Safeguarding *Children and Adolescents* from Online Radicalisation

Submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS)

Inquiry into the Nature and Drivers of Radicalisation in Australia

BRAZILIAN PERSPECTIVES ON PARENTAL SUPERVISION, PLATFORM SAFEGUARDS, AND DIGITAL PROTECTION



Prepared by **Legal Wings Institute**

Bernardo Fico • *Thiago Poloni*

Legal Wings *institute*

About Legal Wings Institute

Legal Wings Institute is a Brazil-based research and advocacy organization dedicated to the legal, regulatory, and institutional challenges raised by emerging technologies and the digital economy. Its work focuses particularly on the governance of artificial intelligence, data protection, platform regulation, digital rights, competition in digital markets, and the broader relationship between technological innovation and fundamental rights.

The Institute develops applied legal research, policy analysis, and strategic contributions to public and regulatory debates, with particular attention to the Brazilian and Global South perspectives. Its activities include the production of reports, studies, and recommendations, as well as engagement with academics, civil society, regulators, and market actors on questions involving responsible innovation, democratic governance, inclusion, and accountability in digital environments.

Legal Wings Institute seeks to contribute to the development of legal and policy frameworks that are both innovation-oriented and rights-respecting, helping ensure that technological progress is aligned with public interest, legal certainty, and the protection of vulnerable groups.

I. Justification of the submission and relevance of the Brazilian experience

The Legal Wings Institute respectfully submits this contribution to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in response to its inquiry into the nature and drivers of radicalisation in Australia.

In Brazil, the protection of children and adolescents in digital environments has been addressed through legislation on digital services and research on parental supervision. Law No. 15,211 of 17 September 2025, known as the Digital Statute for Children and Adolescents (ECA Digital), provides a relevant example of safeguards for young users and the responsibilities of digital services, while the Legal Wings Institute's research examines the role of parental supervision in children's online safety.

The inquiry's express consideration of technology, encrypted communications, algorithms and the radicalisation and grooming of minors underscores the relevance of Brazil's experience to the Committee's assessment. Children and adolescents warrant particular attention because their age and evolving capacities may heighten their vulnerability to grooming, manipulation and recruitment in digital environments. Accordingly, this contribution aims to shed light on how preventive safeguards and platform responsibilities developed in Brazil may help address these risks.

Therefore, this contribution draws on Brazilian legislation and the Legal Wings Institute's research to identify preventive mechanisms relevant to the Committee's assessment, particularly age-appropriate safeguards, parental supervision and platform responsibilities. It presents Brazil's experience as a practical comparative reference for considering how such measures may reduce young people's exposure to harmful content, unwanted contact and recruitment, while preserving the security of encrypted communications.

II. Scope of the contribution

This contribution focuses on the protection of children and adolescents from radicalisation and recruitment on social media. It examines preventive measures that platforms may adopt and considers how those measures relate to encrypted services.

Section III defines radicalisation and discusses a Brazilian government report describing how online communities may contribute to the co-option and mobilisation of adolescents.

Section IV discusses Brazil's experience, including the ECA Digital and the Legal Wings Institute's research on parental supervision. It considers how age-appropriate parental supervision, controls on recommendations and user contact, and reporting tools may help protect young users.

Section V considers how these measures relate to encrypted services. It examines section 8 of the Online Safety (Basic Online Safety Expectations) Determination 2022 and the safeguards it provides, without assuming that the PJCIS inquiry is calling for encryption to be weakened.

III. Radicalisation of Children and Adolescents on Social Media

Radicalisation, as a social phenomenon, may be understood as the process through which a person comes to regard the use of violence or terrorism as necessary and morally justified to achieve a political or ideological end. The Council of Europe's Recommendation CM/Rec(2021)7 adopts this definition for radicalisation for the purposes of terrorism. On that basis, the process can be distinguished from mere exposure to extremist content or the isolated expression of radical views.[1]

In Brazil, the report of the Ministry of Education's Working Group of Experts on Violence in Schools describes dynamics that help illustrate how digital interactions may contribute to the co-option and mobilisation of adolescents. The report examines online communities in which content circulated that glorified perpetrators of mass killings, spread hate speech and encouraged further attacks. The strategies identified include the use of violent humour, aesthetics and language, with misogynistic, sexist and racist references.[2]

The same Brazilian report also records the use of social media, messaging applications, forums and gaming chats to circulate this material and form communities, as well as cases involving the organisation of attacks. These examples do not establish that exposure to extremist content causes radicalisation, but illustrate how digital interactions may form part of broader processes of co-option and mobilisation. This distinction is relevant to the next section, which examines the responsibilities of platforms in addressing those risks.

IV. Protection of Minors and Platform Responsibilities

Radicalisation of children and adolescents may involve social factors, ties formed in online communities and direct contact that, in certain circumstances, may facilitate engagement and recruitment. This understanding informs an approach to digital

[1] Council of Europe, Committee of Ministers, 'Recommendation CM/Rec(2021)7 on measures aimed at protecting children against radicalisation for the purpose of terrorism', CM/Rec(2021)7 (20 October 2021) https://rm.coe.int/0900001680a43979 accessed 26 October 2026, 3.

[2] Brazil, Ministry of Education, Working Group of Experts on Violence in Schools, 'Ataques às escolas no Brasil: análise do fenômeno e recomendações para a ação governamental' (2023) 10, 51–52, 63–68 https://www.gov.br/mec/pt-br/acesso-a-informacao/participacao-social/grupos-de-trabalho/prevencao-e-enfrentamento-da-violencia-nas-escolas/resultados/relatorio-ataque-escolas-brasil.pdf accessed 26 October 2026.

protection that considers not only the content accessed, but also the interactions enabled by services and the design choices that shape users' experiences.

This approach highlights the need for rules that impose duties on digital services and provide families with appropriate tools to protect children and adolescents. Protection should not be assigned solely to families or service operators, since it requires a coordinated framework with complementary responsibilities for providers, families and the State. In Brazil, Law No. 15,211 of 17 September 2025, which established the *Estatuto Digital da Criança e do Adolescente*, known as the ECA Digital, offers an example of this structured protection within the digital environment; as opposed to protection *from* the digital environment. The law combines duties for providers with parental supervision tools and supports the full protection of children and adolescents as they participate in the digital environment, in accordance with their best interests, privacy and progressive autonomy, without excluding them from technology.[3]

This protection requires recognising that digital risks arise not only from the content accessed, but also from the features that organise its circulation and interactions between users. Recommendation systems and engagement mechanisms may influence which narratives reach young people and how often, while communication and group-forming features may facilitate contact and ties with people who promote violence. Design may increase or reduce opportunities for exposure, initial contact and recruitment, and should therefore be part of the analysis of preventive measures.[4]

In addition to imposing obligations on providers, the ECA Digital provides parental supervision tools that support families while respecting the best interests, privacy and progressive autonomy of children and adolescents. The law seeks to protect them as they participate in the digital environment, without excluding them from technologies that can contribute to education, socialisation, civic participation and personality development.

These mechanisms can support families in monitoring potentially harmful contacts and interactions and, in the context examined here, reduce opportunities for initial contact, persuasion and recruitment that may form part of radicalisation pathways. Precisely because protection is understood to depend on shared responsibility among the State, families and technology companies, families should not be left to manage, on their own, risks that also arise from service design.

This framework is particularly relevant when risks involve communication with third parties. In previous work on good practices for parental supervision under the ECA

[3] Brazil, Lei nº 15.211, de 17 de setembro de 2025 (Estatuto Digital da Criança e do Adolescente) https://planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm accessed 27 October 2026.

[4] Home Affairs Committee, *Combatting New Forms of Extremism* (HC 2024–26, 903) paras 33–39 https://publications.parliament.uk/pa/cm5901/cmselect/cmhaff/903/report.html accessed 27 October 2026.

Digital, the Legal Wings Institute discussed how direct contact may expose children and adolescents to intimidation, harassment, grooming and enticement, beginning with an individual approach and progressing through the development of a relationship of trust.[5]

That work brought together practices that may reduce opportunities for such approaches. These include: (i) restricting messages from adults who have not been authorised to contact the adolescent, (ii) allowing adolescents and their guardians to decide who may initiate contact, (iii) identifying suspicious patterns and sending alerts about attempts to interact, (iv) providing reporting channels, (v) creating environments limited to approved contacts, controlled groups and moderated spaces, and (vi) supporting family supervision with information about new contacts and the frequency of interactions, without disclosing the content of conversations, while also enabling parents and guardians to review safety settings and discuss risks with young people.

Given the risk that repeated conversations may spread extremist narratives, strengthen ties with communities and normalise violence, prevention depends on coordinated action by platforms and families. Platforms can provide effective supervision tools, such as information about new contacts, the frequency and timing of interactions, and alerts about suspicious attempts to make contact. Parents and guardians can use these tools to adjust permissions and talk with young people, taking their age and circumstances into account. This makes it possible to respond to concerning situations without requiring access to the content of conversations or constant monitoring, thereby protecting children's and adolescents' privacy.

In summary, Brazil's experience with the ECA Digital indicates that these risks can be addressed preventively through restrictions on unauthorised contact and supervision tools that allow parents to monitor interactions and decide how to respond. Although these measures cannot eliminate every pathway to radicalisation, they show that opportunities for harmful contact can be reduced without accessing the content of conversations. This leads to the discussion of encryption.

V. Safety Measures for Encrypted Services

Finally, protecting children and adolescents from unwanted approaches and recruitment does not necessarily depend on reading private communications. End-to-end encryption limits a provider's access to message content, but it does not prevent the service from taking measures concerning who may initiate contact with a minor, how users reach groups and communities, which content is recommended, or how an attempted approach may be blocked or reported.

[5] Ana Laura Azevedo and others, 'Supervisão Parental no ECA Digital' (Legal Wings Institute 2026) https://legalwings.com.br/wp-content/uploads/2026/08/SupervisaoParental-no-ECA-Digital_final_publicado.pdf accessed 27 October 2026.

In this respect, encryption protects information from unauthorised access. With end-to-end encryption, content is encrypted on the sender's device and can be read only on the devices of the participants in the conversation. As the eSafety Commissioner explains, this architecture makes the centralised detection of harmful content more difficult, but services can adopt appropriate responses in parts of their operations that are not encrypted and in relation to information users choose to report. Possible measures include examining elements not protected by end-to-end encryption, such as group names and the content of reports, and assessing interaction signals or metadata, such as patterns of joining groups and contacts with young users, in each case having regard to the service's architecture and privacy safeguards.[6]

These measures can be combined with controls that operate before or during an interaction. A service may restrict messages from unauthorised users to minors' accounts, enable blocking and reporting, limit invitations to private groups, and review recommendations that direct children and adolescents to risky content or communities. When a report is made, the platform can examine the specific content submitted by the user and, on that basis, consider action concerning the relevant account or group, without obtaining general access to other conversations.

It is in this combination that section 8 of the Online Safety (Basic Online Safety Expectations) Determination 2022[7] provides a useful benchmark. It requires services using encryption to take reasonable steps to develop and implement processes to detect and address unlawful or harmful material or activity, while clarifying that this expectation does not require providers to implement or build a systemic weakness or systemic vulnerability into a form of encrypted service, build a new decryption capability in relation to encrypted services, or render methods of encryption less effective. The provision therefore directs prevention towards each service's architecture and features, without making general access to messages a condition for action. The eSafety guidance develops this approach by presenting alternatives for encrypted services and recommending a proportionate combination of measures.

As discussed above, prevention can address the conditions of contact and interaction offered by services without relying on general access to the content of conversations. The ECA Digital gives effect to this approach by requiring providers to adopt technical measures that enable families and guardians to prevent misuse (Article 5, paragraph 1). It also provides that the default settings of parental supervision tools must prevent unauthorised users from communicating with children and adolescents (Article 17, paragraph 4, item I). The law further provides for controls on personalised recommendation systems, including the option to disable them (Article 17, paragraph 4,

[6] eSafety Commissioner, 'Basic Online Safety Expectations Regulatory Guidance' (February 2026) 40–41 https://www.esafety.gov.au/sites/default/files/2026-02/Basic-Online-Safety-Expectations-regulatory-guidance-February-2026.pdf accessed 27 October 2026.

[7] *Online Safety (Basic Online Safety Expectations) Determination 2022* (Cth) s 8.

item V), and allows guardians to identify the profiles of adults with whom a child or adolescent communicates (Article 18, item III).

By focusing these safeguards on contact permissions, recommendation mechanisms and the identification of interlocutors, the legislation provides concrete means of reducing opportunities for initial contact and recruitment. It enables services to limit approaches by unauthorised users, reduce repeated exposure to risky content or communities, and give guardians information to recognise potentially concerning interactions, without presuming ongoing access to the content of conversations.

Brazil's contribution to this debate is to show how protective duties can be implemented through service design and family tools addressing concrete risks. The law requires providers to adopt technical measures that enable families to prevent misuse and to make parental supervision tools available. At the same time, it prohibits regulations from imposing, authorising or resulting in mass, general or indiscriminate surveillance (Article 37, sole paragraph).

Accordingly, protecting children and adolescents from approaches and recruitment into radicalisation does not require, as a general response, undermining or reducing the effectiveness of encryption. Brazil's experience shows that risks can be addressed preventively through contact controls, reporting tools, assessment of service features and age-appropriate parental supervision. Section 8 of the Online Safety (Basic Online Safety Expectations) Determination 2022 likewise requires providers of encrypted services to take reasonable steps to detect and address unlawful or harmful material or activity, while providing that those steps need not involve implementing or building a systemic weakness or systemic vulnerability into the service, building a new decryption capability, or rendering encryption methods less effective. Together, these frameworks support an approach that protects minors without making general inspection of communications a condition of safety.

Conclusion

Australia's online safety framework already sets expectations for providers, including consideration of the best interests of children and adolescents in the design and operation of services and the adoption of safety measures compatible with features such as encryption. In this context, one possible regulatory approach would be to consider developing safeguards specifically for this group, including parental supervision. The ECA Digital could inform that discussion by providing parameters for measures such as restricting unauthorised contact, controlling recommendations and offering monitoring tools appropriate to each child's or adolescent's age and stage of development.

When proportionate and integrated with the responsibilities of services, families and the State, measures of this kind may reduce opportunities for unwanted approaches

and recruitment by addressing the conditions of contact and exposure. Their implementation does not require generalised access to private communications and should preserve limits on mass, general or indiscriminate surveillance. Safeguards informed by this experience could therefore help give effect to preventive measures within Australia's framework without making the weakening of encryption a condition for protecting children and adolescents.

References

Australia, *Online Safety (Basic Online Safety Expectations) Determination 2022* (Cth) https://www.legislation.gov.au/F2022L00062/latest/text accessed 27 October 2026.

Azevedo AL and others, 'Supervisão Parental no ECA Digital' (Legal Wings Institute 2026) https://legalwings.com.br/wp-content/uploads/2026/08/SupervisaoParental-no-ECA-Digital_final_publicado.pdf accessed 27 October 2026.

Brazil, Lei nº 15.211, de 17 de setembro de 2025 (Estatuto Digital da Criança e do Adolescente) https://planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm accessed 27 October 2026.

Brazil, Ministry of Education, Working Group of Experts on Violence in Schools, 'Ataques às Escolas no Brasil: Análise do Fenômeno e Recomendações para a Ação Governamental' (2023) https://www.gov.br/mec/pt-br/acesso-a-informacao/participacao-social/grupos-de-trabalho/prevencao-e-enfrentamento-da-violencia-nas-escolas/resultados/relatorio-ataque-escolas-brasil.pdf accessed 26 October 2026.

Council of Europe, Committee of Ministers, 'Recommendation CM/Rec(2021)7 on measures aimed at protecting children against radicalisation for the purpose of terrorism' (CM/Rec(2021)7, 20 October 2021) https://rm.coe.int/0900001680a43979 accessed 26 October 2026.

eSafety Commissioner, 'Basic Online Safety Expectations Regulatory Guidance' (February 2026) https://www.esafety.gov.au/sites/default/files/2026-02/Basic-Online-Safety-Expectations-regulatory-guidance-February-2026.pdf accessed 27 October 2026.

Home Affairs Committee, *Combatting New Forms of Extremism* (HC 2024–26, 903) https://publications.parliament.uk/pa/cm5901/cmselect/cmhaff/903/report.html accessed 27 October 2026.