-violencia-nas-escolas/resultados>. Accessed on Aug. 20, 2024.

57 CANTO, Mariana; RAMIRO, André; REAL, Paula C. **Criptografia no STF: O que dizem os votos de Rosa Weber e Edson Fachin e o que podemos aprender com eles**. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Available at <https://ip.rec.br/blog/criptografia-no-stf-o-que-dizem-os-votos-de-rosa-weber-e-edson-fachin-e-o-que-podemos-aprender-com-eles/>. Accessed on 20 June 2024.

58 In April 2022, Minister Alexandre de Moraes, of the Federal Supreme Court, ordered Internet connection providers to block Telegram in Brazil, due to the platform not having complied with court orders to remove illegal disinformation content, hate speech and incitement to violence. The company decided to comply with a series of demands and in less than two days the Minister revoked the blocking decision, which was never carried out. See SUPREMO TRIBUNAL FEDERAL. **Ministro Alexandre de Moraes revoga bloqueio após Telegram cumprir determinações do STF**. 20 Mar. 2022. Available at <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=483712&ori=1>. Accessed on Aug. 20, 2024; SUZUKI, Shin. **Telegram: as mudanças que levaram STF a liberar aplicativo no Brasil**. BBC Brasil, 22 Mar. 2022. Available at <https://www.bbc.com/portuguese/brasil-60841371>. Accessed on 20 Aug 2024.

59 BRAZIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Presidência da República. Available at https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Accessed on 26 Mar. 2024.

60 UN – United Nations Organization. General Assembly. **Convention on the Rights of the Child. [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.

61 UN – United Nations Organization. Committee on the Rights of the Child. **General Comment No. 25**

balancing children's privacy and security on the Internet;⁶² and the Child and Adolescent Statute⁶³ and the Constitution of the Republic,⁶⁴ both laws based on the doctrine of integral protection and with guidelines that can be applied to the digital environment.

As for normative debates on the online protection of children and adolescents in progress at the National Congress⁶⁵ and, in particular, in the Judiciary, it were cited the constitutionality of the Marco Civil da Internet and the blocking of Whatsapp in Brazil, objects of *Ação Direta de Inconstitucionalidade* 5.527⁶⁶ and the *Arguição de Descumprimento de Preceito Fundamental* 403.⁶⁷ However, none of these discussions are closed, in addition to preconize criminal approaches.

Also, for some voices, specific discussions about the protection of children and adolescents do not seem to impact the field of encryption, which would lack autonomous discussion. In this sense, it was mentioned that the defense of encryption appears, for example, around proposals as the last text of the **Bill 2.628/2022**, which deals with the protection of the rights of children and adolescents in online environments; and PL 2.630/2020, which more broadly addresses the regulation of digital platforms to combat disinformation, where, in previous versions of the text, instant message traceability was proposed. Afterwards, from the first version of the Working Group set up in the Chamber, presented at the end of 2021,⁶⁸ the proposal was withdrawn.

It was also pointed out that even bills regulating digital platforms with a focus on protecting the rights of children and adolescents lack depth on encryption. In this restricted dynamic, encryption is approached in binary logic, of antagonism between concerns about privacy and security of digital data *versus* protection against online child sexual abuse and other violations of rights.

(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://criancaeconsumo.org.br/wp-content/uploads/2022/01/comentario-geral-n-25-2021.pdf>. Accessed on 20 June 2024.

62 INSTITUTO ALANA; MINISTÉRIO PÚBLICO DE SÃO PAULO. **Comentário Geral N° 25 (2021) sobre os Direitos das Crianças em relação ao ambiente digital. Versão Comentada.** 16 Apr. 2022. Available at <https://criancaeconsumo.org.br/biblioteca/comentario-geral-n-25/>. Accessed on 20 Jun. 2024.

63 BRAZIL. **Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências.** Presidência da República. Available at https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Accessed on 16 May 2024.

64 BRAZIL. **Constituição da República Federativa do Brasil de 1988.** Presidência da República. Available at http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Accessed on 16 May 2024.

65 BRAZIL. **Projeto de Lei nº 2628, de 2022.** Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais. Senador Alessandro Vieira (PSDB/SE). Congresso Nacional. Available at <https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-2628-2022>. Accessed on 26 Mar. 2024.

66 BRAZIL. Federal Supreme Court. **ADI 5527.** Rapporteur: Rosa Weber. Brasília, DF. Available at <http://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282>. Accessed on 20 Jun 2024.

67 BRAZIL. Federal Supreme Court. **ADPF 403.** Rapporteur: Edson Fachin. Brasília, DF. Available at <http://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500>. Accessed on 20 Jun 2024.

68 BRAZIL. Chamber of Representatives. **REL 1/2021 GTNET – Relatório do Grupo de trabalho para aperfeiçoamento da legislação brasileira sobre Internet.** 28 Oct. 2021. Available at <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2305033>. Accessed on 16 Jul 2024.

The interviews also mentioned several **documents** of civil society organizations in the country with the intersection between encryption and the rights of children and adolescents online. A set of initiatives address everything from international regulations to specific challenges in Brazil, seeking to guarantee the doctrine of integral protection: IP.Rec translated the CRIN and Defend Digital Me report,⁶⁹ in addition to producing its own studies;⁷⁰ in the report “*Global Platform, Partial Protection*”, on the regulation of privacy and security for young people around the world, Data Privacy Brasil carried out a comparison of WhatsApp’s terms of use in Brazil, India and Europe;⁷¹ the Instituto Alana collaborated in the aforementioned CRIN research; the Brazil Chapter of the Internet Society is heavily dedicated to encryption,⁷² with debates on the impact of legislative proposals on the privacy of vulnerable groups⁷³ and the preparation of an open letter to the STF,⁷⁴ but also with the translation detailed analysis of legal norms in other countries⁷⁵ and the impacts on the LGBTQIA+ community;⁷⁶ relevant studies are produced by IRIS; and SaferNet⁷⁷ and Placa Mãe⁷⁸ work at the protection and digital education of young people. We reiterate that such works do not constitute the existence of a broad debate on the topic, since they are products of the efforts of specialists, without broad reach in normative debates. Along these lines, no specific production by public authorities on the intersection of themes was identified, having been pointed out the general immaturity regarding encryption, especially in comparison to the production on the rights of children and adolescents.

69 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.

70 RAMIRO, André; *et al.* **O Mosaico Legislativo da Criptografia no Brasil: uma análise de projetos de Lei.** Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), 2020. Available at <https://ip.rec.br/publicacoes/o-mosaico-legislativo-da-criptografia-no-brasil-uma-analise-de-projetos-de-lei/>. Accessed on 20 June 2024.

71 FAIRPLAY. **Global Platforms, Partial Protections.** 12 Jul 2022. Available at <https://fairplayforkids.org/design-discrimination-july2022/>. Accessed on 20 Jun. 2022. P. 3-4.

72 INTERNET SOCIETY - BRAZIL CHAPTER. **Conteúdos da Internet Society sobre criptografia.** 18 Aug. 2020. Available at <https://isoc.org.br/noticia/conteudos-da-Internet-society-sobre-criptografia>. Accessed on 20 Jun. 2024.

73 INTERNET SOCIETY - BRAZIL CHAPTER. **SBSeg | A Criptografia na Proteção a Grupos Vulneráveis.** 12 Sep. 2022. Available at <https://isoc.org.br/noticia/sbseg-a-criptografia-na-protecao-a-grupos-vulneraveis>. Accessed on 20 June 2024.

74 INTERNET SOCIETY - BRAZIL CHAPTER. **Manifestação ao STF para reconhecer a importância da criptografia na proteção a direitos fundamentais.** 08 Jun. 2023. Available at <https://isoc.org.br/noticia/manifestacao-ao-stf-para-reconhecer-a-importancia-da-criptografia-na-protecao-a-direitos-fundamentais>. Accessed on 20 Jun. 2024.

75 BARKER, George. LEHR, William. LONEY, Mark. SICKER, Douglas. **O impacto econômico das leis que enfraquecem a criptografia.** Law & Economics Consulting Associates (LECA). 05 Apr. 2021. Translation: Paulo Rená da Silva Santarém. Internet Society - Brazil Chapter, 08 Jul. 2021. Available at <https://isoc.org.br/noticia/o-impacto-economico-das-leis-que-enfraquecem-a-criptografia>. Accessed on 20 June 2024.

76 INTERNET SOCIETY - BRAZIL CHAPTER. **Factsheet: Criptografia essencial para a comunidade LGBTQIA+.** 16 Jun. 2021. Available at <https://isoc.org.br/noticia/factsheet-criptografia-essencial-para-a-comunidade-lgbtqia>. Accessed on 20 June 2024.

77 SAFERNET. **SaferNet recebe o prêmio Neide Castanha de Direitos Humanos de Crianças e Adolescentes.** 15 May 2024. Available at <https://new.safernet.org.br/content/safernet-recebe-o-premio-neide-castanha-de-direitos-humanos-de-criancas-e-adolescentes>. Accessed 20 June 2024.

78 PLACAMAE.ORG. **Cyberbullying: como se proteger?** 30 Jun. 2024. Available at <https://placamae.org/publicacao/cyberbullying-como-se-protoger/>. Accessed on 20 June 2024.

Two people interviewed identified **technological artifacts** proposals to protect children and adolescents in digital environments in general, such as help lines (*helplines*) and assistance systems, which guarantee privacy through encryption, allowing young people to express their difficulties and seek help safely. Also mentioned was the client-side scanning⁷⁹ as a proposal from Apple, which was criticized precisely for affecting encryption in the attempt to protect children's rights.

As for the **positioning** of the people interviewed about whether weakening or breaking encryption would be the way to protect children and adolescents in encrypted environments, the interviews expressed complex views. In general, they recognized the importance of encryption as a fundamental technique to guarantee the privacy and security of young people, and the need for a broader and more collaborative approach was highlighted. One of them emphasized the importance of not placing all the chips on a single solution, proposing a network construction that involves several tools to protect children's rights. Another highlighted that encryption should allow parents access to important information without compromising data security, pointing homomorphic encryption ("technology that allows operations on encrypted data without decrypting it")⁸⁰ as a search for this approach.

A third acknowledged the complexity of the issue, and reported that it has not yet published a specific position on the subject. The responses were cautious in assuming an uncompromising defense of one aspect or another, although it is possible to identify inclinations based on the analysis of the points raised and the suggestions for solutions mentioned. In any case, a balanced approach was valued, which considers information security and privacy equally in relation to guaranteeing the rights of children and adolescents.

In relation to potential **risks and concerns** associated with encryption in the protection of children and adolescents online, according to the people interviewed there are: a) a

79 The concept of "Client-Side Scanning", according to a report produced by IRIS, refers to "[...] scanning techniques carried out on users' devices ("clients") to identify instances of sharing materials considered illicit – especially involving sexual content of child and teenagers abuse or CSAM (child sexual abuse material) – in environments protected by secure encryption, instead of performing this scanning at the server level." The technique is harshly criticized by researchers and organizations in the field of digital rights, for weakening encryption, and having no guarantee against "false positives", technological errors, which in this case of Apple's proposal to combat CSAM, could attribute crimes to innocent people, due to technological error. In PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. **Varredura pelo lado do cliente: uma revisão sistemática**. Belo Horizonte: Instituto de Referência em Internet e Sociedade (IRIS), November 2022. Available at <https://irisbh.com.br/publicacoes/comunicacoes-privadas-investigacoes-e-direitos-varredura-pelo-lado-do-cliente/>. Accessed on: 30 Nov. 2022. p.5.

80 CRIN; Defend Digital Me (2023, p. 7). The conclusion is that (*on. cit*, p. 50) "*The technology is not completely developed, and developing such solutions is expensive. Furthermore, it presents security risks, raises jurisdictional questions, and breaches privacy*".

The theoretical purpose of homomorphic encryption, conceived as an idea in 1978, is to allow calculations with encrypted data, that is, without the need to decrypt it, generating an encrypted "in the same way" result, that is, identical to that obtained with unencrypted data. It would allow, among other implementations, to analyze data in the cloud without affecting the encryption attributes, searching, for example, for correspondence between the analyzed material and a bank of sexual abuse materials against children and adolescents. A Holy Grail in the field, its practical applications still bring some type of vulnerability. For a Brazilian perspective, see BUSATTO JÚNIOR, Narciso. **Criptografia homomórfica**. Monograph (Bachelor's Degree in Communication Network Engineering) – Department of Electrical Engineering, Universidade de Brasília, Brasília, 2013. Available at <https://bdm.unb.br/handle/10483/15372>. Accessed on 20 June 2024.

warning about the potential for absorption of the child protection agenda to instrumentalize discourses and implement overly reactive solutions to encryption; b) the trend towards techno-solutionism and criminalization is seen as a disproportionate response that could harm privacy and freedom of expression; c) encryption is perceived as a barrier to the detection of harmful content, making it difficult to combat online violence and compromising the control of harmful practices; d) concerns about the possibility of rights violations and the weakening of protection for vulnerable groups; e) the exploitation of deepfakes and the dissemination of doctored images are cited as examples of the growing dangers faced by children and adolescents. These reflections highlight the complexity of the debate and the need for balanced approaches that protect fundamental rights without compromising online security.

Normative artifacts

In search of understanding which legal rules in Brazil are related to our object of study,⁸¹ we considered the following normative artifacts.⁸²

THEMATIC FOCUS	NORMATIVE ARTIFACT	SUMMARY
Children and Adolescents	Constitution of the Federative Republic of Brazil, 1988	Legal norm that underpins the country's legal system.
Children and Adolescents	Decree nº 99.710/1990	Promulgates the Convention on the Rights of the Child
Children and Adolescents	Act nº 8.069/1990	Statute of Children and Adolescents

81 We chose to restrict this list to normative artifacts that are directly relevant to the research object, relating, to repeat, to the intersection between encryption and online protection of children and adolescents against sexual violence. To this extent, legal norms were left out whose subject matter, for example, is restricted to regulating the use of encryption in the field of personal data protection in general, such as Decree nº 8.771, of 2018, which regulates *Marco Civil da Internet* in relation to log collection; and as Decree nº 11.856, of 2023, which – while establishing the National Cybersecurity Policy and the National Cybersecurity Committee – lists as one of the objectives “to guarantee the confidentiality, integrity, authenticity and availability of the solutions and data used”. Likewise, we did not consider legislative debates on broader legal norms, such as the reform of the Code of Criminal Procedure and the creation of a Criminal LGPD, in addition to Brazil's recent accession to the Budapest Convention on Cybercrime. Our option is reinforced by the fact that such pieces of legislation were not mentioned during the interviews.

82 For timing reasons, we left out of our analysis Resolutions No. 245 and 246 of the National Council for the Rights of Children and Adolescents, dated April 5 and June 12, 2024, respectively, providing for the rights of children and adolescents in a digital environment, and establishing a Thematic Group to develop the corresponding National Policy. See BRAZIL. Presidência da República. 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.

Children and Adolescents	Act nº 11.829 of 2008	Includes predictions to combat child pornography in the ECA
Children and Adolescents	Decree-Law nº 2.848/1940	Penal Code
Children and Teens / Encryption	Act nº 12.965/2014	Civil Rights Framework (“Marco Civil”) for the Internet in Brazil
Children and Teens / Encryption	Act nº 13.709/2018	General Personal Data Protection Law
Children and Adolescents	Act nº 13.431/2017	Creates a system to guarantee the rights of children and adolescents who are victims or witnesses of violence
Children and Adolescents	Act nº 13.441/2017	Provides for the online infiltration of police officers to investigate crimes against the sexual dignity of children and adolescents
THEMATIC FOCUS	BILLS	SUMMARY
Encryption	Bill nº 9808/2018	Provides for access to communication data through Internet applications for criminal prosecution purposes
Encryption / Children and Adolescents	Bill nº 2630/2020	Establishes the Brazilian Law on Freedom, Responsibility and Transparency on the Internet.
Children and Adolescents	Bill nº 2628/2022	Provides for the protection of children and adolescents in digital environments

The table shows us that, both through preliminary searches and from the “snowball” carried out in the interviews, no legal norms were identified – current or under debate – specific to the intersection that is the subject of this research. Bills that focus on the protection of children and adolescents in encrypted environments are debated. However, in addition to the Federal Constitution, we selected eight ordinary laws and three bills as relevant, as they address some point about the protection of children and adolescents in private online conversations, or about information security and/or access to data in digital environments, with predictions related to encryption.

The **Constitution of the Federative Republic of Brazil**, from 1988, is pioneer in joining the doctrine

of integral protection of the rights of children and adolescents, and in Brazil it is the basis of the alignment of legal norms to this new paradigm. The art. 227 ensures absolute priority, attributes shared duties to the State, family and society, asserts guarantees and prohibits violations, allowing us to infer the need for effective digital security measures for children and adolescents under age 18 in online environments.

Then the **Child and Adolescent Statute – ECA (Act nº 8.069/1990)** can be seen as the country's central norm on the subject. Its general part contains basic definitions and fundamental rights, and regulates prevention against rights violations; the special part provides the service policy, protection measures, defines an infraction, imposes sanctions for parents and guardians, creates guardianship councils, deals with access to justice, and typifies crimes and administrative infractions.

Of its total of 311 articles (including main and supplementary articles), at least 26 are directly or indirectly related to a possible investigation into sexual violence against children and adolescents in digital environments with encryption: 3rd, 4th, 5th, 6th, 15, 16, II, IV, V, VII, 17, 18, 70, 71, 86, 87, 98, 100, 190-A, 190-B, 190-C, 190-E, 240, 241-A, 241-B, 241-C, 241-D, 241-E, 244-A, and 244-B.

We highlight two more specific groups of provisions. The arts. 190-A, 190-B, 190-C and 190-E, included by **Act nº 13.441/2017**, regulate the infiltration of police officers on the Internet to investigate crimes against the sexual dignity of children and adolescents;⁸³ and the arts. 240, 241-A, 241-B, 241-C, 241-D, 241-E, 244-A and 244-B, inserted by **Act nº 11.829/2008**, typify various conducts as a crime of sexual violence against children and adolescents: from the production of records of explicit or pornographic sex scenes with children or adolescents, to corruption for the commission of a criminal offense, by any electronic means, including online chat rooms. The investigation of these sexual violence must have these provisions as the main axis.

Another norm regarding childhood, **Act nº 13.431/2017** structures the system for guaranteeing the rights of children and adolescents who are victims or witnesses of violence. We highlight art. 4, which defines the legal concept of sexual violence, and art. 13, which imposes on anyone the duty to report all violence against children and adolescents of which they are aware.

In criminal law, we count on **Penal Code (Decree-Law nº 2.848/1940)** eight criminal types relevant to combating sexual violence against children and adolescents that could involve online environments: arts. 213 (rape), 217-A (rape of a vulnerable person), 218 (corruption of minors), 218-A (gratification of lasciviousness through the presence of a child or adolescent), 218-B (encouragement of prostitution or other forms of sexual exploitation of a child or adolescent or of a vulnerable person), 218-C (disclosure of a rape scene or rape scene of a vulnerable person, of a sex scene or of pornography), 227 (mediation to serve the lust of others) and 230 (ruffianism) .

83 The infiltration provided for in ECA refers to the concealment of the police officer's identity to collect evidence of the authorship and materiality of crimes via the internet, and should not be confused with the practice of government hacking, in which technological vulnerabilities are exploited through the use of spy programs on digital devices. In that restricted sense, the undercover agent enters communities where illegal content is shared and participates in online communication in order to obtain evidence. This is a concealment technique, without any breach of encryption or its attributes of authenticity, integrity, confidentiality and non-repudiation, as the investigation procedure does not interfere in any way with digital technology.

In particular about online environments, in **Civil Rights Framework (“Marco Civil”) for the Internet in Brazil (Lei nº 12,965/2014)**, the art. 2nd reinforces the importance of human rights, the development of personality and the exercise of citizenship in digital media; the art. 7th ensures the right to inviolability and confidentiality of communications in flow and stored; the art. 10 deals with the preservation of intimacy and private life in the custody and availability of personal data and the content of private communications; and art. 29 provides for the right to parental control in the protection of children and adolescents, as well as the duty of education for the digital inclusion of children and adolescents. These are not articles inherent to our research topic, but we see an indirect relationship, which can serve as a parameter to recognize both the rights of children and adolescents online and abuses in criminal investigations. Furthermore, Marco Civil has been the subject of specific normative proposals, and its constitutionality is in question in the cases of blocking WhatsApp in Brazil, which involve the limits of legality of the use and offer of encryption.

The **General Personal Data Protection Law – LGPD (Act nº 13.709/2018)** connects to the object of this research in four provisions: art. 6th, item VII, takes security as one of the guiding principles of personal data processing activities, providing for responsibility and the need to employ technical and administrative measures to protect such data; the art. 14 regulates the processing of personal data of children and adolescents, promoting their best interests and requiring express and specific consent from a legal guardian; the art. 46 requires processing agents to adopt measures capable of protecting personal data against unauthorized access; and art. 48 cites the use of encryption (“*appropriate technical measures that render the affected personal data unintelligible*”) as a criterion for judging the severity of an incident.

Regarding the normative proposals under discussion in the federal legislature, three bills help us to understand the debates in the country on our research topic. Focusing on childhood, **Bill 2628/2022**, currently being processed in the Senate, seeks to regulate the protection of children and adolescents in digital environments.

Focusing on criminal prosecution, the **Bill 9808/2018** intends to regulate access to communication data through Internet applications. It seeks to allow police officers, when investigating flagrant crimes, to access, without judicial authorization, metadata and content of private communications on mobile devices, including requesting the cryptographic keys that allow access.

And **Bill 2630/2020**, or “*PL das Fake News*”, always mentioned in interviews, seeks to regulate the obligations of digital platforms to confront disinformation and hate speech, with rules of freedom, transparency and responsibility. The first point relevant to our research, there was debate about the provision of an instant messaging traceability system, which was expressed in the text approved in the Senate, but which appears to have been completely overcome during the turbulent proceedings in the Chamber of Representatives.⁸⁴ As already mentioned, this system would seriously affect the

84 At the end of the first half of 2024, the situation with PL 2630 is one of apparent complete inertia. A new working group was created by the Chamber of Representatives, in order to restart the debate on the project, supposedly free from the ideologies and disputes that led to the impasse over the vote. See XAVIER, Luiz Gustavo; SILVEIRA, Wilson. Lira cria grupo de trabalho para análise de projeto que trata das redes sociais. **Agência Câmara de Notícias**, 05 Jun. 2024. Available at <https://www.camara.leg.br/noticias/1069265-lira-cria-grupo-de-trabalho-para-analise-de-projeto-que-trata-das-redes-sociais/>. Accessed on: 16 Jul. 2024.

attributes of encryption.⁸⁵ On a second point, there was a more recent debate regarding the so-called “duty of care”,⁸⁶ which would create a general obligation for digital platforms to act comprehensively to prevent “systemic risks” and curb certain types of illicit conduct, including crimes against children and adolescents. This aspect was still undefined, although it was included in the text version of Bill 2630/2020 of May 2023.⁸⁷

3.4. Paraguay

Interviews

Four experts from different institutions were interviewed. Of these, Paulo Castros and Paloma Gomez, specialists involved with issues related to the rights of children and adolescents, and Pamela Ivenz and Pedro Taviniz who focus their work on communication, Internet and technology.

There was a consensus among the people interviewed on the pressing need to protect children and adolescents in the online environment. However, there was no consensus on the existence of a **specific debate on the intersection** of children’s rights and encryption.

To Paulo Castros, despite the numerous cases of online violence against children and adolescents, including sexual violence, the debate on the subject does not receive attention or seriousness on the public agenda and among sectors of society. In his opinion, however, discussions in the field of the rights of children and adolescents predominate.

You and we who work with childhood issues can identify what is a problem and what needs to be talked about. But we don’t talk, we don’t address. (Paulo Castros)

Despite this interviewee’s perception that the debate still focuses predominantly on agents who work specifically with the issue of children and adolescents’ rights, another interviewee highlighted a point that caught our attention. In Pedro Taviniz’s perception, the issue of sexual violence against children

85 See more on the topic in RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. **Comunicações privadas, investigações e direitos: rastreabilidade de mensagens instantâneas**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, May 2022. Available at <https://irisbh.com.br/publicacoes/comunicacoes-privadas-investigacoes-e-direitos-rastreabilidade-de-mensagens-instantaneas/>. Accessed on: 30 Nov. 2022.

86 In favor of the duty of care provision, see CAMPOS, Ricardo; OLIVEIRA, Samuel Rodrigues de. SANTOS, Carolina Xavier. **O conceito de dever de cuidado no âmbito das plataformas digitais**. Revista Consultor Jurídico, 21 Mar. 2023. Available at <https://www.conjur.com.br/2023-mar-21/direito-digital-conceito-dever-cuidado-ambito-plataformas-digitais/>. Accessed on 20 Aug. 2024; against the legislative adoption of this concept, see SANTARÉM, Paulo Rená da Silva. **O “dever de cuidado” seria um descuido indevido**. Desinformante, 8 May 2023. Available at <https://desinformante.com.br/dever-de-cuidado-riscos/>. Accessed on 20 Aug. 2024.

87 GALF, Renata; PINHO, Angela. **Entenda quais itens do PL das Fake News têm relação com moderação de conteúdo**. Folha de S.Paulo, 06 May 2023. Available at <https://www1.folha.uol.com.br/poder/2023/05/entenda-quais-itens-do-pl-das-fake-news-tem-relacao-com-moderacao-de-conteudo.shtml>. Accessed on Aug. 20, 2024.

and adolescents in digital environments is often associated with the discussion about the breaking or weakening of encryption, in the narratives of the Public Ministry of Paraguay, as the main strategy to confront and hold accountable such violence.

As for the **notorious cases**, all experts mentioned different examples involving violations of the human rights of children and adolescents through ICTs, which were used as the main channel for carrying out aggression or access to violence. A case presented by specialist Pamela Ivenz drew attention due to its correlation with the use of gamification⁸⁸ as a strategy to reduce victims' resistance and perceptions of violence.

Last year, we witnessed a high-profile case of child abuse and, with some investigations carried out, this abuse occurred within the framework of a game that had been proposed on the Internet, where there were certain instructions that the participants of that game had to follow, and among them there was this, the abuse of a child of around seven years old. (Pamela Ivenz)

Despite the numerous cases highlighted by the people interviewed, Paraguay is not a country with legislative omission on the topic. So, when asked about the **normative artifacts**, all participants mentioned the existence of **Act nº 5.653/2016**⁸⁹ as a legal framework on the subject, which aims to protect children and adolescents against harmful content on the Internet. However, unanimous recognition of the existence of the law in force does not imply recognition of its applicability. On the contrary, according to all the experts interviewed, social and political issues have prevented the adequate application of regulations.

By example, **Act nº 5.653/2016** determines that Internet service providers must find ways to filter content delivered to children and adolescents, in order to protect them from harmful content. This strategy includes obtaining and registering the telephone SIM card number on behalf of the child/adolescent, but this does not occur due to social issues, such as the lack of dissemination of regulations and/or the resistance/adaptation of Paraguayans responsible for children and adolescents. Furthermore, it is important to mention that all interviewees recognize opportunities in the legislation to defend the rights of children and adolescents online, but also identify risks, such as the weakening of encryption and the child's progressive autonomy.

88 The concept of gamification of violence or hate can be understood as “[...] the use of digital infrastructures capable of ‘making activities look like games’, intensifying a person’s efficiency, voluntariness and involvement in a given activity. This structure is very effective for various activities, including the promotion of hate speech. In this specific case, the use of gamified dynamics can intensify recruitment to hate groups on networks and adherence to online challenges that promote violence against certain groups.” (p. 234) in HALFELD, Emanuella; TEREZA, Julia; SANTOS, Pedro Henrique M. A gamificação do ódio no cenário brasileiro: um mapeamento das estratégias de enfrentamento do GT do Ministério dos Direitos Humanos e da Cidadania. In: SILVA, Fernanda dos Santos Rodrigues; VIEIRA, Victor Barbieri Rodrigues (orgs). **Anais do IV Seminário Governança das Redes**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024. Available at: <https://bit.ly/4dn76bB>. Accessed on: 02 Jul 2024.

89 PARAGUAY. **Ley nº 5.653 / Protección de Niños, niñas y Adolescentes contra Contenidos Nocivos de Internet**. 29 Sep. 2016. Biblioteca y Archivo Central del Congreso de La Nación. Available in <https://www.bacn.gov.py/leyes-paraguayas/5167/proteccion-de-ninos-ninas-y-adolescentes-contra-contenidos-nocivos-de-Internet>. Accessed on 20 June 2024.

As for the **documents**, specialist Paulo Castros mentioned the existence of the plan “*Tu escuela en casa*”,⁹⁰ a national education plan for the context of the pandemic. This document was highlighted for demonstrating a ministerial commitment, including in the students’ digital literacy process, aiming to use technology as a learning channel during the COVID-19 period.

Just one **technological artifact** was identified, but only under the condition of a legal provision. It is the requirement at **Act n° 5.653/2016**, that there must be a tool for parental monitoring of children and adolescents, as explained by Pamela Ivenz:

[...] service providers must make a free software tool available, with free licensing, to mobile phone operators or fixed Internet users, which allows them to control what information they are viewing. Based on the information they are producing (Pamela Ivenz).

However, as the same interviewee highlighted, despite the express determination in the law, the proposal has not yet been implemented in practice. And, both she and the other people interviewed mentioned the risk of surveillance when using a tool like this, due to the lack of specific safeguards for related rights.

Regarding the **positioning** of people interviewed about whether weakening or breaking encryption would be the way to protect children and adolescents in encrypted environments, none of them took a clear position in favor of weakening or breaking encryption as a crucial mechanism for combating online sexual violence. On the other hand, the analysis of presented discourses reveals a greater inclination towards the protection of strong encryption, in view of a required harmonization with the normative field of rights of children and adolescents. As pointed out by the following excerpt from interviewee Pedro Taviniz:

And without, obviously, failing to recognize that children and adolescents need all the protection in the digital environment, but if not, the way forward is not to necessarily abandon encryption, but in any case to strengthen precisely children, girls and teenagers in their capabilities to use this type of technology to their advantage (Pedro Taviniz).

Finally, the main potentials **risks and concerns** associated with encryption in protecting children and adolescents online according to the people interviewed are: a) extortion of data from children and adolescents for sexual purposes (*doxing*); b) weakening of encryption that can generate digital spaces with less security and discouraging advancement and investment in these tools; c) physical and psychological harm to children and adolescents; d) hyper-exposure of children and adolescents online by those responsible; e) risk of Latin American countries being used as channels for disseminating child and adolescent sexual violence content due to weakened regulations and/or supervision; f) absence of public policies on digital literacy for children and adolescents; and g) the digital divide as a challenge to be overcome in terms of access to technology.

90 PARAGUAY. **Education plan in times of pandemic “Your school at home” 2020**. SITEAL – Educational Trends Information System in Latin America. Available at <https://siteal.iiep.unesco.org/pt/node/2861>. Accessed on 03 Jul 2024.

Normative artifacts

In order to understand which legal rules in Paraguay are related to our object of study, we considered the following normative artifacts:

THEMATIC FOCUS	NORMATIVE ARTIFACT	SUMMARY
Children and Adolescents	National Constitution of the Republic of Paraguay, 1992	Legal norm that underpins the country's legal system.
Children and Adolescents	Act nº 57/1990	Approves and ratifies the United Nations Convention on the Rights of the Child
Children and Adolescents	Act nº 1.160/1997	Penal Code
Children and Adolescents	Act nº 1.680/2001	Childhood and Adolescence Code
Children and Adolescents	Act nº 2.861/2006	Represses the trade and commercial or non-commercial dissemination of pornographic material, using the image or other representation of minors or incapacitated people.
Children and Adolescents	Act nº 4.439/2011	Changed the art. 140 of the Penal Code to classify the crime of sexual exploitation of images of children and adolescents.
Children and Adolescents	Act nº 5.653/2016	Law for the Protection of Boys, Girls and Adolescents against Harmful Internet Content
Children and Adolescents	Act nº 6.002/2017	Inserted art into the Penal Code. 135b., which typifies the crime of Abuse by technological means.

Despite Paraguay not having specific legislation on the joint theme of this research, eight current regulations were selected, as they debate to some extent the online protection of children and adolescents. About encryption nothing specific was found, not even from the interviews.

The **National Constitution of Paraguay, 1992**, adopts integral protection and guarantees the rights of children and adolescents with priority, in the event of a conflict of norms, to their best interests. The art. 54 provides for the co-responsibility of family, society and the State for balanced and complete development, and for the full exercise of these rights, including protection from abandonment,

malnutrition, violence, abuse, trafficking, exploitation, etc. Anyone has the right to ask the competent authorities to guarantee these protections and punish those who violate them.

Along similar lines, the **Childhood and Adolescence Code (Act n° 1.680/2001)** defines and regulates the rights, protections and obligations of children and adolescents. It also typifies the crime of sex trade, in art. 31, with the prohibition of the use of children and adolescents in commercial sexual activities, as well as the prohibition of their participation in the production, distribution or elaboration of content of this nature.

In turn, the **Paraguay Penal Code (Act n° 1.160/1997)**, in the current wording, criminalizes the commercial exploitation of children and adolescents in several articles.

The art. 140 of the Penal Code, as amended by **Act n° 4.439/2011**, punishes anyone who produces publications that represent sexual acts or the display of genital parts of people under eighteen years of age; organize, finance or promote shows, public or private, with the participation of minors under 18 in sexual acts; distribute, import, export, offer, exchange, display, disseminate, promote, finance or carry out the production or reproduction of this type of publications, or have their possession. The penalties increase if children under 14 are involved; in the case of responsibility for custody, duty of care or guardianship, or collaboration of those responsible; chaos of violence, coercion, deception, reward, or repeated commercial performance.

The same law inserted two more articles on improper access and interception of data. The art. 146-B criminalizes breaching security systems and gaining access to data stored or transmitted electronically, magnetically or in a form not immediately visible. And the art. 146-C prohibits the interception of this data by technical means without authorization. In our reading, These provisions involve the protection of personal data, a central aspect in the various rights of children and adolescents in digital environments, in a way that contributes to thinking about encryption as a means of cyber protection against unauthorized processing.

Act n° 6.002/2017 changed art. 135, which deals with crimes against the sexual autonomy of children and adolescents, classifying abuses and exploitations that harm their physical and psychological integrity, including through technological means. Furthermore, art. 135-A, typifying the practice of sexual acts with a child, the induction to practice it in oneself or in third parties, and sexual acts that are manifestly relevant in the presence of a child, directed at them, or that induce them to practice them in the presence of themselves or in the presence of a child. third parties; and art. 135-B, defining the act of, through electronic communications, telecommunications or other data transmission technology, requesting or demanding in any way that a child send images of themselves of sexual content. So, even without talking about strong encryption, these articles encompass online conduct against children and adolescents.

Outside the Penal Code, **Act n° 2.861/2013** represses the trade and dissemination, commercial or otherwise, of erotic or sexual material with the image or other representation of minors or incapacitated people. The art. 1st makes it a crime to produce or reproduce this material in order to stimulate sexual appetite, or display genital parts for pornographic purposes. The art. 2nd punishes distributing,

importing, exporting, offering, exchanging, displaying, disseminating, promoting or financing the production or reproduction of this content. And the art. 3rd prohibits the participation of children and adolescents in public or private shows with “erotic actions of a sexual nature”, also punishing those who organize, finance or promote such events.

Finally, the **Act n° 5.653/2016**, in another tone, ensures the full protection of children and adolescents against potential harmful effects of content accessed online by children and adolescents. Art. 2nd establishes that the National Secretariat for Children and Adolescence is responsible for regulating which contents are considered harmful. Art. 3rd addresses active protection, requiring Internet service providers to provide their customers, upon registration, with free software with systems for detecting, filtering, classifying, removing and blocking harmful content. Thus, the legal norm highlights the responsibility of providers, but imposes monitoring technology that, in order to promote security, can introduce vulnerabilities.

3.5. Uruguay

Interviews

In Uruguay, two experts from different institutions were interviewed: Ubeatan Cristhin, who focuses on children’s and adolescents’ rights, and Ursula Iviz, who specializes in communication, internet, and technology.

During the discussion on the intersection of these themes, there was a strong consensus among participants regarding the need to establish minimum standards for the protection of children and adolescents in digital media. Additionally, they noted the lack of a regulatory framework that simultaneously addresses encryption and the rights of young people. While Uruguay has a well-established system for protecting children’s rights, discussions about encryption primarily stem from interpretations within the legal domains of privacy and data protection.

Inclusive, specialist Ursula Iviz highlighted how much of a gap there is between specialists in the two areas:

I don’t anticipate a scheduled discussion on this topic because the institutions that focus on various aspects of minors’ lives often lack a deep engagement with technological issues. Typically, they rely on recommendations from agencies like the Electronic Government Agency or the Computer Incident Center (C2I Uruguay) before adopting any measures. This reliance on external guidance contributes to the absence of a dedicated dialogue on the subject. (Ursula Iviz)

The experts were unable to mention any **notable cases** of violence against children and adolescents in the digital context that had a direct correlation with the issue of encryption.

Regarding the **existence of regulations**, expert Ubeatan Cristhin noted that there is little development

of regulations on encryption in Uruguay. This was reiterated in the interview with Ursula Iviz, who stated that significant progress is more focused on data protection, particularly with the Personal Data Protection Law, and on access to public information, through the Access to Information Law .

Ubeatan Crishin also highlighted the existence of a bill in progress, which aims to develop initiatives to raise awareness and training, as well as other educational policies to promote the responsible and safe use of digital technologies from childhood.⁹¹

Regarding documents from the government, civil society, and various institutions, expert Ubeatan Crishin mentioned the existence of the plan “*Pantallas en Casa*”,⁹² a guide developed in partnership with UNICEF with the aim of strengthening those responsible for supporting children and adolescents using digital technologies at home. Furthermore, the department “*Ciudadanía y Bienestar Digital*” was mentioned,⁹³ from CEIBAL,⁹⁴ focused on the development and dissemination of best practices for the responsible and safe use of the Internet. The interviewees were unable to respond regarding the existence of specific **technological artifacts**.

As for the interviewees’ **positions** on whether the path to protecting children and adolescents in encrypted environments would involve weakening or breaking encryption, it was not possible to identify a consensus or even a common trend. While one interviewee took a transparent stance aligned with encryption, even advocating for a perspective in which all internet traffic is encrypted, the other did not provide a clear direction. No suggestions or reflections were offered that considered the harmonization of both fields.

Finally, the main **risks and concerns** raised by experts regarding the investigated themes, according to the interviewees, are: a) the risk of phishing aimed at creating social engineering schemes to manipulate children and adolescents online; b) sexting as a means of manipulating the sexuality of children and adolescents for purposes of abuse or sexual exploitation; c) grooming, which refers to harassment targeting minors; d) cyberbullying; e) excessive screen time for children and adolescents, which can harm not only their mental health but also expose them to numerous other risks; and f) the development of a culture of hypervigilance towards children and adolescents driven by fear, meaning that parents and caregivers create such a strong culture of control that it undermines the freedom and development of these individuals.

91 We were unable to locate what this bill would be.

92 ESTEFANELLI, Lorena. **Screens at Home: Guidelines to accompany safe browsing on the Internet. Guide for families.** Plan Ceibal, ANEP, UNICEF, Nov. 2023. Available at <https://www.unicef.org/uruguay/informes/pantallas-en-casa>. Accessed on 27 June 2024.

93 CEIBAL. **Citizenship and Digital Wellbeing.** Available at <https://ceibal.edu.uy/institucional/ciudadania-digital/marco-institucional/>. Accessed on 03 Jul 2024.

94 O CEIBAL (“*Basic Computing Educational Connectivity for Online Learning*”) is a socio-educational innovation project with digital technologies in Uruguay, created in 2007 (See CEIBAL. **What is Ceibal?** Available at <https://ceibal.edu.uy/institucional/que-es-ceibal/>. Accessed on 03 Jul 2024).

Normative artifacts

To understand which bills of the Uruguay legal system are related to our object of study, we considered the following normative artifacts:

THEMATIC FOCUS	NORMATIVE ARTIFACT	SUMMARY
Children and Adolescents	Constitution of the Eastern Republic of Uruguay	Norm that underpins the country's legal system.
Children and Adolescents	Act nº 16.137/1990	Approval of the Convention on the Rights of the Child
Children and Adolescents	Act nº 9.155/1933	Penal Code
Children and Adolescents	Act nº 17.815/2004	Sexual violence against children, adolescents or those with disabilities
Encryption	Act nº 18.331/2008	Personal Data Protection Law and Habeas Data Action
Children and Adolescents	Act nº 19.580/2018	Increased penalty in art. 93, for victims under 18 years old

Uruguay also does not have any regulations on encryption, but we found some legislation regarding the protection of children and adolescents applicable to the online environment.

The **Constitution of Uruguay**, in Article 41, explicitly addresses the issue of children and adolescents by highlighting the duty and right of parents to care for and educate their children so they can achieve their full physical, intellectual, and social development. This demonstrates the country's commitment to protecting this social group and the responsibility of parents in their development.

In the **Personal Data Protection Law (Act nº 18.331/2008)**, Article 1 reinforces this guarantee among the human rights protected in Article 72 of the Constitution. Article 4 includes information about sexual life in the concept of sensitive data, which can be interpreted as a protection for everyone, including children and adolescents in specific contexts. Furthermore, Article 18, by deepening the protection of this data, delineates the guarantees for individuals under investigation, stipulating that personal data related to criminal offenses can only be processed by competent public authorities in accordance with laws and regulations. We can also expand this interpretation to encompass the data of children and adolescents as a vulnerable group, more susceptible to abuse, especially in procedures aimed at safeguarding their rights.

In the criminal field, we highlight the **Penal Code (Act nº 9.155/1933)**, whose Articles 274, 275, 277-BIS, and 278 classify as crimes, respectively, corruption for the commission of libidinous acts, rape, pornographic exhibition, and offenses against the sexual integrity of persons under 18 years through digital means—conducts that can occur online against children and adolescents. Additionally, **Act nº 19,580/2018** amended Article 92 to increase the penalties for the crime of distributing images and recordings of intimate content when involving minors under 18.

Moreover, **Act nº 17,815/2004** addresses sexual violence against children, adolescents, or vulnerable individuals through the use of their image or other representation: it criminalizes acts of producing, selling, disseminating, and facilitating the sale or dissemination of such material. These crimes can be directly or indirectly related to technological contexts, such as through encrypted communication apps, exemplified by the circulation or sale of content related to sexual violence against minors. Furthermore, these apps can both facilitate and hinder the perpetration of acts of violence, such as rape or grooming.

3.6. Venezuela

Interviews

From Venezuela, two specialists from different organizations were interviewed. Valeriano Ivon works in digital rights, while Venisha Carry focuses on the rights of children and adolescents.

Venezuela is the only suspended member of MERCOSUR, since 2017,⁹⁵ due to a series of internal and external political, legal, and economic conflicts, including international political sanctions. The interviews emphasized that this context affects the perception of the enforcement of existing human rights law.

In this sense, it was agreed that the **specific debate on the intersection of the themes** encryption and protection of children and adolescents does not find priority on the country's agenda. The severe economic crisis faced by the country has shifted attention to issues of work, food, and education, as mentioned by Venisha Carry:

Our agenda addresses complex issues of humanitarian emergencies, food issues, health issues, and education issues. We have public education, but many schools are operating only two mornings or two afternoons a week. Students attend because, during the rest of the time, teachers have to take on other jobs to make a living, as salaries are very low. (Venisha Carry)

Both interviewees also discussed the abusive processes of information control by state agents, which directly impacts the ability to propose regulations for the Internet, even if it is for the protection of human rights.

95 MERCOSUR. **Decisão sobre a suspensão da Venezuela no MERCOSUL**. São Paulo, 05 Aug. 2017. Available at <https://www.mercosur.int/pt-br/decisao-sobre-a-suspensao-da-republica-bolivariana-da-venezuela-no-mercosul/>. Accessed on June 17th. 2024.

Honestly, it is not a topic of debate in our country; we are not aware of any legislative initiatives, public policies, or government actions. In the country, unfortunately, due to the political situation, any initiative to control, protect, or impose limits in the online world is immediately perceived by society as part of what the government might use to control and restrict freedom of expression. (Venisha Carry)

Regarding **notable cases**, the experts highlighted reports of the use of physical violence as a way to bypass privacy, making the judicial breaking or weakening of encryption unnecessary, as abusive police conduct is sufficient.⁹⁶ In relation to cases involving children and adolescents, the specialist Valeriano Ivon mentioned gamification as a method for committing online violence. An example cited was the “Blue Whale Challenge”,⁹⁷ which has led to a debate about parents’ lack of knowledge about their children’s online activities.

There was a case that became very well-known a couple of years ago involving a challenge called the Blue Whale, something like that—I don’t remember the exact name—but it was a challenge where participants had to do increasingly risky tasks. There was a boy who committed suicide during these challenges, which sparked a major debate. These challenges were advertised on social media, and parents were often unaware that their child was participating; they didn’t have timely information and didn’t know about the profiles their child had, where they would post, ‘I’ve completed challenge 1,’ ‘I’ve completed challenge 2,’ and so on. He was the only one who dared to finish it. (Valeriano Ivon)

According to the experts, there are no **regulations** that directly link the fields of encryption and the rights of children and adolescents. Although there are specific laws for the protection of this group, such as the “*Ley Orgánica para la Protección del Niño, Niña y Adolescente*” and a regulation from 2006 aimed at protecting children and adolescents in digital environments, there are no specific provisions for online environments with encryption. Regarding encryption, the country has the Special Law against Cyber Crimes, but there is little public awareness of this regulation, neither among legal practitioners nor the general population.

96 The vulgar expression “rubber hose cryptanalysis” refers to this acute possibility that physical violence trivialized by the State will render any digital security resource useless. On the topic, see RODRIGUES, Gustavo Ramos. **Police access to cell phones in Brazil and the trivialization of “rubber hose cryptanalysis”**. IRIS - Internet and Society Reference Institute, 26 Oct. 2022. Available at <https://irisbh.com.br/aceso-policial-a-celulares-no-brasil-e-a-banalizacao-da-criptoanalise-de-mangureira-de-borracha/>. Accessed on 20 June 2024.

97 “The way the game reached Brazil and other Latin American countries, such as Mexico and Colombia, is as uncertain as its origin. The first signs of the challenge’s existence were identified in Russia, after the suicide of several young people who were said to be participating in virtual communities. The story, however, mixed with the legend and was surrounded by exaggerations, rumors and fake viral news, which raised the number of Russian teenagers killed because of the game to 130, between November 2015 and April 2016. The figure was never confirmed.

Nor is there an official explanation about the origin of the name, which could be associated with the whales’ habit of run aground on the beaches in a group”. BEDINELLI, Talita; MARTÍN, Maria. Blue Whale: the mysterious game that exposed the taboo of youth suicide. **The Country**, 02 May 2017. Available at https://brasil.elpais.com/brasil/2017/04/27/politica/1493305523_711865.html. Accessed on 03 Jul 2024.

The interviewees were unable to identify a **specific document** representing the position of the Internet governance sectors and the rights of children and adolescents on this issue in the country. Additionally, no **technological solutions** have been developed or are in development to address online crimes against children and adolescents in encrypted environments.

Regarding the **interviewees' stance** on whether weakening or breaking encryption would be a way to protect children and adolescents in encrypted environments, none of the specialists acknowledged this as an important means to combat online sexual violence. On the contrary, in light of the Venezuelan context of human rights violations, both emphasized the need to strengthen mechanisms for individuals' privacy and security. Within these limits, they also did not express specific concerns about the topic, nor could they offer any solutions on how to protect children and adolescents without compromising their safety.

Finally, the main **risks and concerns** presented by the experts regarding the topics investigated are: a) the low digital literacy of children and adolescents; b) online sexual violence practices, such as grooming, sexual exploitation, pedophilia; c) the digital divide, as a challenge to be overcome in terms of access to technology; d) gaps in the distribution of electrical energy in the country.

Normative artifacts

To understand which rules of the Venezuelan legal system are related to our object of study, we considered the following normative artifacts:

THEMATIC FOCUS	NORMATIVE ARTIFACT
Children and Adolescents	<u>Constitution of the Bolivarian Republic of Venezuela, 1999</u>
Children and Adolescents	<u>Law approving the Convention on the Rights of the Child, 1990</u>
Encryption / Children and Teens	<u>Special Law against Computer Crimes of 2001</u>
Children and Adolescents	<u>Law for the Protection of Boys, Girls and Adolescents in Rooms Using the Internet, Video Games and other Multimedia, of 2006</u>

99 *Venezuela's legal norms are not numbered, being referenced by their name in full, with edition and publication date of the Official Gazette.*

THEMATIC FOCUS	NORMATIVE ARTIFACT
Children and Adolescents	<u>Organic Law for the Protection of Boys, Girls and Adolescents (LOPNNA), 2007</u>
Encryption / Children and Teens	<u>Constitutional Law against hate, for Peaceful Coexistence and Tolerance, of 2017</u>
Children and Adolescents	<u>Law for the Prevention and Eradication of Sexual Abuse Against Girls, Boys and Adolescents, 2021</u>

Although Venezuela does not have specific legislation on the thematic intersection addressed in this research, we selected seven laws that are relevant to our analysis. They address the protection of children and adolescents and can be extrapolated to online environments. Specifically regarding encryption, two of them are relatively pertinent.

The Venezuelan **Constitution** of 1999 contains a commitment to the comprehensive protection of children and adolescents. Article 78 ensures the absolute priority and prevalence of their best interests, as well as the state’s duty to guarantee their progressive incorporation into active citizenship. It also assigns the state the role of forming public policies to safeguard their rights. We also highlight Article 58, which guarantees them the right to access appropriate information to ensure their comprehensive development.

The Special Law against Cyber Crimes of 2001, in addition to addressing children and adolescents, also discusses encryption by consolidating provisions on cybercrimes. Among its articles, we highlight four.

Article 2, in defining data messages, addresses the possibility of encryption in communications, implicitly recognizing it as a legally protected mechanism. Regarding the security of communications, Article 9 stipulates an increased penalty for unauthorized access or sabotage of systems protected by security measures, which includes the adoption of encryption. Articles 23 and 24 deal with combating the production and circulation of sexual content involving children and adolescents, as well as their exposure to sexual content without prior warning or measures that allow age restrictions.

The Law for the Protection of Children and Adolescents in Internet, Videogame, and Multimedia Use Areas was established in 2006 with the purpose of safeguarding the rights of children and adolescents in physical spaces designated for digital connection. Among the articles of the legislation, Articles 1, 2, 5, 8, 10, and 11 stand out.

Article 1 establishes the objectives of the law, which aim to ensure the promotion of appropriate use

98 *Venezuela’s legal norms are not numbered, being referenced by their name in full, with edition and publication date of the Official Gazette.*

of online educational and recreational services in Information and Communication Technologies (ICT) spaces. Article 2 stipulates the obligations of the state, companies, and establishments to adopt necessary and appropriate measures to guarantee the rights of children and adolescents. In line with this, Articles 5 and 11 mandate that online gaming companies establish minimum guidelines for the comprehensive protection of children and youth, with potential liability for non-compliance. Article 8 guarantees access to appropriate information, in accordance with the development of children and adolescents, prohibiting access to a list of harmful content, including sexual violence against children and adolescents. Finally, Article 10 requires online service providers to make available controls, mechanisms, and security programs for children and adolescents, in accordance with regulations from the National Telecommunications Commission.

The **Organic Law for the Protection of Boys, Girls and Adolescents (LOPNNA)**, established in 2007, aims to guarantee the full rights of children and adolescents in the country, with emphasis on articles 2, 4, 10, 13, 28, 32, 33, 50, 63, 65, 66, 67, 68, 88, 258, 259 and 260. Article 2 establishes the normative concepts of child (under 12 years old) and adolescent (from 12 to 18 years old). Additionally, it introduces an important innovation not found in other regulations from neighboring countries: the presumption of childhood and adolescence, which means that in cases of doubt about whether an individual is a child or adolescent, this status is presumed until proven otherwise.

Article 4 assigns an unyielding responsibility to the state to ensure the rights and guarantees of children and adolescents, as well as the shared responsibility of the family and society for their integral protection. It establishes the principles of the best interests of the child and absolute priority. Article 10 explicitly declares children and adolescents as subjects of rights, affirming that they enjoy the same rights guaranteed to any other individual. Additionally, Article 13 emphasizes the progressive nature of the personal exercise of their rights, guarantees, and duties, in line with the development of their personal capacities.

Following this progression, Article 28 guarantees the free development of personality, while Article 32 guarantees the right to physical, psychological, and moral integrity, holding the state, family, and society responsible for ensuring this protection against violence. In the same vein of combating violence, Article 33 ensures the right to protection against sexual violence, specifically abuse and exploitation, imposing a duty on the state to establish support programs for victims.

Article 50 guarantees the right to information about sexual and reproductive health for free and safe exercise, while Article 63 provides for the right to rest, recreation, leisure, sports, and play for the full, integral, and safe development of children and adolescents, highlighting the state's responsibility to develop ongoing campaign strategies to discourage the use of violent games. Article 65 guarantees the right to honor, reputation, self-image, private life, and family privacy, safeguarding these rights. Similarly, Article 66 ensures the inviolability of the home and correspondence for children and adolescents. In line with fundamental guarantees, Articles 67 and 68 provide for freedom of expression and the right to information. Furthermore, Article 88 guarantees the right to defense and due process.

Finally, in a more conceptual manner, Articles 258, 259, and 260 define the crimes of sexual exploitation, sexual abuse of children, and sexual abuse of adolescents. It is noteworthy that the legislation establishes different categories of abuse for children and adolescents, requiring the absence of consent to constitute abuse in the case of adolescents, while for children, the possibility of consent does not exist.

The **Constitutional Law Against Hate, for Peaceful Coexistence and Tolerance** of 2017 aims to establish minimum standards to prevent and eradicate violence.¹⁰⁰ This law was identified in the analysis as directly correlates to the topic of encryption and indirectly in the field of protecting children and adolescents, with emphasis on the 7th, 13, 14, 19 and 22.

Article 7 addresses public policy for peaceful coexistence and imposes on the state the duty to promote and guarantee peaceful coexistence in family, educational, and communicational processes, with an emphasis on children, adolescents, and youth, as well as on prevention and control processes, among others, regarding violence. Therefore, there is a legal mandate to confront sexual violence.

Articles 13 and 14 prohibit the promotion of war and messages of hate, including in electronic media, subjecting platforms to criminal and civil liability and requiring them to implement appropriate measures to prevent the dissemination of such content. Article 22 stipulates that if content is not removed within six hours of publication, a monetary fine and blocking of the portal will occur. These rules can be interpreted as a mandate to weaken encryption. Additionally, Article 19 establishes a shared duty among public authorities, the private sector, and society to fulfill the law's purpose by actively collaborating to eradicate all forms of violence.

Finally, the **Law for the Prevention and Eradication of Sexual Abuse Against Girls, Boys and Adolescents**, from 2021, establishes national parameters for a policy that aims to prevent and eradicate this type of violence. We highlight articles 1, 7 and 9.

Article 1 presents the objectives of the legislation, which consist of guaranteeing the safety of children and adolescents against any type of sexual abuse, invoking the principle of co-responsibility for this guarantee. Article 7 mentions the principle of absolute priority, aimed at ensuring the swift processing and decision-making of administrative and judicial procedures related to sexual abuse against children and adolescents. Finally, Article 9 establishes general obligations for the prevention and eradication of any form of sexual abuse against children and adolescents.

100 Despite the need to be careful regarding the complexity of the political situation in Venezuela, we consider it pertinent to record, after the external review carried out of our document, that this law was the subject of criticism by civil society organizations, which highlighted a risk to freedom of expression online, due to the lack of precision in the normative text, punishment for crimes of opinion, blocking of websites and the attribution of responsibility to digital platforms for expressions of users. See PUBLIC SPACE. **“Law against hate” in Venezuela threatens free expression in Latin America.** 17 Nov. 2017. Available at <https://espaciopublico.org/ley-odio-venezuela-amenaza-la-libre-expresion-america-latina/>. Accessed on 08/14/2024.

3.7. MERCOSUR

In this section, we will expressively apply the tools provided by the body of works selected in our theoretical framework, along with the data from the interviews compiled so far, to make comprehensive considerations on the intersection of encryption issues and the online protection of children and adolescents in the region.

3.7.1. Specific debate on the intersection of the topics

In analyzing the intersection between encryption and the protection of children and adolescents in the online context, we began with the perceptions highlighted by CRIN and Defend Digital Me. That report concludes that it is urgent to recognize the harmonization between the topics, as encryption can serve to protect and secure children and adolescents, in addition to safeguarding other rights, such as the safe development of LGBTQIA+ identities.¹⁰¹ However, as mentioned in the theoretical framework, such research is limited by perspectives from the Global North, which compels us to question: how are the debates in MERCOSUR?

In general, the political discussions connecting encryption and the protection of children and adolescents in MERCOSUR are still in their early stages. The normative proposals that jointly address both topics are not part of the construction of local political agendas and are often seen as relatively unimportant. Nonetheless, we highlight that the interviewed experts shared their concerns and worries regarding these issues.

The visions align with the premises present in Costa¹⁰² and Liguori¹⁰³, suggesting that arguments for weakening or banning strong encryption are explained by a criminalizing perspective focused on restricting rights rather than promoting them. This perspective is fueled by a weak narrative that claims there are feasible techniques for enabling secure monitoring by state agents, replicating positions that have long been present in the history of political debates on encryption and privacy since the widespread adoption of ICTs.

A reflection of this is that none of the notable cases mentioned by the interviewees illustrate the intersection between encryption and the protection of children and adolescents. The cases cited were more closely related to hate speech, fake news, incitement to self-harm, among other forms of violence, which did not directly correspond to encrypted environments as a barrier or obstacle to investigation. Even the more concrete debate in the region regarding encryption and criminal investigations, surrounding the constitutionality of WhatsApp bans in Brazil, is detached from the specific online protection issues of children and adolescents.

101 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.

102 COSTA, André Barbosa Ramiro. **Encryption policies: between the codification of rights, public regulation and cipher-activism.** 2021. Dissertation (Master's in Computer Science) - Federal University of Pernambuco, Recife, 2021. Available at <https://repositorio.ufpe.br/handle/123456789/42872>. Accessed on 25 Mar. 2024.

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

In normative terms, even in Brazil, where considerable political debates stand out, the maturity of discussions can be seen as more restricted to specialists in the field, according to the interviews conducted. On the other hand, Venezuela is characterized by more basic humanitarian concerns regarding food, health, education, and economic security, with ICT issues taking a back seat, which even allows for abuses by public authorities.

Furthermore, no critical examination was identified regarding the potential lack of proportionality in investigative methods in notable cases that involved serious risks of sexual violence against children and adolescents. This group includes situations where online communications were used to organize in-person violence, such as attacks on schools in Brazil, the specific case of Mica Ortega in Argentina, the “Blue Whale” challenge in Venezuela, and harmful challenges on digital platforms.

Another element of similarity among the countries was the existence of what is called the gamification of violence, meaning the use of gaming strategies and games as mechanisms to nurture hate speech, bullying, harassment, and other forms of violence that directly expose children and adolescents to contexts of mental distress, and in more severe cases, even to physical and sexual risks. Gamification as a form of violence was identified in interviews in countries such as Argentina, Paraguay, and Brazil. Platforms like Discord have been widely used as channels for spreading violence through gamified experiences that sought to reduce children and adolescents’ resistance to the violence they experienced. With these gaming strategies, it is possible to simulate an act of sexual abuse as a “game,” even among children, where both can be identified as victims in this scenario.

One of the sexual abuse strategies, from the “offline” mode, is the construction of tactics that conceal the violence, disguising it as jokes, games, affection, among other narratives constructions that reduce the possibility of the child or adolescent being perceived as a victim of sexual assault.¹⁰⁴ Thus, gamification can reproduce old tactics in the digital realm, perpetuating violence against vulnerable groups. In Pereira’s reflection,¹⁰⁵ the construction of “camouflages” for sexual violence reveals the even more acute risk of strategies such as the “gamification of hate” when it comes to children and adolescents.

Discussions about childhood, in turn, prevail throughout MERCOSUR. If any aspect of these discussions touches on digital security, the topic tends to be framed within the context of sexual violence or other offenses against children and adolescents, such as debates on grooming, cyberbullying, and sexting. Part of this may explain the origin of actions that indirectly seek to reduce digital security, based on a narrative of combating sexual violence against children and adolescents that does not even

104 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.

105 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.

mention or consider its impacts on that same population. Thus, proposals emerge to facilitate access to encrypted communications, allow the decryption of mobile devices in criminal investigations, or enable the traceability of instant messages. This invisibility regarding the importance of encryption, however, as Liguori warns, is itself a political option in the legal debate.

The emotion and sensitivity surrounding the topic of sexual violence sometimes serve to prevent certain prior inquiries, such as questioning the possibility of the alleged perpetrator's innocence. A notable example was the Escola Base case in São Paulo¹⁰⁶, when the owners and staff of a school were unjustly accused by the mainstream media of producing child sexual abuse content, before any investigation and fact-finding, harming the institution, the individuals involved, and their families.

From this perspective, we dare to infer that without serious and evident illegality, society would indeed feel comfortable turning a blind eye to real abuses committed by public security authorities against an adult (or even a teenager) suspected of committing a crime (or offense) against childhood. Actions that invade, break, or manipulate encryption weaken security, regardless of the results achieved in the investigation. However, identifying the suspect would not be enough to eliminate risks to the innocent. Abuses compromise the safety of everyone, including children and adolescents, in their unique status as developing individuals, making encryption a diffuse interest, as Liguori points out.¹⁰⁷

Some questions may arise from this analysis: to what extent do local governments seek—or might they come to seek—to use these narratives as a way to justify actions of vigilantism and excessive state control? The construction of narratives based on binary/dualistic frameworks often places the central themes discussed in completely distinct poles, masking the real problems that need to be addressed and the democratic and legitimate ways to control violence, for example.

With this perspective in mind, we can even extrapolate and regard as violators of the rights of children and adolescents the proposals that, concerned with the legitimate urgency of ensuring comprehensive online protection, view the weakening of encryption as an acceptable means, or digital monitoring and surveillance procedures for children and adolescents, as is the case with one of the provisions in PL 2628/2022,¹⁰⁸ in Brazil. We reiterate that privacy is also a fundamental right of this group and there is no scientific evidence, as far as our analysis was concerned, that breaking encryption for criminal investigation purposes would result in a reduction in violence against children and adolescents in digital environments.

In this context, we can explain one of the possible reasons why we find social organizations and legislative discussions dedicated to childhood issues in their various aspects more readily. In interviews with these experts, when asked about the challenges posed by the digitization of social relations, encryption as a technique was not questioned; rather, the focus was solely on issues of education, misinformation, hate speech, and personal data.

106 <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2024/03/28/caso-escola-base-30-anos.htm>

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

108 BRAZIL. **Bill No. 2628, of 2022**. Provides for the protection of children and adolescents in digital environments. Senator Alessandro Vieira (PSDB/SE). National Congress. Available at <https://www.congressonacional.leg.br/materias/materias-bicameras/-/ver/pl-2628-2022>. Accessed on 26 Mar. 2024.

Despite the lack of the intersection that we were looking for, we observed a growing rapprochement between the topics of technological security and personal data protection. This approach references Argentina and Uruguay's adherence to the European norm of Convention 108+. This connection can be seen as a response to international pressure for compliance with the standard established by the General Data Protection Regulation, in effect in Europe since 2018, reflecting possible historical influences stemming from the colonial period. However, it is important to note that regulations focused on data protection were not central subjects of this study, as already outlined in the methodology of this report.

By creating a map of risks and concerns mentioned by our interviewees, we found that the most frequently cited are: a) risk of exposure of children/adolescents; b) low digital literacy among youth and their guardians; c) digital divide in terms of technology and infrastructure; d) violences such as doxxing, cyberbullying, hate speech, sexting, grooming, among others; e) the weakening of encryption serving as a deterrent to the adoption and development of security and privacy measures; f) the capture of youth rights agendas in the context of platform regulation.

Regarding specific risks for each country, in Argentina we identified the need to create public security policies that do not place children and adolescents solely in a passive condition, worthy of protection, but also as subjects of the security process, establishing open and emancipatory dialogues. This element is consistent with Bretan literature¹⁰⁹ on the need to establish new perspectives of protection beyond the "passive victim" scenario, in which the victim is merely an object of pity in the relationship, distant and forgotten. This creates a new criminological logic for understanding the existing relationships within a given context.

In Brazil, the existing context of clashes over the regulation of digital platforms, as well as the idea of a tech-solutionism for holding individuals accountable, have been highlighted as risks. This is because the lack of normative parameters for accountability, or the relentless pursuit of a singular digital solution, can create room for legitimizing state actions that are contrary to the protection of fundamental rights, such as privacy. The search for narratives with popular appeal against violent actions aimed at children and adolescents can elucidate political disputes existing in a given social context and their capacity to generate strong mobilization and social commotion. As Bretan puts it: "[...] the issue of sexual violence against children and adolescents has a mobilizing power that goes beyond political convictions, as it has a strong popular appeal. [...] Who will have the courage to oppose it?"¹¹⁰

Paraguay highlighted an important reflective empirical risk: the use by Latin American countries of normative and/or oversight fragility to benefit structures involved in the production and/or commercial circulation of sexual violence content involving children and adolescents. This possibility, even without precise data, points to the need for deeper investigation to understand whether there is any basis for this speculation, particularly for advancing regulations that involve international cooperation, such as the development of a MERCOSUR agenda to combat online sexual violence against children and adolescents.

109 BRETAN, Maria Emilia Accioli Nobre. *Op. Cit.*

110 BRETAN, Maria Emilia Accioli Nobre. *Op. Cit.* p. 255

Finally, among the risk topics mentioned in the context of Uruguay, we would like to highlight the risk presented by the possible construction of a culture of hypervigilance of children and adolescents. The establishment of total control by parents or the State over the use of digital technologies by children and adolescents is contrary to their progressive autonomy and may represent a violation of their rights. If we recognize that sexuality, as a basic element of the human experience, needs to be understood as a human right,¹¹¹ so would technological intimacy and privacy.

Therefore, it is worth asking ourselves in what scenario such rights would be guaranteed to children and adolescents, especially LGBTQIA+, when we witness exacerbated social surveillance. This risk of total surveillance, and possible persecution of groups of children and adolescents crossed by different social markers, is not a risk identified only in Uruguay; the possibility of using narratives to combat sexual violence can be used in other social contexts as a way of monitoring and persecuting LGBTQIA+ children, for example, even more so in the case of authoritarian governments¹¹².

Finally, a risk highlighted exclusively in the context of Venezuela serves as a reminder that, even within an economic bloc like MERCOSUR, there are significant asymmetries between countries and regions, whether economic, digital, or energetic. Interviewed experts pointed to energy distribution as a gap that clearly affects technological infrastructure and digital access. This risk is mentioned for analysis, as we do not consider juvenile vigilantism a viable protection strategy; we also recognize that digital exclusion is not a protective benefit, but rather another challenge that urgently requires consolidated advancements to be addressed.

3.7.2. Normative and technological artifacts

By combining the interviews with our own highlighted analysis of the current legal framework under discussion in each country, we recognize that MERCOSUR has a **vast normative landscape concerning the rights of children and adolescents**, partly due to adherence to the Convention on the Rights of the Child. We thus identify a clear legal positioning by the States demonstrating their commitment to this issue.

Notably, the LOPNNA Bil from Venezuela stands out. We do not overlook the delicate political-legal situation in the country, including issues related to human rights, both general and specific to childhood and youth, as highlighted by the interviewees. However, in normative terms, the legislation offers important elements for the protection of the rights of children and adolescents within MERCOSUL in at least two respects.

First, the presumption of youth, which states that in cases of doubt, the individual should be treated as under eighteen. This rule removes any exemption of responsibility for digital platforms regarding content moderation. For example, in cases of sexist hate speech, it would not be appropriate to infer that the victim is an adult solely based on the mature appearance of their body, as is sometimes argued

111 PEREIRA, Wilson Guilherme Dias. *Op. Cit.*

112 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.

in Brazilian courts—a practice that Pereira criticizes in their research, categorizing it as the “[...] role of Brazilian law in the flexibilization of guarantees for sexual rights [...]”¹¹³, and for the author, such flexibilization reflects issues that range from the culture of rape to a cultural process of child marriage.

Second, the inviolability of the home and the confidentiality of correspondence also apply in the context of children and adolescents, not just from the perspective of protecting adults. Supporting this progressive guarantee of privacy for children and adolescents highlights the importance of strong encryption, considering that in the information society, instant messages serve the role of traditional paper letters. As affirmed by the research from CRIN and Defend Digital Me¹¹⁴ encryption occupies an important space in protecting the rights of children and adolescents, regarding their privacy.

Nonetheless, **the majority of countries do not mention encryption in their legislation.** Those that do, limit it to the protection of personal data, without any express approach to the rights of children and adolescents. Only a hermeneutic effort allows us to deal with the intersection that is our object in this research.

In the same vein of prevalence regarding absence, concerning **technological artifacts** to protect children and adolescents in digital environments with encryption, we see in MERCOSUL a general scenario of a **lack of implemented or effectively proposed tools for this shared purpose.** We did not identify actions aimed at the development or application of technological artifacts from government, the private sector, academia or even civil society initiatives aimed at protecting children and adolescents in encrypted environments.

Even in Brazil, the helplines and assistance systems can only operate after a threat or violation of rights, and are not specific to this specific issue, in addition to not falling within the concept of technological artifacts that we consider in this research. In turn, the already mentioned and disproportionate client-side scanning announced by Apple to be available in the U.S. in 2021 did not even have a scheduled implementation date in the MERCOSUR countries.¹¹⁵ Likewise, the inadequate legal provision in Paraguay requiring telecoms to offer a parental control tool was not implemented in practice, which incidentally has no explicit rules on encryption (and, it must be repeated, lacks

113 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. 53 and 54.

114 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.

115 Account “*Features available in the U.S*” (“resources available in the US”, in English) in the document “Expanded Protections for Children — Technology Summary”, available on the company’s website (APPLE. Expanded Protections for Children — Technology Summary. August 2021. Available at https://www.apple.com/childsafety/pdf/Expanded_Protections_for_Children_Technology_Summary.pdf. Accessed on October 13th. 2022. P. 3). For more details on Apple’s proposal, see PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. **Client-side scanning: a systematic review.** Belo Horizonte: Internet and Society Reference Institute, November 2022. Available at <https://irisbh.com.br/publicacoes/comunicacoes-privadas-investigacoes-e-direitos-varredura-pelo-lado-do-cliente/>. Accessed on: 30 Nov. 2022. p. 13-14.

appropriate safeguards). Additionally, we recall, along with Costa¹¹⁶ and Liguori,¹¹⁷ that the use of private software by the public authority for state surveillance and the private market for personal data are undergoing a joint expansion.

Concerns also arise about how software intended for young audiences can be used for commercial profiling, exposing children and adolescents to targeted and potentially exploitative advertisements. The lack of effective regulation and the inconsistent implementation of these measures highlight the urgent need for more comprehensive and stringent policies to protect the privacy and safety of children and adolescents on digital platforms.

In a comparative analysis, it seems to us that the methods to combat sexual violence against children and adolescents in digital environments, as well as the documentary narratives of government institutions, center primarily around criminalization and the field of criminal law, in a focus criticized by Liguori¹¹⁸. Thus, despite the critical questions in society regarding the methods to confront these violences¹¹⁹, the institutional narrative and state actions still focus on the criminal area. This may occur, as hypothesized here, due to the prevailing narrative that it is necessary to break encryption to protect children and adolescents in online environments, supported by the logic of the criminal field, or, more likely, because states choose not to invest in preventive measures such as digital literacy.

The lack of normative discussions that encompass both the protection of children and adolescents from online sexual violence and the protection of encryption and privacy for this group can open the door to illegal excessive monitoring by public security institutions and create a false sense that, in addressing issues of complex social magnitude and seeking criticality for effective actions, one side of the coin must be chosen. Creating a political agenda based on a multisectoral discussion could be one of the pathways proposed for actions that include the protection of children and adolescents, as well as their privacy.

In this sense, a possible next step would be to investigate the practical reality of investigations into sexual violence crimes against children and adolescents in each country, both to assess potential bottlenecks that ICT security may be imposing on the efforts of public security authorities in the region, and to evaluate the seriousness of the absence of minimum protocols for the online protection of human rights and fundamental guarantees, including those concerning children and adolescents living in MERCOSUR.

116 COSTA, André Barbosa Ramiro. **Encryption policies: between the codification of rights, public regulation and cipher-activism**. 2021. Dissertation (Master's in Computer Science) - Federal University of Pernambuco, Recife, 2021. Available at <https://repositorio.ufpe.br/handle/123456789/42872>. Accessed on 25 Mar. 2024.

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

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

119 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.

4. Final considerations

Narratives, norms and technology in MERCOSUR on encryption and online sexual violence against children and adolescents

In seeking to overcome the false polarization in the interrelationship between encryption and the human rights of children and adolescents in the digital sphere, the study “Privacy and Protection: a children’s rights approach to encryption”¹²⁰ concludes, among other points, that the public debate on cryptography and the online sexual exploitation and abuse of children has become ““hostile and emotional in a way that hindered change,” with “a tendency to shift away from targeted criticism of arguments towards more personal complaints related to what many consider insensitive and immoral positions.”¹²¹.

In order to understand the regional scenario, considering the complex theme of narrative disputes between the fields of child and adolescent protection and cryptography in MERCOSUR countries,, our research sought to undertake reflections combining academic readings and semi-structured interviews with local experts in both fields, in order to identify the political, social and economic contexts.

As a theoretical framework, the works of CRIN; Defend Digital Me, Liguori, Costa, Pereira, and Betran provided us with tools for a comprehensive view of the topics of cryptography, understood as a political security technology, and online sexual violence against children and adolescents, understood as a type of offense against the sexual rights of a population that is legally prioritized for protection due to its peculiar developmental status.

In our analysis of normative discourses and the narratives of the interviewees, we found that MERCOSUL countries: a) lack specific legislation regarding the protection of the rights of children and adolescents in digital environments with cryptography, particularly concerning online sexual violence; b) engage in rare and incipient legislative debates on this intersection, and do not provide space for the participation of the target audience of public policies that directly affect their unique developmental status, nor do they recognize them as active rights subjects capable of contemplating their own legal and technological situation; c) lack existing legal norms specific to encryption, with Brazil conducting more developed legislative debates, but without effective outcomes in legislation or public policies; d) do not have technological artifacts—either due to their non-existence or the lack of knowledge among the interviewees regarding this specific field.

Regarding the specific legal framework for children and adolescents, which follows the international

120 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.

121 CRIN; Defend Digital Me. *On cit.* P. 62.

norms of the UN Convention, practices vary according to the implementation of the guaranteed rights. In this context, Brazil leads more intense discussions, while Venezuela focuses on concerns such as food security and formal education, relegating technological issues to a secondary level. However, it is worth mentioning Venezuela's LOPNNA Bill, which, despite the country's delicate political-legal context, significantly addresses the protection of the rights of children and adolescents in MERCOSUR in at least two important normative aspects. First, there is the juvenile presumption, where it is assumed that, in case of doubt, the individual must be treated as under eighteen years of age, which prevents exemptions from liability for digital platforms in content moderation; and, second, the inviolability of the home and the secrecy of correspondence extends to the children's context.

Furthermore, the risks associated with the lack of specific regulation range from the potential emergence of protective legal provisions that require technological vulnerabilities, leading to criminalization and the use of the criminal justice system, to the possibility of regulations that unnecessarily and disproportionately restrict the citizenship rights, privacy, and freedom of expression of children and adolescents in digital environments. Additionally, there is the imminent threat of this group being overexposed to inappropriate content, without the implementation of adequate technological security measures, both in domestic settings and on digital platforms. Lastly, it is important to emphasize that these risks are exacerbated by the widespread lack of digital literacy and the absence of appropriate discursive approaches aimed at the youth population.

Despite the absence of specific discussions in those countries, the majority of respondents support the need to create laws that balance the protection of encryption with the rights of children and adolescents. This highlights the lack of minimum standards to promote fundamental rights such as privacy and sexual integrity for these young people. Arguments against limiting encryption are seen as restrictive, not promotional, reflecting historical debates about privacy since the popularization of digital technologies. Proposals that weaken encryption or allow abusive digital monitoring of young people are considered potentially harmful to the protection of their fundamental rights. However, the defense of strong encryption lacks practical solutions to balance security and protection against online violations of children and adolescents, with no specific initiatives identified in the studied countries.

5. References

ARGENTINA. **Act nº 23.849. Apruébase la Convención sobre los Derechos del Niño.** Boletín Oficial, 22 Oct. 1990. Available at <https://www.argentina.gob.ar/normativa/nacional/ley-23849-249/texto>. Accessed on 20 Jun. 2024.

ARGENTINA. **Ley nº 26.061. Ley de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes.** Boletín Oficial, 26 Oct. 2005. Available at <http://www.saij.gob.ar/26061-nacional-ley-proteccion-integral-derechos-ninas-ninos-adolescentes-lns0004968-2005-09-28/123456789-0abc-defg-g86-94000scanyel>. Accessed on 25 Mar. 2024.

ARGENTINA. **Ley nº 26.904. Modificación del Código Penal. Delitos contra la Integridad Sexual. Grooming.** Boletín Oficial, 13 Nov. 2013. Available at <http://www.saij.gob.ar/26904-nacional-modificacion-codigo-penal-delitos-contra-integridad-sexual-grooming-lnn0029869-2013-11-13/123456789-0abc-defg-g96-89200ncanyel>. Accessed on 25 Mar. 2024.

ARGENTINA. **Ley nº 27.436. Modificación del Código Penal en la Parte correspondiente a Delitos contra la Integridad Sexual.** Boletín Oficial, 23 Apr. 2018. Available at <http://www.saij.gob.ar/27436-nacional-modificacion-codigo-penal-parte-correspondiente-delitos-contra-integridad-sexual-lnn0029908-2018-03-21/123456789-0abc-defg-g80-99200ncanyel>. Accessed on 25 Mar. 2024.

ARGENTINA. **Ley nº 27.590. Ley Mica Ortega. Programa Nacional de Prevención y Concientización del Grooming o Ciberacoso contra Niñas, Niños y Adolescentes.** Boletín Oficial, 11 Nov. 2020. Available at <http://www.saij.gob.ar/27590-nacional-ley-mica-ortega-programa-nacional-prevencion-concientizacion-grooming-ciberacoso-contra-ninas-ninos-adolescentes-lns0006926-202-0-11-11/123456789-0abc-defg-g62-96000scanyel>. Accessed on 25 Mar. 2024.

ARGENTINA. Ministerio de Justicia de La Nación. **Sistema Argentino de Información Jurídica.** Available at <http://www.saij.gob.ar/>. Accessed on 25 Mar. 2024.

BARKER, George. LEHR, William. LONEY, Mark. SICKER, Douglas. **O impacto econômico das leis que enfraquecem a criptografia.** Law & Economics Consulting Associates (LECA). 05 Apr. 2021. Portuguese Translation: Paulo Rená da Silva Santarém. Internet Society - Brazil Chapter, 08 Jul. 2021. Available at: <https://isoc.org.br/noticia/o-impacto-economico-das-leis-que-enfraquecem-a-criptografia>. Accessed on 20 June 2024.

BEDINELLI, Talita; MARTÍN, María. **Baleia Azul: o misterioso jogo que escancarou o tabu do suicídio juvenil. El País,** 02 May 2017. Available at https://brasil.elpais.com/brasil/2017/04/27/politica/1493305523_711865.html. Accessed on 03 Jul 2024.

BRAZIL. **Decreto nº 99.710, de 21 de novembro de 1990. Promulga a Convenção sobre os Direitos da Criança.** Presidência da República. Available at https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm. Accessed on 20 Jun. 2024.

BRAZIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal.** Presidência da República. Available at https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Accessed on 25 Mar. 2024.

BRAZIL. **Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências.** Presidência da República. Available at https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Accessed on 25 Mar. 2024.

BRAZIL. **Lei nº 11.829, de 25 de novembro de 1990. Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na Internet.** Presidência da República. Available at https://www.planalto.gov.br/ccivil_03/ato2007-2010/2008/lei/l11829.htm. Accessed on 25 Mar. 2024.

BRAZIL. **Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Presidência da República. Available at https://www.planalto.gov.br/ccivil_03/ato2011-2014/2014/lei/l12965.htm. Accessed on 25 Mar. 2024.

BRAZIL. **Lei nº 13.431, de 4 de abril de 2017. Estabelece o sistema de garantia de direitos da criança e do adolescente vítima ou testemunha de violência e altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente).** Presidência da República. Available at https://www.planalto.gov.br/ccivil_03/ato2015-2018/2017/lei/l13431.htm. Accessed on 25 Mar. 2024.

BRAZIL. **Lei nº 13.441 de 8 de maio de 2017. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na Internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente.** Presidência da República. Available at https://www.planalto.gov.br/ccivil_03/ato2007-2010/2008/Lei/L11829.htm. Accessed on 16 May 2024.

BRAZIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Presidência da República. Available at https://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/L13709compilado.htm. Accessed on 26 Mar. 2024.

BRAZIL. Presidência da República. **Portal da Legislação.** Available at <https://www4.planalto.gov.br/legislacao>. Accessed on 25 Mar. 2024.

BRAZIL. **Projeto de Lei nº 2628, de 2022. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais.** Senator Alessandro Vieira (PSDB/SE). National Congress. Available at <https://www.congressonacional.leg.br/materias/materias-bicameras/-/ver/pl-2628-2022>. Accessed on 26 Mar. 2024.

BRAZIL. **Projeto de Lei nº 2630, de 2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet.** Senator Alessandro Vieira (CIDADANIA/SE). National Congress. Available at <https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-2630-2020>. Accessed on 26 Mar. 2024.

BRAZIL. **Projeto de Lei nº 9808/2018. Acrescenta os parágrafos 5º e 6º ao art. 10 da Lei nº 12.965, de 23 de abril de 2014, para dispor sobre o acesso a dados de comunicação por meio de aplicativos de Internet para fins de persecução criminal, nos casos que especifica.** Federal Representative João Campos (PRB/GO). National Congress. Available at <https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-9808-2018>. Accessed on 26 Mar. 2024.

BRAZIL. Chamber of Representatives. **REL 1/2021 GTNET – Relatório do Grupo de trabalho para aperfeiçoamento da legislação brasileira sobre Internet.** 28 Oct. 2021. Available at <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2305033>. Accessed on 16 Jul 2024.

BRAZIL. Federal Supreme Court. **ADI 5527.** Rapporteur: Rosa Weber. Brasília, DF. Available at: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282>. Accessed on 20 Jun 2024.

BRAZIL. Supremo Tribunal Federal. **ADPF 403.** Rapporteur: Edson Fachin. Brasília, DF. Available at: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500>. Accessed on 20 Jun 2024.

BRETAN, Maria Emilia Accioli Nobre. **Violência sexual contra crianças e adolescentes mediada pela tecnologia da informação e comunicação: elementos para a prevenção vitimal.** São Paulo, 2012. Thesis (PhD) – Faculdade de Direito da Universidade de São Paulo. Available at <https://doi.org/10.11606/T.2.2012.tde-22042013-111456>. Accessed on 25 Mar. 2024.

BUSATTO JÚNIOR, Narciso. **Criptografia homomórfica.** Monograph (Bachelor's Degree in Communication Network Engineering) – Department of Electrical Engineering, Universidade de Brasília, Brasília, 2013. Available at <https://bdm.unb.br/handle/10483/15372>. Accessed on 20 Jun. 2024.

CAMPOS, Ricardo; OLIVEIRA, Samuel Rodrigues de. SANTOS, Carolina Xavier. **O conceito de dever de cuidado no âmbito das plataformas digitais.** Revista Consultor Jurídico, 21 Mar. 2023. Available at <https://www.conjur.com.br/2023-mar-21/direito-digital-conceito-dever-cuidado-ambito-plataformas-digitais/>. Accessed on Aug. 20, 2024.

CANTO, Mariana; RAMIRO, André; REAL, Paula C. **Criptografia no STF: O que dizem os votos de Rosa Weber e Edson Fachin e o que podemos aprender com eles.** Instituto de Pesquisa

em Direito e Tecnologia do Recife (IP.rec). Available at <https://ip.rec.br/blog/criptografia-no-stf-o-que-dizem-os-votos-de-rosa-weber-e-edson-fachin-e-o-que-podemos-aprender-com-eles/>. Accessed on 20 Jun. 2024.

CARA, Daniel (rap.). **Ataque às escolas no Brasil: análise do fenômeno e recomendações para a ação governamental**. Relatório do Grupo de Trabalho Interministerial de Prevenção e Enfrentamento da Violência nas Escolas. Brasília: Ministério da Educação, 03 Nov. 2023. Available at <https://www.gov.br/mec/pt-br/aceso-a-informacao/participacao-social/grupos-de-trabalho/prevencao-e-enfrentamento-da-violencia-nas-escolas/resultados>. Accessed on 20 Aug. 2024.

CEIBAL. **Ciudadanía y Bienestar Digital**. Available at <https://ceibal.edu.uy/institucional/ciudadania-digital/marco-institucional/>. Accessed on 03 Jul 2024.

CEIBAL. **Qué es Ceibal**. Available at <https://ceibal.edu.uy/institucional/que-es-ceibal/>. Accessed on 03 Jul 2024

CETIC.BR – Regional Center for Studies for the Development of the Information Society. **TIC Kids Online Brasil - 2023. Pais e responsáveis**. 29 Aug. 2023. Available at <https://cetic.br/pt/pesquisa/kids-online/indicadores/>. Accessed on 25 Mar. 2024.

CHICOS.NET. **#Elige Tu Forma**. Available at <https://www.eligetufirma.org/home>. Accessed on 03 Jul 2024.

CHICOS.NET. **Mi primer dispositivo**. Available at <https://www.chicos.net/programa/mi-primer-dispositivo>. Accessed on 03 Jul 2024.

COPE, Sophia; CROCKER, Andrew; TRUJILLO, Mario. **The STOP CSAM Act Would Put Security and Free Speech at Risk**. Electronic Frontier Foundation, 21 Apr. 2023. Available at <https://www.eff.org/pt-br/deeplinks/2023/04/stop-csam-act-would-put-security-and-free-speech-risk>. Accessed on Aug. 9, 2024.

COUNCIL OF EUROPE. **Chart of signatures and ratifications of Treaty 108. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – ETS nº 108**. Available at <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>. Accessed on Aug. 20, 2024

COUNCIL OF EUROPE. **Chart of signatures and ratifications of Treaty 223. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - CETS nº. 223**. Available at <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223>. Accessed on Aug. 20, 2024.

COSTA, André Barbosa Ramiro. **Políticas de encriptação: entre a codificação de direitos, regulação pública e o cipher-ativismo**. 2021. 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.

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.

CRIN – Child Rights International Network. **Argentina: National Laws**. 7 Jul. 2011. Available at <https://archive.crin.org/en/library/publications/argentina-national-laws.html>. Accessed on 25 Mar. 2024.

CRIN – Child Rights International Network. **Brazil: National Laws**. 6 Jun. 2012. Available at <https://archive.crin.org/en/library/publications/brazil-national-laws.html>. Accessed on 25 Mar. 2024.

CRIN – Child Rights International Network. **Paraguay: National Laws**. 8 Dec. 2011. Available at <https://archive.crin.org/en/library/publications/paraguay-national-laws.html>. Accessed on 25 Mar. 2024.

CRIN – Child Rights International Network. **Uruguay: National Laws**. 26 Jul. 2013. Available at <https://archive.crin.org/en/library/publications/uruguay-national-laws.html>. Accessed on 25 Mar. 2024.

CRIN – Child Rights International Network. **Venezuela: Children's Rights References In The Universal Periodic Review**. 25 May. 2017. Available at <https://archive.crin.org/en/library/publications/venezuela-childrens-rights-references-universal-periodic-review.html>. Accessed on 25 Mar. 2024.

DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Rená da Silva; VIEIRA, Víctor Barbieri Rodrigues. **Hacking Governamental: uma revisão sistemática**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, February 2023. Available at <https://bit.ly/3YdVcIL>. Accessed on: 26 June 2024.

DUTRA, Luiza Correa de Magalhães; SANTARÉM, Paulo Rená da Silva; VIEIRA, Víctor Barbieri Rodrigues; PEREIRA, Wilson Guilherme Dias. **Guia Informativo: Artefatos Normativos Sobre Direitos de Crianças e Adolescentes em Ambientes Digitais no MERCOSUL**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024. Available at <https://bit.ly/3VsxQzz>. Accessed on: 20 June 2024.

PUBLIC SPACE. **“Ley contra el odio” en Venezuela amenaza la libre expresión en América Latina**. 17 Nov. 2017. Available at <https://espaciopublico.org/ley-odio-venezuela-amenaza-la-libre-expresion-america-latina/>. Accessed on 08/14/2024.

ESTEFANELLI, Lorena. **Pantallas em Casa: Orientaciones para acompañar una navegación segura en Internet. Guía para las familias**. Plan Ceibal, ANEP, UNICEF, Nov. 2023. Available at <https://www.unicef.org/uruguay/informes/pantallas-en-casa>. Accessed on 27 Jun. 2024.

FAIRPLAY. **Global Platforms, Partial Protections.** 12 Jul 2022. Available at <https://fairplayforkids.org/design-discrimination-july2022/>. Accessed on 20 June 2022.

FIGHT FOR THE FUTURE. **Letter: Civil rights groups reaffirm opposition to KOSA, emphasize continued threat to LGBTQ youth.** 29 June 2023. Available at: <https://www.fightforthefuture.org/news/2023-06-29-letter-civil-rights-groups-reaffirm-opposition-to-kosa-emphasize-continued-threat-to-lgbtq-youth>. Accessed on: 27 Mar. 2024.

FIGUEIREDO, Ana Luiza. Congresso dos EUA avança com medidas de proteção infantil na Internet. **Olhar Digital.** 27 Jul 2023. Available at <https://olhardigital.com.br/2023/07/27/seguranca/congresso-dos-eua-avanca-com-medidas-de-protecao-infantil-na-Internet/>. Accessed on 20 June 2024.

FUKE FACHINETTI, Aline; CAMARGO, Guilherme. **Convenção 108+: o tratado de proteção de dados e a relevância do tema para o Brasil.** Revista Consultor Jurídico, 04 Jul. 2021. Available at <https://www.conjur.com.br/2021-jul-04/opinio-convencao-108-relevancia-protecao-dados/>. Accessed on Aug. 20, 2024

GALF, Renata; PINHO, Angela. **Entenda quais itens do PL das Fake News têm relação com moderação de conteúdo.** Folha de S.Paulo, 06 May 2023. Available at <https://www1.folha.uol.com.br/poder/2023/05/entenda-quais-itens-do-pl-das-fake-news-tem-relacao-com-moderacao-de-conteudo.shtml>. Accessed on Aug. 20, 2024.

HALFELD, Emanuella; TEREZA, Júlia; SANTOS, Pedro Henrique M. A gamificação do ódio no cenário brasileiro: um mapeamento das estratégias de enfrentamento do GT do Ministério dos Direitos Humanos e da Cidadania. In: SILVA, Fernanda dos Santos Rodrigues; VIEIRA, Victor Barbieri Rodrigues (orgs). **Anais do IV Seminário Governança das Redes.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024. Available at <https://bit.ly/4dn76bB>. Accessed on 02 Jul. 2024.

INSTITUTO ALANA; MINISTÉRIO PÚBLICO DE SÃO PAULO. **Comentário Geral N° 25 (2021) sobre os Direitos das Crianças em relação ao ambiente digital. Versão Comentada.** 16 Apr. 2022. Available at <https://criancaconsumo.org.br/biblioteca/comentario-geral-n-25/>. Accessed on 20 June 2024.

INTERNET SOCIETY - BRAZIL CHAPTER. **Conteúdos da Internet Society sobre criptografia.** 18 Aug. 2020. Available at <https://isoc.org.br/noticia/conteudos-da-Internet-society-sobre-criptografia>. Accessed on 20 Jun. 2024.

INTERNET SOCIETY - BRAZIL CHAPTER. **Factsheet: Criptografia essencial para a comunidade LGBTQIA+.** 16 Jun. 2021. Available at <https://isoc.org.br/noticia/factsheet-criptografia-essencial-para-a-comunidade-lgbtqia>. Accessed on 20 Jun. 2024.

INTERNET SOCIETY - BRAZIL CHAPTER. **Manifestação ao STF para reconhecer a importância da criptografia na proteção a direitos fundamentais.** 08 Jun. 2023. Available at <https://isoc.org.br/>

[noticia/manifestacao-ao-stf-para-reconhecer-a-importancia-da-criptografia-na-protecao-a-direitos-fundamentais](#). Accessed on 20 Jun. 2024.

INTERNET SOCIETY - BRAZIL CHAPTER. **SBSeg | A Criptografia na Proteção a Grupos Vulneráveis**. 12 Sep. 2022. Available at <https://isoc.org.br/noticia/sbseg-a-criptografia-na-protecao-a-grupos-vulneraveis>. Accessed on 20 Jun. 2024.

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

MACKEY, Aaron; KELLEY, Jason. **Analyzing KOSA's Constitutional Problems In Depth**. Electronic Frontier Foundation, 15 Mar. 2024. Available at <https://www.eff.org/deeplinks/2024/03/analyzing-kosas-constitutional-problems-depth>. Accessed on 2 Aug. 2024.

MARQUES, Cláudia Lima; LIMA, Cíntia Rosa Pereira de; PEROLI, Kelvin. **A proteção de dados pessoais nos Estados-membros do MERCOSUL**. Revista Eletrônica CNJ, Brasília, v. 7, no. 1, p. 45-56, Jan./Jun. 2023. Available at <https://bdjur.stj.jus.br/jspui/handle/2011/177398>. Accessed on 03 Jul 2024.

MERCOSUR. **Decisão sobre a suspensão da Venezuela no MERCOSUL**. São Paulo, 05 Aug. 2017. Available at <https://www.mercosur.int/pt-br/decisao-sobre-a-suspensao-da-republica-bolivariana-da-venezuela-no-mercosul/>. Accessed on June 17th. 2024.

MERCOSUR. **Quem somos em poucas palavras**. Available at: <https://www.mercosur.int/pt-br/quem-somos/em-poucas-palavras/>. Accessed on: 19 June. 2024.

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; 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.

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.

UN – United Nations Organization. Committee on the Rights of the Child. **Comentário Geral Nº 25 (2021) sobre os Direitos das Crianças em relação ao ambiente digital**. 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://criancaeconsumo.org.br/wp-content/uploads/2022/01/comentario-geral-n-25-2021.pdf>. Accessed on 20 June 2024.

PARAGUAY. **Biblioteca y Archivo Central del Congreso de La Nación**. Available at <https://www.bacn.gov.py/>. Accessed on 25 Mar. 2024.

PARAGUAY. **Constitución Nacional de la República del Paraguay**. Asunción, 20 Jun. 1992. Biblioteca y Archivo Central del Congreso de La Nación. Available in <https://www.bacn.gov.py/constitucion-nacional-de-la-republica-del-paraguay>. Accessed on 17 Jun. 2024.

PARAGUAY. **Ley nº 57/1990. Que aprueba y ratifica la Convención de Las Naciones Unidas sobre los derechos del Niño**. Corte Suprema de Justicia. Available at <http://www.csj.gov.py/cache/lederes/P-0-20121990-L-57-1.pdf>. Accessed on 20 Jun. 2024.

PARAGUAY. **Ley nº 1.160 / Código Penal**. 16 Nov. 1997. Biblioteca y Archivo Central del Congreso de La Nación. Available in <https://www.bacn.gov.py/leyes-paraguayas/3497/ley-n-1160-codigo-penal>. Accessed on 25 Mar. 2024.

PARAGUAY. **Ley nº 1.680 / Código De La Niñez Y La Adolescencia**. 04 Jun. 2001. Biblioteca y Archivo Central del Congreso de La Nación. Available in <https://www.bacn.gov.py/leyes-paraguayas/5261/ley-n-1680-codigo-de-la-ninez-y-la-adolescencia>. Accessed on 25 Mar. 2024.

PARAGUAY. **Ley nº 2.861 / Reprime El Comercio Y La Difusion Comercial O No Comercial De Material Pornografico, Utilizando La Imagen U Otra Representacion De Menores O Incapaces**. 17 Jan. 2013. Biblioteca y Archivo Central del Congreso de La Nación. Available in <https://www.bacn.gov.py/leyes-paraguayas/1944/ley-n-2861-reprime-el-comercio-y-la-difusion-comercial-o-no-comercial-de-material-pornografico-utilizando-la-imagen-u-otra-representacion-de-menores-o-incapaces>. Accessed on 25 Mar. 2024.

PARAGUAY. **Ley nº 4.439 / Modifica Y Amplia Varios Artículos De La Ley Nº 1160/97 “Código Penal”**. 05 Nov. 2011. Biblioteca y Archivo Central del Congreso de La Nación. Available in <https://www.bacn.gov.py/leyes-paraguayas/3777/modifica-y-amplia-varios-articulos-de-la-ley-n-116097-codigo-penal>. Accessed on 25 Mar. 2024.

PARAGUAY. **Ley nº 5.653 / Protección de Niños, niñas y Adolescentes contra Contenidos Nocivos de Internet**. 29 Sep. 2016. Biblioteca y Archivo Central del Congreso de La Nación. Available in <https://www.bacn.gov.py/leyes-paraguayas/5167/proteccion-de-ninos-ninas-y-adolescentes-contra-contenidos-nocivos-de-Internet>. Accessed on 20 Jun. 2024.

PARAGUAY. **Ley nº 6.002 / Modifica El Artículo 135 De La Ley Nº 1160/97 “Código Penal”, Modificado Por El Artículo 1º De La Ley Nº 3440/08 “Que Modifica Varias Disposiciones De La Ley Nº 1160/97 ‘Código Penal’”**. Biblioteca y Archivo Central del Congreso de La Nación. Available in <https://www.bacn.gov.py/leyes-paraguayas/9906/ley-n-6002-modifica-el-articulo-135-de-la-ley-n-116097-codigo-penal-modificado-por-el-articulo-1-de-la-ley-n-344008-que-modifica-varias-disposiciones-de-la-ley-n-116097-codigo-penal>. Accessed on 25 Mar. 2024.

PARAGUAY. **Plan de educación en tiempos de pandemia “Tu escuela en casa” 2020**. SITEAL –

Educational Trends Information System in Latin America. Available at <https://siteal.iiep.unesco.org/pt/node/2861>. Accessed on 03 Jul 2024.

PEREIRA, Wilson Guilherme Dias. **ONDE ESTAVAM VOCÊS QUANDO EU PRECISEI? Percepções de vítimas de violência sexual infantojuvenil LGBTQIA+ sobre o Sistema de Garantia de Direitos de Porto Velho**. Porto Velho, 2023. Dissertation (Master's) – Interdisciplinary Professional Master's Postgraduate Program in Human Rights and Justice Development. Universidade Federal de Rondônia. Available at <https://dhjus.unir.br/pagina/exibir/22968>. Accessed on 17 Jun. 2024.

PEREIRA, Wilson Guilherme Dias; VIEIRA, Victor Barbieri Rodrigues. **Violência Sexual Online e Criptografia**. Instituto de Referência em Internet e Sociedade, 05 Mar. 2024. Available at <https://irisbh.com.br/violencia-sexual-online-e-criptografia/>. Accessed on July 15th. 2024.

PLACAMAE.ORG. **Cyberbullying: como se proteger?** 30 Jun. 2024. Available at <https://placamae.org/publicacao/cyberbullying-como-se-proteger/>. Accessed on 20 Jun. 2024.

RAMIRO, André; et al. **O Mosaico Legislativo da Criptografia no Brasil: uma análise de projetos de Lei**. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), 2020. Available at <https://ip.rec.br/publicacoes/o-mosaico-legislativo-da-criptografia-no-brasil-uma-analise-de-projetos-de-lei/>. Accessed on 20 Jun. 2024.

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 20 Jun. 2024.

RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. **Comunicações privadas, investigações e direitos: rastreabilidade de mensagens instantâneas**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, May 2022. Available at <https://irisbh.com.br/publicacoes/comunicacoes-privadas-investigacoes-e-direitos-rastreabilidade-de-mensagens-instantaneas/>. Accessed on 20 Jun. 2024.

SAFERNET. **SaferNet recebe o prêmio Neide Castanha de Direitos Humanos de Crianças e Adolescentes**. 15 May 2024. Available at <https://new.safernet.org.br/content/safernet-recebe-o-premio-neide-castanha-de-direitos-humanos-de-criancas-e-adolescentes>. Accessed 20 Jun. 2024.

SAFERNET. **Safernet recebe recorde histórico de novas denúncias de imagens de abuso e exploração sexual infantil na Internet**. 06 Feb. 2024. Available at <https://new.safernet.org.br/content/safernet-recebe-recorde-historico-de-novas-denuncias-de-imagens-de-abuso-e-exploracao-sexual>. Accessed on 26 Mar. 2024.

SANTARÉM, Paulo Rená da Silva. **O “dever de cuidado” seria um descuido indevido**. Desinformante, 08 May 2023. Available at <https://desinformante.com.br/dever-de-cuidado-riscos/>. Accessed on 20 Aug. 2024.

SANTARÉM, Paulo Rená da Silva; PEREIRA, Wilson Guilherme Dias. **Caminhos da pesquisa: nossos marcos teóricos para criptografia**. Instituto de Referência em Internet e Sociedade, 01 Jul. 2024. Available at <https://irisbh.com.br/marcos-teoricos-para-criptografia/>. Accessed on 15 Jul. 2024.

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/violencia-sexual-online-e-criptografia/>. Accessed on 15 Jul. 2024.

SITEAL – Educational Trends Information System in Latin America; UNICEF – United Nations Children’s Fund; ARCOR FOUNDATION. **Perfil de País: Argentina**. 19 Jun. 2022. Available at <https://siteal.iiep.unesco.org/pt/pais/primer-infancia-pdf/argentina>. Accessed on 25 Mar. 2024.

SITEAL – Educational Trends Information System in Latin America; UNICEF – United Nations Children’s Fund; ARCOR FOUNDATION. **Perfil de País: Brasil**. 19 Jun. 2022. Available at <https://siteal.iiep.unesco.org/pt/pais/primer-infancia-pdf/brasil>. Accessed on 25 Mar. 2024.

SITEAL – Educational Trends Information System in Latin America; UNICEF – United Nations Children’s Fund; ARCOR FOUNDATION. **Perfil de País: Paraguai**. 19 Jun. 2022. Available at <https://siteal.iiep.unesco.org/pt/pais/primer-infancia-pdf/paraguay>. Accessed on 25 Mar. 2024.

SITEAL – Educational Trends Information System in Latin America; UNICEF – United Nations Children’s Fund; ARCOR FOUNDATION. **Perfil de País: Uruguai**. 19 Jun. 2022. Available at <https://siteal.iiep.unesco.org/pt/pais/primer-infancia-pdf/uruguay>. Accessed on 25 Mar. 2024.

SITEAL – Educational Trends Information System in Latin America; UNICEF – United Nations Children’s Fund; ARCOR FOUNDATION. **Perfil de País: Venezuela**. 19 Jun. 2022. Available at <https://siteal.iiep.unesco.org/pt/pais/primer-infancia-pdf/venezuela>. Accessed on 25 Mar. 2024.

FEDERAL SUPREME COURT. **Ministro Alexandre de Moraes revoga bloqueio após Telegram cumprir determinações do STF**. 20 Mar 2022. Available at <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=483712&ori=1>. Accessed on 20 Aug. 2024.

SUZUKI, Shin. **Telegram: as mudanças que levaram STF a liberar aplicativo no Brasil**. BBC Brasil, 22 Mar. 2022. Available at <https://www.bbc.com/portuguese/brasil-60841371>. Accessed on 20 Aug. 2024.

UNESCO – United Nations Educational, Scientific and Cultural Organization. Office for Latin America and the Caribbean. IIEP – International Institute for Educational Planning. **Políticas e regulamentações**. SITEAL – Educational Trends Information System in Latin America. Available at <https://siteal.iiep.unesco.org/pt/politicas>. Accessed on 09 Aug. 2024.

UNICEF – United Nations Children’s Fund. **Convenção sobre os Direitos da Criança**. UNICEF Brasil, 29 Sep. 2017. Available at <https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca>.

Accessed on 25 Mar. 2024.

UNICEF – United Nations Children’s Fund. **How many children and young people have Internet access at home?** Dec. 2020. Available at <https://data.unicef.org/resources/children-and-young-people-Internet-access-at-home-during-covid19/>. Accessed on 25 Mar. 2024.

UNICEF – United Nations Children’s Fund. **Remote learning and digital connectivity.** 26 Jul. 2021. Available at <https://data.unicef.org/topic/education/remote-learning-and-digital-connectivity>. Accessed on 25 Mar. 2024.

UNICEF – United Nations Children’s Fund. **UNICEF Argentina Country Office Annual Report 2023.** 16 Feb. 2024. Available at <https://www.unicef.org/reports/country-regional-divisional-annual-reports-2023/Argentina>. Accessed on 25 Mar. 2024.

UNICEF – United Nations Children’s Fund. **UNICEF Brazil Country Office Annual Report 2023.** 16 Feb. 2024. Available at <https://www.unicef.org/reports/country-regional-divisional-annual-reports-2023/Brazil>. Accessed on 25 Mar. 2024.

UNICEF – United Nations Children’s Fund. **UNICEF Paraguay Country Office Annual Report 2023.** 16 Feb. 2024. Available at <https://www.unicef.org/reports/country-regional-divisional-annual-reports-2023/Paraguay>. Accessed on 25 Mar. 2024.

UNICEF – United Nations Children’s Fund. **UNICEF Paraguay Country Office Annual Report 2023.** 16 Feb. 2024. Available at <https://www.unicef.org/reports/country-regional-divisional-annual-reports-2023/Venezuela>. Accessed on 25 Mar. 2024.

UNICEF – United Nations Children’s Fund. **UNICEF Paraguay Country Office Annual Report 2023.** 19 Feb. 2024. Available at <https://www.unicef.org/reports/country-regional-divisional-annual-reports-2023/Uruguay>. Accessed on 25 Mar. 2024.

URUGUAY. **Constitucion de la República.** 02 Feb. 1967. IMPO. Available at <https://www.impo.com.uy/bases/constitucion/1967-1967>. Accessed on June 17th. 2024.

URUGUAY. **Ley nº 9.155. Código Penal.** 04 Dec. 1933, att. 26 Oct. 1967. IMPO. Available at <https://www.impo.com.uy/bases/codigo-penal/9155-1933>. Accessed on 25 Mar. 2024.

URUGUAY. **Ley nº 16.137/1990. Aprobación de la Convención sobre los derechos del niño.** 09 Nov. 1990. IMPO. Available at <https://www.impo.com.uy/bases/leyes/16137-1990>. Accessed on 20 June 2024.

URUGUAY. **Ley nº 17.815. Violencia Sexual Contra Niños, Adolescentes O Incapaces.** 14 Sep. 2004. IMPO. Available at <https://www.impo.com.uy/bases/leyes/17815-2004>. Accessed on 25 Mar. 2024.

URUGUAY. **Ley nº 18.331. Ley De Proteccion De Datos Personales.** 18 Aug. 2008. IMPO. Available

at <https://www.impo.com.uy/bases/leyes/18331-2008>. Accessed on 25 Mar. 2024.

URUGUAY. **Ley n° 19.580. Ley De Violencia Hacia Las Mujeres Basada En Genero. Modificacion A Disposiciones Del Codigo Civil Y Codigo Penal. Derogacion De Los Arts. 24 A 29 De La Ley 17.514.** 09 Jan. 2018. IMPO. Available at <https://www.impo.com.uy/bases/leyes/19580-2017>. Accessed on 25 Mar. 2024.

URUGUAI. IMPO – National Directorate of Official Printings and Publications. **Normativa y Avisos Legales del Uruguay.** Available at <https://www.impo.com.uy/cgi-bin/bases/consultaBasesBS.cgi?tipoServicio=3>. Accessed on 25 Mar. 2024.

VALENÇA, Lucas. Carlos Bolsonaro intervém em compra de aparelho espião e cria crise militar. **UOL Notícias**, 19 May. 2021. Available at <https://noticias.uol.com.br/politica/ultimas-noticias/2021/05/19/briga-entre-militares-e-carlos-bolsonaro-racha-orgaos-de-inteligencia.htm>. Accessed on 01 Dec. 2022.

VENEZUELA, Bolivarian Republic of. National Assembly. **Constitución de la República Bolivariana de Venezuela de 1999. Con la Enmienda N° 1, sancionada por la Asamblea Nacional el 14/1/2009, aprobada por el Pueblo Soberano en Referéndum Constitucional el 15/2/2009 y promulgada por el Presidente de la República Bolivariana de Venezuela, Hugo Chávez Frías, el 19 de febrero de 2009.** Available at https://siteal.iiep.unesco.org/sites/default/files/sit_accion_files/constitucion_de_la_republica_bolivariana_de_venezuela.pdf. Accessed on 17 Jun. 2024.

VENEZUELA, Bolivarian Republic of. **Ley Constitucional Contra El Odio, Por La Convivencia Pacífica Y La Tolerancia.** Gaceta Oficial Número 438,638. 10 nov. 2017. SITEAL – Educational Trends Information System in Latin America. Available at <https://www.asambleanacional.gob.ve/storage/documentos/leyes/ley-constitucional-contra-el-odio-por-la-convivencia-pacifica-y-la-tolerancia-20220215163238.pdf>. Accessed on 17 Jun. 2024.

VENEZUELA, Bolivarian Republic of. **Ley Especial contra Los Delitos Informáticos.** Gaceta Oficial Número 37,313. 30 Oct. 2001. Available at <https://www.asambleanacional.gob.ve/leyes/sancionadas/ley-especial-contra-los-delitos-informaticos>. Accessed on 25 Mar. 2024.

VENEZUELA, Bolivarian Republic of. **Ley para la Prevención y Erradicación del Abuso Sexual Contra Niñas, Niños y Adolescentes.** Gaceta Oficial Número 6,655. 7 Oct. 2021. Available at <https://www.asambleanacional.gob.ve/leyes/sancionadas/ley-para-la-prevencion-y-erradicacion-del-abuso-sexual-contra-ninas-ninos-y-adolescentes>. Accessed on 25 Mar. 2024.

VENEZUELA, Bolivarian Republic of. **Ley para Protección de Niños, Niñas y Adolescentes en Sala de Uso de Internet, Video Juegos y otros Multimedia.** Gaceta Oficial Número 38,529. 25 Sep. 2006. National Assembly. Available at <https://www.asambleanacional.gob.ve/leyes/sancionadas/ley-para-proteccion-de-ninos-ninas-y-adolescentes-en-sala-de-uso-de-Internet-video-juegos-y-otros-multimedia>. Accessed on 25 Mar. 2024.

VENEZUELA, Bolivarian Republic of. **Ley nº 1/1990. Ley aprobatoria de la Convención Sobre los Derechos del Niño. 23 Ago. 1990.** SITEAL – Educational Trends Information System in Latin America. Available at <https://siteal.iiep.unesco.org/bdnp/873/ley-11990-ley-aprobatoria-convencion-derechos-nino>. Accessed on 20 Jun. 2024.

VENEZUELA, Bolivarian Republic of. **LLey nº 5859/2007. Ley Orgánica para la Protección de Niños, Niñas y Adolescentes.** 10 Dec. 2007. SITEAL – Educational Trends Information System in Latin America. Available at <https://siteal.iiep.unesco.org/pt/bdnp/582/ley-58592007-ley-organica-proteccion-ninos-ninas-adolescentes>. Accessed on 25 Mar. 2024.

VENEZUELA, Bolivarian Republic of. National Assembly. **Leyes Vigentes.** Available at <https://www.asambleanacional.gob.ve/leyes/vigentes>. Accessed on 25 Mar. 2024.

XAVIER, Luiz Gustavo; SILVEIRA, Wilson. Lira cria grupo de trabalho para análise de projeto que trata das redes sociais. **Agência Câmara de Notícias**, 05 Jun. 2024. Available at <https://www.camara.leg.br/noticias/1069265-lira-cria-grupo-de-trabalho-para-analise-de-projeto-que-trata-das-redes-sociais/>. Accessed on 20 Jun. 2024.

6. Appendix 1 - interview script

- Introduction of the interviewer:
- IRIS – Institute for Research on Internet and Society: independent and interdisciplinary research center dedicated to strengthening human rights in the digital world. We carry out research, advocacy on public policies and scientific dissemination.
- Name, role, team “Private Communications, Investigations and Rights”.
- Project “INFORMATION SECURITY AND PROTECTION OF CHILDREN AND ADOLESCENTS: DISCOURSES AND REGULATORY PROPOSALS IN SOUTH AMERICA”: understanding the regulatory and technological landscape related to combating violence against children and adolescents in online environments with encryption in the context of Mercosur.”
- Stage: interview to collect input regarding the context of each country (Argentina, Brazil, Paraguay, Uruguay, Venezuela)
- Introduction of the person interviewed (normally this first question is to make the person feel more comfortable)
- Institution, Country
- Name, Function
- Age, Race, Gender
- Personal trajectory in the professional field
- Is there a debate in your country about the protection of children and adolescents in digital environments?
- Is it legislative, executive, judicial, technological, or academic?
- Does it specifically involve encryption technologies?
- Has there recently been any controversy or a socially sensitive case involving children and adolescents and the use of technology, or regarding the use or plans for adopting any research technology by security forces?”
- Is there any legal norm (constitutional provision, ordinary law, decree, court decision, etc.) in force or under discussion that relates to the theme of information security

involving the rights of children and adolescents?”

- Could you also indicate some public positions from civil society, institutional documents or academic studies that debate the topic?
- Could you indicate any technological solution adopted in your country that relates to this topic?
- What would be the risks or problems, in your view, related to information security involving the rights of children and adolescents?
- What possible normative and technological pathways could enhance the protection of children and adolescents in digital environments with encryption?
- What is your position, or that of your institution, on the formation, creation or establishment of legislation that protects children and adolescents in digital environments, prioritizing end-to-end encryption?
- Who are the other key stakeholders in your country that we should engage with regarding information security and the rights of children and adolescents in encrypted digital environments?
- Civil Society Organizations, national or international?
- Research institutes or individual academics?
- Members of public security?
- Public institutions in general?
- National or international companies?

7. Appendix 2 - Atlas.ti Analysis Codes

- 1.1 There are interdisciplinary debates.
- 1.2 There are partial debates. Crypto.
- 1.3 There are partial debates. CA
- 1.4 There are no debates
- 1.5 Could not provide an opinion
- 2. Notable cases (CA or CRYPTO or Interdisciplinary)
- 3.1 There is an interdisciplinary legal norm.
- 3.2 There is a partial legal norm. Crypto.
- 3.3 There is a partial legal norm. CA
- 3.4 There is no legal norm
- 3.5 Could not provide an opinion
- 4.1 Civil Society Documents
- 4.2 Public Power Documents
- 4.3 Private Sector Documents
- 4.4 Academic Documentation
- 5.1 There is an implemented technological solution (CA or CRYPTO or Interdisciplinary)
- 5.2 There is a proposed technological solution (CA or CRYPTO or Interdisciplinary)
- 6.1 Institution's position pro-cryptography
- 6.2 Institution's position on harmonization
- 6.3 Institution's position pro-child
- 6.4 No Position
- 7. Identified risks (CA or CRYPTO or Interdisciplinary)

iris

INSTITUTE
FOR RESEARCH
ON INTERNET
AND SOCIETY