"It Takes a Village to Raise a Child" - Who and What to Consider in Designing Parental Mediation Features?

George Valença[1], João Victor Assis[1], Maria Góes de Mello[2]

[1]Departamento de Computação – Universidade Federal Rural de Pernambuco (UFRPE)
Recife – PE – Brasil

[2]Instituto Alana
São Paulo – SP – Brasil

{george.valenca,joao.ctassis}@ufrpe.br, maria.mello@alana.org.br

Abstract. Introduction: *The pandemic intensified children's use of connected devices, especially social media apps. The 2024 TIC Kids survey shows that over 60% of children aged 9–12 have profiles on these platforms (despite being under the minimum age of 13). This exposes them to risks like privacy loss, inappropriate content, and commercial exploitation.* ***Objective:*** *We aim to understand the main recommendations to design parental mediation and control features arising from the public consultation on platform regulation by CGI.br.* ***Methodology or Steps****: We analyzed the contributions on parental mediation regulations through thematic synthesis.* ***Results:*** *Based on this, we derived early requirements and evaluated TikTok and Instagram on these requirements.*
Keywords *Parental Control, Child Protection, Design, Requirements.*

1. Introduction

Changes in daily habits brought on by the pandemic accelerated the integration of smartphones and other connected devices into the culture of children. Whether chatting with friends, completing school assignments, or simply seeking entertainment through games and vlogs, this group have become increasingly immersed in digital environments. In Brazil, children are being introduced to digital technologies at ever younger ages: those who accessed the internet for the first time at age six rose by 10.5% between 2018 and 2022. According to the 2024 TIC Kids Online survey, 60% of children aged 9–10 already have social media profiles and use YouTube several times a day. Overall, 83% of those aged 9–17 maintain some type of online profile [NIC.BR 2024].

The same study showed that 76% of children and adolescents access social networks and messaging apps, and 72% say they are allowed to use these platforms when alone—indicating a degree of autonomy in app usage. However, only 46% reported knowing how to adjust their privacy settings. This takes place in a global context where children make up one-third of all internet users [Winther et al. 2019], highlighting their importance to technology companies—on whose platforms 62% of Brazilian children have already searched for products to buy [NIC.BR 2024].

In these environments, ensuring children's well-being involves preventing the misuse of their data and safeguarding them from online risks. This is the premise behind the growing design of mediation, supervision, and parental control features in the most popular apps among youth. The three main social media platforms used by Brazilian

children in this age group (TikTok, Instagram, and Facebook) each offer their own tools for parental mediation. These features aim to mitigate issues flagged by the Brazilian Society of Pediatrics (SBP), which warns that early and excessive exposure to digital devices can lead to social and behavioral issues, sleep and eating problems, increased anxiety, and exposure to age-inappropriate content [Domingos 2017]. News reports even indicate that former employees of major tech companies express concern about the safety of their own children on social media [Silva 2023].

Despite Instagram and TikTok setting 13 as the minimum age for account creation, age verification mechanisms remain weak. As a result, children under that age are often able to access these platforms without appropriate safety measures or age-based customizations [Pasquale et al. 2020]. In parallel, many parents are unaware of the technological tools available within these apps, which hinders their ability to guide or properly configure settings (something that digital literacy could help address, especially when it comes to preventing exposure to harmful content [Geržičáková et al. 2023]).

According to TIC Kids 2024, only (i) 32% of parents use tools to limit who their child can contact through messaging; (ii) 28% use ad-blocking tools; (iii) 26% use alerts when a child attempts to make purchases; and (iv) 24% use tools to limit time spent on apps [NIC.BR 2024]. In parallel, less than 10% of teenagers on Instagram have activated the parental supervision feature, and the parental controls on TikTok are also underused [Ghedin 2024]. This low usage is largely due to a lack of awareness or difficulty navigating these tools. For example, some parents report that Roblox's parental control settings are overly complex and hard to use, limiting their effectiveness [dos Santos Madeira et al. 2023]. This scenario highlights the growing importance of parental mediation tools, as reinforced by various laws and regulations. For instance, Brazil's General Data Protection Law (LGPD – Law No. 13.709/2018) regulates the processing of children's personal data, requiring parental consent for those under 13 and mandating that data be processed in the child's best interest.

In this study, motivated by the context described, we aim to understand the main recommendations to design parental mediation and control features arising from the public consultation on platform regulation conducted by The Brazilian Internet Steering Committee (CGI.br). By using Thematic Synthesis to analyze this dataset, we identified five key dimensions to guide IT companies (particularly, Big Techs) in creating these features, such as *Time Limitation*, *Age Rating and Content Management* and *Age Verification*. Finally, we outline early requirements for designing parental mediation features, which are used to analyse the parental mediation features designed by Instagram and TikTok. Our main goal is reinforcing both the duty of care that should be assumed by Big Tech companies and the growing expectation for stronger protections for children and adolescents online (from both a technological and legal standpoint).

2. Conceptual Background

The Brazilian Statute of the Child and Adolescent defines children as individuals up to 12 years of age and adolescents as those aged 12 to 18 [Castro e Macedo 2019]. However, in the international context, the United Nations Convention on the Rights of the Child (CRC) defines a child as any person under the age of 18 [United Nations 1989]. To allow for broader generalization, we adopt the CRC's broader definition.

The limitations of age verification mechanisms on digital platforms, which is part of the broader framework of parental mediation and protection tools, have been clearly demonstrated in previous studies [Pasquale et al. 2020]. Their work highlights the top 10 social platforms used by children, including YouTube Kids and TikTok. On some of these platforms, users are not even required to provide their age when registering or creating a profile. In Brazil, TikTok allows access to its content feed without registration and has been the subject of investigation by the National Data Protection Authority (ANPD). Besides, few child-specific versions of popular apps exist for those under 13 years old (YouTube Kids being a rare exception). Hence, many children end up using standard versions of apps, which often expose them to inappropriate, adult-oriented content.

Within this context, parental control or mediation tools refer to technological features built into platforms (such as modules within TikTok, for instance) or available as standalone applications. These tools are designed to allow both parents and children to monitor and manage app usage [Nouwen et al. 2017]. Examples of such functionalities include: limiting screen time; blocking inappropriate content; restricting activities (e.g., in-app purchases such as buying items in games); preventing interactions with unknown users (those outside a friends or followers list); and managing online activities, including browsing history [Zaman et al. 2016].

It is worth noting that there is a growing preference for the term *parental mediation* over *parental control*, due to the latter's potentially negative and interventionist connotations. Designing platform features around the notion of control may suggest a reduction in children's autonomy and decision-making capabilities. This framing, even in communications about the tools, can discourage teenagers from engaging with them. In contrast, parental mediation emphasizes open dialogue between caregivers and children about technology use, supporting the gradual development of digital autonomy. These interactions—while not sufficient in isolation—can lead to family agreements that foster digital literacy, reduce risks, and encourage self-regulation. This includes impulse control and the development of strategies for navigating online risks [Wisniewski et al. 2017].

From a regulatory view, the Brazilian Civil Rights Framework for the Internet (Federal Law n. 12.965/2014) outlines ethical principles and guarantees for a democratic and safe digital environment, including privacy and data protection. Brazilian law also prohibits advertising targeted at children[1] and prioritizes child rights protections by families, the State, and society at large[2]. The UN General Comment No. 25 emphasizes that digital leisure time can expose children to risks like deceptive advertising and manipulative design resembling gambling (practices that states must require companies to avoid[3]). Internationally, the Children's Online Privacy Protection Act (COPPA) in the U.S. regulates the collection and use of data for children under 13. The General Data Protection Regulation (GDPR) in Europe recognizes children as a vulnerable group, requiring special safeguards for processing their personal information, particularly for those under 16. Both frameworks restrict data processing without parental consent.

[1]Federal Law No. 8.078. provides for consumer protection and other measures (1990) - available at http://tinyurl.com/46zs5r8z

[2]Constitution of the Federative Republic of Brazil (1988) - available at http://tinyurl.com/2ktersxk

[3]United Nation's General comment No. 25 on children's rights in relation to the digital environment (2021) - available at https://tinyurl.com/2xu6hhwh

3. Research Method

We started this research by **understanding the CGI.br data** from a public consultation conducted in 2023, which received a total of 1,336 contributions from individuals and organizations across the government, civil society, private sector, and the scientific and technological community. These inputs were used to inform the regulation of digital platforms. The results of this consultation (published in various formats, such as website, PDF, and CSV) included recurring references to terms such as *parental mediation*, *control*, and *supervision*, which translate the problem explored by this research. Hence, we performed a **mapping and labelling procedure to support the analysis**, i.e. we mapped these terms and categorized the related excerpts to build an interpretative framework around the challenges, opportunities, and solutions in this area.

By searching for these expressions in the PDF version of the report, we identified 12 text excerpts (segments of contributions) that specifically addressed the topic. These excerpts were labeled using a Thematic Analysis or Synthesis method [Cruzes e Dyba 2011], a technique that helps identify, analyze, and report patterns across data, organizing and describing it in depth. This method interprets discourse within the data, gaining strength when labels are supported by evidence from academic literature. In total, the excerpts were classified into five main themes:

- Consent and Family Guidance;
- Role of the Medical Community;
- Right to Privacy;
- Digital Literacy of Children and Guardians;
- Role of the State and Regulatory Bodies; and
- Parameters.

As we aimed at **proposing guidelines**, we further interpreted the data associated with the sixth theme (*Parameters*), which we divided into six subthemes: *Content Restriction*, *Usage Limits*, *Age Rating* and *Content Management*, *Age Verification*, *Account Pairing* and *Privacy and Security*. Finally, we derived early requirements in light of the subthemes for **inspecting a set of social media platforms**[4]. In Results sections, we interpret the contributions based on the proposed themes and present early requirements for parental mediation on platforms, which are used as lenses of analysis of the design of corresponding features on TikTok and Instagram. The phases of the investigation are shown on a timeline in Fig. 1, with activites performed in 2024 and 2025.

4. Results

The analysis of data on parental mediation submitted during the CGI.br public consultation revealed a valuable set of elements to consider when designing features for caregivers' oversight on platforms, which are described here in terms of responsibilities of multiple actors involved in this process. For example, the role of regulatory bodies to ensure the implementation of age restrictions and privacy settings to protect child users. We show these actors and related duties in Fig. 2, with details in the following sections.

[4]The full association between themes (and subthemes) and the corresponding contributions is publicly available for transparency and potential replication of the research, at the following address: `https://tinyurl.com/mr7daw8c`. It is important to note that the text excerpts were used exactly as made available by CGI.br

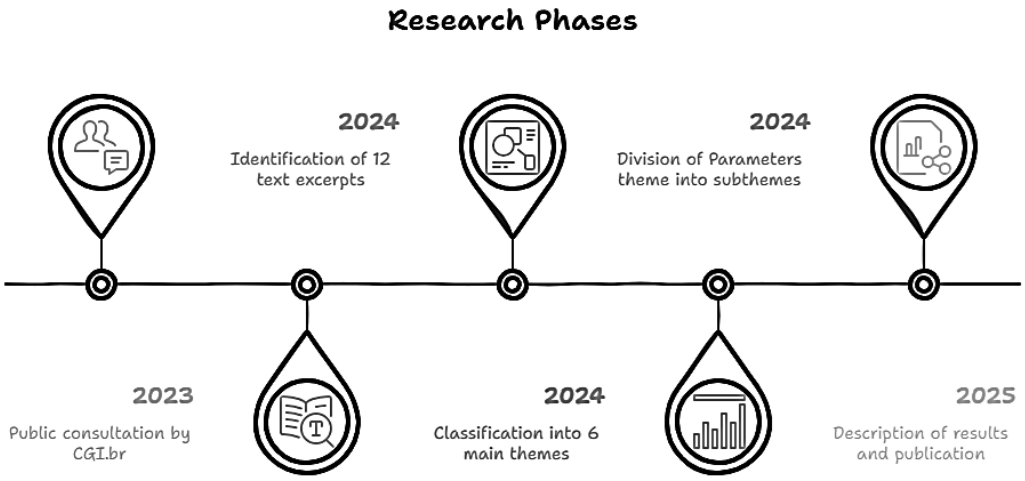

Figure 1. Research Phases.

4.1. Shared Responsibility of Governments and Platforms for Families' and Children's Digital Literacy

The mapped contributions highlighted that the Global South faces not only socioeconomic inequalities, but also disparities in internet access and, more critically, in access to adequate knowledge about the risks and opportunities children encounter on digital platforms. As mentioned in a response to the consultation, *"(children) have fewer resources available for appropriate mediation and support to benefit from digital technologies"*.. Hence, this lack of digital literacy requires an intersectional lens: just as we must address the reality of multiple childhoods, we must also reflect on multiple forms of parenting during this design process. Socially and economically vulnerable families often have fewer resources to provide adequate supervision— *"greater vulnerabilities in offline life are linked to greater vulnerabilities online"*.

In light of this, the analyzed data pointed to the importance of action by platforms (with an informative design approach instead of manipulative design practices [Albuquerque et al. 2024]) and authorities (with programs to spread main concepts related to digital literacy) to provide caregivers with the knowledge needed to understand:

1. **The risks, dangers, and harms of social media:** not only caregivers, but also educators — given their close interaction with children and their guiding role —should raise awareness about these issues.
2. **The child's right to privacy and how adult practices may infringe upon it:** *"they should also be advised on practices that can help them respect and protect children's privacy in the digital environment, while keeping them safe"*.
3. **Supporting and managing children's online access in alignment with their age and developmental stage:** as one contribution to the consultation emphasized, *"monitoring a child's digital activity by mothers, fathers, and caregivers should be proportionate and aligned with the child's evolving capacities"*.

4.2. Responsibility of Governments to Set Parameters for Parental Mediation Tools

The data also reinforced the crucial role of authorities in regulating digital environments, including the definition of **specific measures** that technology companies must implement

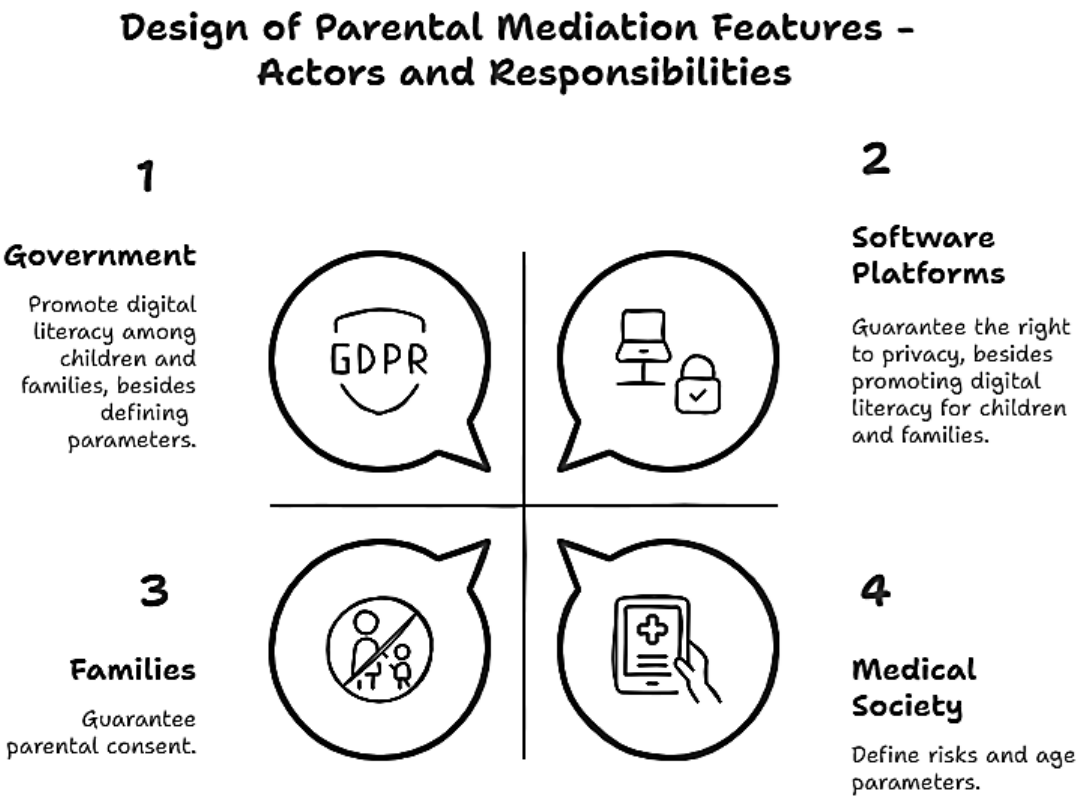

Figure 2. Actors and main duties in designing parental mediation features.

on their platforms to safeguard the interests of children. According to one of the contributions, these measures should go beyond parental mediation and include *"age restrictions, appropriate privacy policies, and digital safety education"*. In this sense, digital platforms are seen as environments where caregivers in general should be able to understand how to support children and *"manage their children's access to online networks"*. Co-designing with parents to enable friendly interfaces is the best way for them to understand the nuances of applications they may seldom or never use [Cao et al. 2024].

Therefore, for such protection to be truly effective, a triad of action is needed: legislators, caregivers, and platforms must work together, as established by Article 227 of the Brazilian Federal Constitution. These actors should join forces to ensure that children (the users most vulnerable to privacy risks, safety threats, and exposure to inappropriate content) can both protect themselves and benefit from varied digital platforms.

4.3. Responsibility of Platforms to Ensure Privacy by Design

One of the studied contributions highlighted the risk that parental intervention (or the design of features focused solely on control) could overshadow the goals of guidance and ensuring children's safety. The concern is that privacy features within parental mediation tools on platforms must not become *"tools for surveillance"* and should never be implemented without the child's awareness. This approach aims not only to preserve the child's right to privacy, but more importantly, to foster their active **participation**

in the pursuit of greater safety and well-being in digital environments. As stated in a contribution, it supports the *"progressive development of [their] capacities"* - something that can be understood as an ethical guideline for designing or evolving parental mediation tools on platforms such as games and social media.

4.4. Responsibility of Families to Guarantee Parental Consent

One of the contributions highlighted **parental consent**, a legal basis under Brazil's General Data Protection Law. The design of such specific feature (e.g. explicit, opt-in consent or opt-out), which is part of parental mediation, must also consider caregivers' limited digital literacy. The same survey reports that 27% of parents rarely feel able to teach their children how to use the internet safely. Therefore, regardless of whether parental consent is provided, children's rights and best interests must always be guaranteed with absolute priority by both digital platforms and the State. However, such contribution warned that it should not be *"the sole mechanism for ensuring children's protection in digital environments"*. The reliance on families for this protection raises two critical concerns: (i) it reflects a strategy by platforms to outsource their responsibility; (ii) in many cases, parental supervision simply does not occur. According to the 2024 TIC Kids Online survey, 19% of parents never check their child's phone activity, 28% never set usage rules, and 31% never implement screen breaks [NIC.BR 2024].

4.5. Responsibility of Medical Society to Define Risks and Propose Parameters

Another key finding in the data is the need to listen to the medical community regarding risks, particularly the **mental health harms to children and adolescents** caused by social media platforms designed to encourage compulsive and passive use [Baroni e Pereira 2024]. This includes manipulative design strategies such as attention-capturing patterns — constant notifications, short-form videos, personalized recommendations, and incentives for continuous connection [Albuquerque et al. 2024].

A further recommendation — both for family discussions and for broader societal debate (e.g., through position papers essential to regulatory processes) — concerns the **appropriate age for children** to create social media accounts. One contribution noted that *"13 years — the minimum age allowed by many platforms — is the onset of adolescence and a phase of significant development, and may not be compatible with unrestricted access to social media content"*. Hence, it is proposed that the minimum age requirement be reassessed, incorporating perspectives from health professionals. This mirrors recent steps taken by the Australian government, which now proposes raising the minimum age for creating social media profiles to 16 years [5].

5. A Proposal of Requirements for Parental Mediation

The analyzed consultation also yielded inputs that address principles and guidelines for the broad regulation of digital platforms. Our interpretation of criteria for parental mediation in platforms generated a set of early requirements (ER) for these environments, which can act as design guidelines by (i) supporting stakeholder analysis activities and (ii) clarifying the "whys" underlying future system requirements for parental mediation.

[5]Deutsche Welle. "Australia launches bill banning social media for under 16s" (2024). Available at https://tinyurl.com/55xfyppw

Such requirements can support designers in the process of empathizing with the previously mentioned actors (mainly, parents and child users) to understand their context, map additional needs and motivations as well as design alternatives and their and effects. Hence, these early requirements provide a preliminary blueprint of parental mediation domain, considering these multiple stakeholders [Horkoff e Yu 2016]. Below, we describe them in the following sections, which represent five dimensions.

In the first dimension, **Time Limitation**, we concluded that platforms should *offer mechanisms to set daily screen time limits and define usage schedules (ER1)*, such as making the app inaccessible during nighttime hours. This functionality could include default settings for adolescent accounts and features that encourage breaks from social media use, promoting disconnection and offline experiences.

The second dimension, **Age Rating and Content Management**, aims that platforms should *require age-appropriate content classification from all users who publish content (ER2)*. They must also *provide tools for age-based content restriction (ER3)*, allowing parents to supervise and restrict access to specific content via parental mediation settings. An example cited in the consultation is the parental supervision controls available via Google's Family Link. One contribution suggested that platforms could offer features that *"encourage teens to switch topics if they've been engaging with the same type of content for a prolonged period"*, promoting their well-being.

The third dimension, **Age Verification**, involves the definition of effective age controls to prevent children from creating profiles by misrepresenting their age. This means that platforms should *develop robust age verification mechanisms that work in conjunction with parental mediation features (ER4)* — without which such features lose effectiveness. In the fourth dimension, **Account Pairing Between Children and Parents**, we identified that platforms should *provide a feature that enables caregivers to link their accounts with children's profile (ER5)* for children under 16. Such mechanism allows an easy and effective supervision.

Finally, the fifth dimension, **Privacy and Security**, highlights platforms must **develop features and mechanisms that enhance user protection, in a privacy-by-design paradigm (ER6)**. The suggestions for child security from analyzed data included:

- Restricting messaging between adults and minors;
- Providing security warnings in direct messages;
- Providing tools that limit bullying or harassment-related comments and messages;
- Provide tools for monitoring online activities, including device and service tracking features - whose design should be simple and intuitive; and
- Setting adolescent and child accounts as "private by default".

Otherwise, as one contribution pointed out, *"they may prevent a child from accessing a help center or searching for sensitive information"*. A noteworthy point concerns respect for children's individuality. Another contribution also reinforced that there is a *"need for parameters and criteria for parental mediation mechanisms that respect children's privacy and the progressive development of their capacities, as well as their right to privacy"*. In Table 1, we list all the previous early requirements.

In the subsequent sections, we exemplify whether and how two highly popular platforms among children implement such guidelines: Instagram and TikTok. We selected

Table 1. Early Requirements (ER) and Guidelines per Dimension.

Dimension	Early Requirement / Design Guideline
Time Limitation	Offer mechanisms to set daily screen time limits and define usage schedules (ER1).
Age Rating and Content Management	Require age-appropriate content classification from all users who publish content (ER2). Provide tools for age-based content restriction (ER3).
Age Verification	Implement robust age verification to prevent children from misrepresenting their age (ER4).
Account Pairing	Allow caregivers to link their accounts with children's profiles for supervision (ER5).
Privacy and Security	Enhance user protection using privacy-by-design mechanisms (ER6).

them in light of the results from 2024 TIC Kids Online survey, which indicate that Instagram, Whatsapp, TikTok and Youtube are the platforms more frequently accessed by young users in Brazil [6] [NIC.BR 2024].

5.1. Instagram

Regarding **Time Limitation**, we observed that Instagram offers built-in features designed to help users manage and limit their screen time, which encourage healthier usage habits on children. These mechanisms are accessible through the app's settings and are available both for individual users and, in a more supervised format, for parents or guardians overseeing adolescent accounts. For individual users, the features can be accessed via the "Teen safety settings" section in the app (see Figure 3).

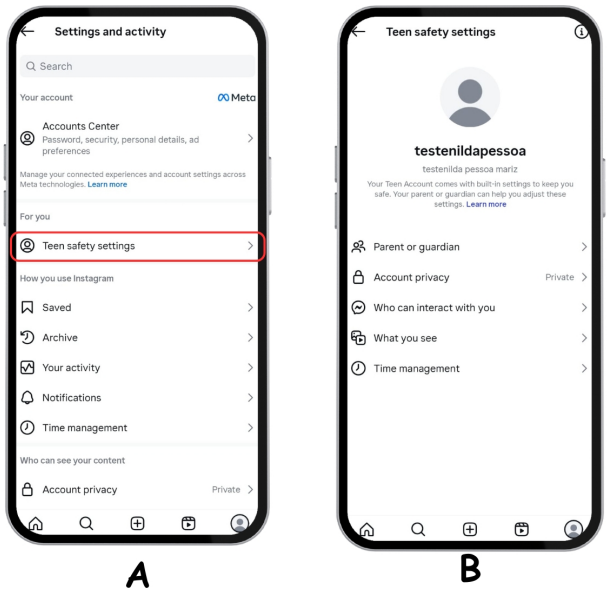

Figure 3. Instagram's Teen Safety Settings (A: Teen Safety section in the settings; B: children's view of Teen Safety settings).

[6] 2024 TIC Kids Online Survey - "Children And Adolescents, by Frequency Of Use Of Digital Platforms" https://cetic.br/pt/tics/kidsonline/2024/criancas/C7/

After tapping the profile icon and navigating through the menu, users can enter the “Time management” section, where they are able to set daily time limits ranging from 15 minutes to 2 hours (see Figure 4A). Once the user reaches this limit, Instagram sends a notification, helping to promote mindful usage (Figure 4B). Complementary to these time-related tools, Instagram allows the management of push notifications through its “Notifications” settings (see Figure 4C), enabling users to pause all notifications or customize them according to activity type.

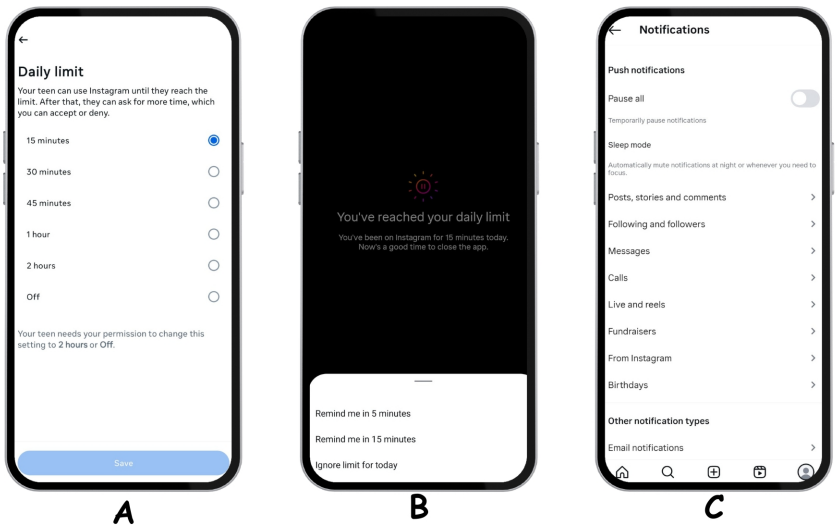

Figure 4. Time Limitations and notification screenshots in Instagram (A: daily time limits; B: shows the options for the young user when reaching daily limit; C: shows notification settings).

For the **Age Rating and Content Management** dimension, Instagram does not require manual age ratings for posts, but employs AI and human moderation to identify and remove sensitive or inappropriate content. Branded content creators must flag paid partnerships, and accounts promoting restricted products (alcohol, tobacco) can set a minimum viewing age (ER2). The “Sensitive Content Control”, illustrated in Figure 5, allows users, with more restrictive standards for those under 16 (automatically set to "Less"), to adjust the amount of sensitive content viewed and restrict recommendations in Explore, Reels, Search, hashtag pages, and comments on posts (ER3). Parents, through Parental Supervision, see sensitivity settings and can monitor the accounts their child follows, but they do not have access to age-specific filters for all content.

In the **Age Verification** dimension (ER4), Instagram establishes a minimum age of 13 for profile creation, initially based on self-declaration during registration. However, the platform uses artificial intelligence to identify age inconsistencies and has implemented more robust verification mechanisms for specific situations, such as when a user tries to change their date of birth to 18 or older, or when there is suspicion of an incorrect age. These mechanisms[7] include (i) sending an identity document, (ii) recording a video selfie to be evaluated by an age estimation technology from the platform or confirming mutual friends (the idea of “social vouching”).

[7]Instagram claims it is building technology to proactively find accounts belonging to teens, even if the account lists an adult birthday. It expects to begin testing in the US in early 2026 - `https://about.instagram.com/blog/announcements/instagram-teen-accounts`.

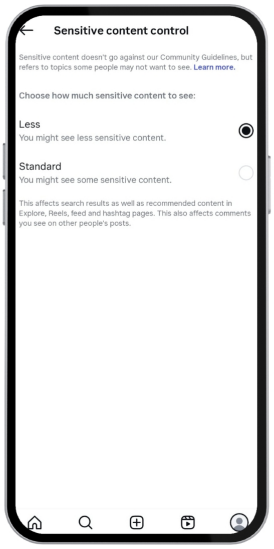

Figure 5. Age rating and content management in Instagram.

The dimension **Account Pairing** (ER5) is addressed by Instagram via its "Family Center", which provides a set of parental supervision tools, whose home screen can be seen in Figure 6A. Through this tool, parents can link their account to that of a teen (under 18), upon invitation and mutual consent. This allows parents to monitor usage and establish boundaries (See Figure 6B). Once supervision is set up, parents can configure daily screen time limits similar to the individual user options. They can also define specific "sleep mode", preventing usage during specific periods, such as school hours or bedtime (See Figure 6C). Additional features include visibility into who the child interacts with on the platform and reports on modifications made to privacy or safety settings.

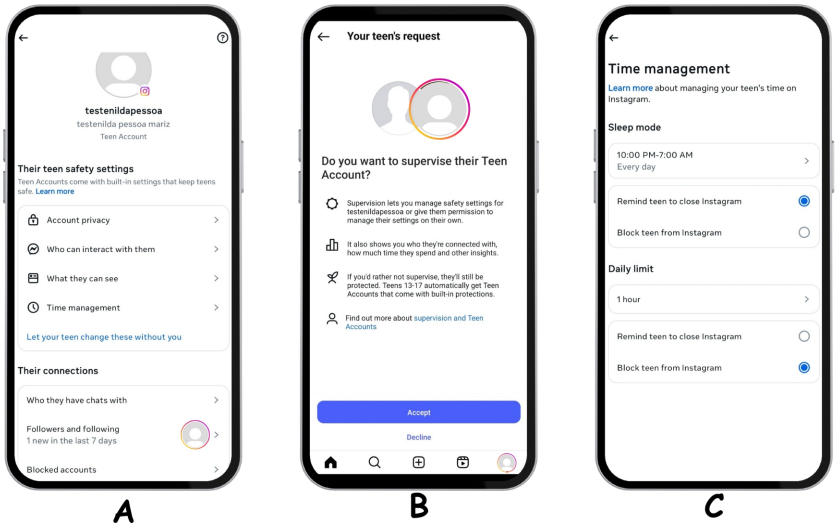

Figure 6. Account pairing on Instagram (A: parental supervision home screen; B: supervision request; C: time management in a parent profile).

Changes to settings made by teenagers require parental approval via Family Center, pairing promotes dialogue and guidance, and surveillance is not hidden, so that the teenager is informed about what his/her guardian supervises, as demonstrated in Figure 7.

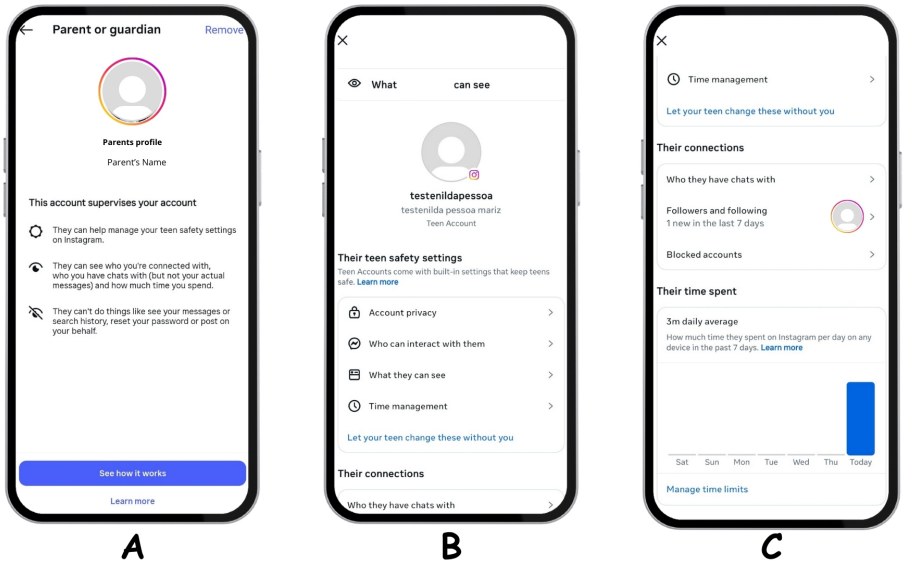

Figure 7. Teen's knowledge about what is being supervised on Instagram.

Finally, regarding **Privacy and Security** (ER6), Instagram adopts privacy-by-design in many controls. New accounts for those under 16 are set to private by default. Unknown adults cannot send DMs to teenagers; security warnings appear in suspicious interactions; "Hidden Words" and "Limits" filters mitigate bullying and spam; and there are tools for blocking and reporting content. Other features, such as two-factor authentication and security checkup, reinforce protection. However, the effectiveness depends on the reading of features and active configuration by the teenager or guardian.

Despite significant investment in protection features, challenges persist in the effectiveness of safeguarding children and adolescents on Instagram. There is no effective blocking of accounts for exceeding the daily time limit for adolescents, only notification, without automatic intervention. Active parental supervision is required for the guardian to trigger the blocking of use when the daily limit is reached, and the adolescent must request an extension of this time after reaching it. The lack of a universal requirement for content to be rated as age-appropriate by publishers (ER2) may limit the granularity of filters. Additionally, age verification, although advanced, still begins with self-declaration. The "Sensitive Content Control", although positive, works as a filter and not as an absolute block, and the overall effectiveness of all these tools remains highly dependent on awareness, configuration and active use by adolescents and their guardians.

5.2. TikTok

Regarding **Time Limitation** (ER1), TikTok presents robust mechanisms, both for the individual user and for parental control. The platform allows all users to set a daily screen time limit (e.g., 40, 60, 90, 120 minutes, or a custom time), requiring a password to continue using after this period ends. Notably, for adolescents between 13 and 17 years old, a default limit of 60 minutes per day is activated, and although it can be deactivated, a weekly summary of screen time is provided. Additionally, the platform sends "Break Reminders" and "Sleep Reminders", and provides a "Screen Time Control Panel" (Figure 8). Through the "Family Pairing" feature, guardians can also control these options, restricting the teen from getting lighter settings.

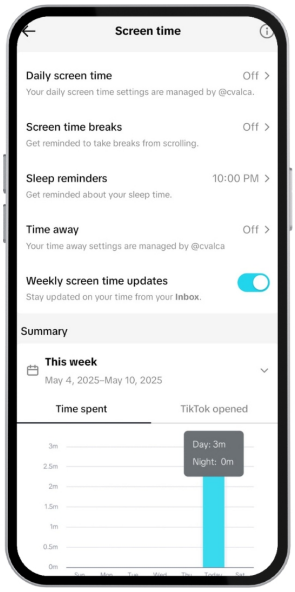

Figure 8. Teen's screen time options on TikTok.

Regarding **Age Rating and Content Management**, although it does not require each user to individually rate their videos by age when posting (ER2), Tiktok adopt a system of "Content Levels". This mechanism organizes the material based on thematic maturity, preventing videos with content aimed at older audiences from appearing in the "For You" feed for those under 18 (ER3). The "Restricted mode", manageable by parents via Family Sync and protected by a password, limits exposure to potentially inappropriate content, as demonstrated in Figure 9A. Keyword filters allow you to hide unwanted videos and comments (exemplified on Figure 9B), and Community Guidelines, supported by AI and human moderation, remove material that violates child safety and platform standards.

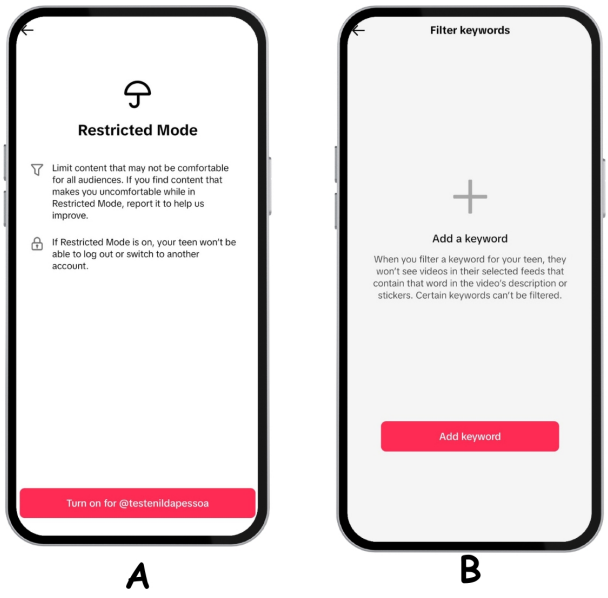

Figure 9. TikTok's content management on parent's phone (A: Teen's screen time options; B: keyword filter page).

The **Age Verification** (ER4) dimension is addressed by TikTok by requiring a minimum age of 13 to create accounts, starting with self-declaration upon registration (Figure 10). However, the platform invests in technology and moderation to identify and remove accounts suspected of belonging to users under the minimum age. To access specific features, such as live broadcasts (TikTok LIVE) or monetization features, a minimum age of 18 is required, with the option to request age verification via documents or other technologies (cf. Figure 10). In some markets, TikTok directs users identified as under 13 to a more restricted and curated experience ("TikTok U13 Experience").

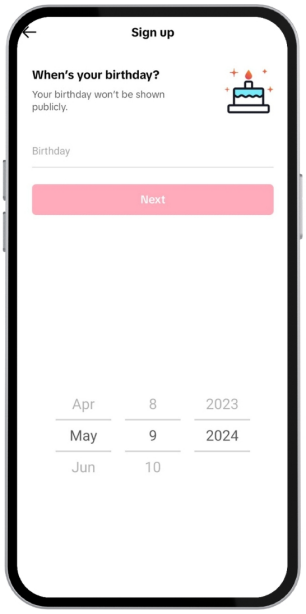

Figure 10. Teen's age self-declaration when creating an account on TikTok.

Parent-Child Account Pairing (ER5) is supported by the "Family Pairing" feature, which allows parents to link their teen's (13-17 years old) through both consent. This feature gives parents the ability to manage screen time, enable "Restricted Mode", control search permissions, set the teen's account visibility (private or public, depending on age), restrict who can send direct messages (DMs), and decide who can see videos liked by the teen. Parents can also receive a weekly summary of their child's activity. The family pairing screen with the options for parental supervision can be found in Figure 11.

Under **Privacy and Safety** (ER6), TikTok adopts a series of default settings and tools to protect young users. Accounts of users between the ages of 13 and 15 are set to private by default, with automatic restrictions on who can comment, DM, "Duet" their videos, watch teen's liked videos, and disabling downloads of their content by others, configurable aspects as seen in Figure 12.

For the 16-17 age group, similarly restrictive default settings can be relaxed by the user, but they include safety warnings on suspicious interactions and restrict, hidden Words and limits tools to combat bullying. The platform also provides safety warnings in DMs and offers multiple tools to limit bullying and harassment, such as comment filters, bulk comment management and "Comment Warnings" that encourage reconsideration of potentially offensive posts. Despite such robust features, there are some areas that require continued attention to protect children and young people on TikTok.

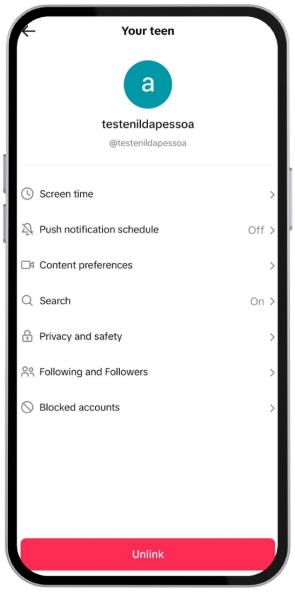

Figure 11. Family pairing connection on a parent's phone on TikTok.

Although age verification for certain features is more rigorous, initial account creation is still based on self-declaration, which can be a vulnerability. The "Content Levels" system, while a positive initiative, relies on the platform's accuracy in categorizing a massive and dynamic volume of videos, and "Restricted Mode" does not guarantee absolute blocking of all potentially inappropriate content. Also, the time-limiting tools that require a password to continue can be bypassed if the teen has access or sets the password. We also observed a lack of transparency about the content actually viewed by the teen, as only usage time data is available. Finally, there is no activity reporting in DMs, potentially hiding risky interactions.

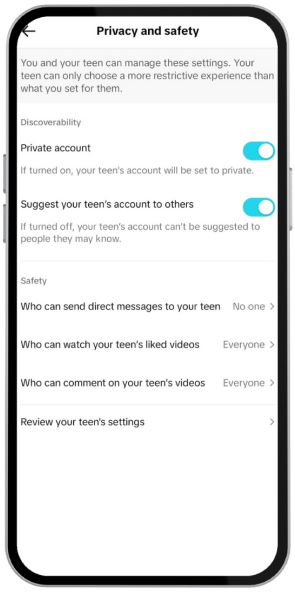

Figure 12. Privacy and safety on a parent's TikTok app.

6. Discussion and Conclusion

Our study's main **contribution** is highlighting the growing and urgent importance of safeguarding the rights, safety, and well-being of children in digital environments, especially considering their early access to technology, particularly social media platforms. The public consultation conducted by CGI.br revealed both the need for regulatory initiatives and the necessity of more effective practices by platforms, the State, and caregivers. Moreover, there is a pressing need for ongoing educational efforts to promote digital literacy among families and educators. A study by Ofcom[Ofcom 2022], the UK's independent communications regulator, which informed the development of the Online Safety Bill, analyzed the concepts of "harms", "risk factors", and "dangers" in the digital context. Clearly distinguishing between these terms is essential for designing effective protection strategies and policies. The term "danger" refers to online experiences that have the potential to cause harm—for example, exposure to violent content, harmful interactions with other users, cyberbullying, and manipulative platform design features such as infinite scroll and "like" buttons. However, the mere presence of danger does not guarantee harm. That relationship is mediated by "risk factors" - contextual elements that increase the likelihood that a danger will translate into harm.

The solutions mapped from the consultation data include robust regulatory measures such as effective age verification systems, intuitive and appropriate parental mediation tools, and the promotion of ethical design practices that prioritize privacy and security. Without these, we face scenarios such as:

- Attention-capturing mechanisms are especially harmful to children and adolescents—individuals at a unique stage of biopsychosocial development, whose prefrontal cortex, the brain region responsible for decision-making, is still forming. This limits their capacity for planning and impulse control [Gray et al. 2024].
- The potential misuse of parental control tools for surveillance purposes, as seen with the *mSpy* app—a parental monitoring tool that enables tracking of dependent devices, including reading messages, GPS location, and device data—raises serious concerns.

It is crucial to emphasize that when introducing or applying data protection, privacy-by-design, security-by-design, or other regulatory measures, States Parties must ensure that companies do not target children using these or other techniques designed to prioritize commercial interests over children's rights [Committee et al. 2021]. Furthermore, for parental mediation strategies on platforms to be effective, a collaborative and multidisciplinary approach is required—one that includes technology companies, lawmakers, the executive branch, health experts, and civil society.

Finally, it is essential to adopt an intersectional, plural, and decolonial perspective that reflects the diverse cultural, social, and normative realities of children and their caregivers in the Brazilian context. This includes addressing structural challenges such as meaningful access to technology while also questioning dominant frameworks that risk reproducing colonial or exclusionary logics. Only by integrating these critical approaches into evidence-based regulatory solutions - such as age verification, ethical design, and inclusive policymaking - can we build a digital environment that prioritizes the rights,

autonomy, and healthy development of all children and adolescents, as guaranteed by the Brazilian Federal Constitution [de Oliveira et al. 2024].

One **limitation** of our study is the possibility that relevant excerpts from CGI.br's consultation regarding parental mediation may not have been identified during our data extraction process - despite our best efforts to combine syntactic expressions in a structured way to collect as much evidence as possible.

Related studies have addressed the need for guidelines to design parental control features. Previously, Iftikhar and colleagues [Iftikhar et al. 2021] highlighted that an increasing number of children online is a situation that requires parental control tools to empower caregivers to regulate Internet usage. Their work describe a systematic literature review on the design of these tools from 2011-2021, synthesizing proposed design guidelines and future opportunities for the HCI community. Another work that has a similar goal was performed by Albuquerque et al., but focusing on smart toys.

In this scenario, which also grows in terms of popularity among children, the authors present privacy risks of such technologies together with proposed technical and domain-specific solutions [de Paula Albuquerque et al. 2020]. In their turn, Yao and colleagues [Yao et al. 2025] adopted a legal stance to map regulations across different countries related to children and adult-oriented apps. They described that several countries employ a multi-faceted approach that includes age verification and parental controls to prevent children from accessing adult content online, for example. Finally, Baughan et al. [Baughan et al. 2024] investigated Children's Social Video Games to propose a set of recommendations for parental control, such as creating features that make parents aware of moments of or interrupt game play during user-paced traveling or game initiated pauses. Those are previous studies that embrace related scenario (such as games or smart toys) that are also part of children's daily routines and that need to be improved in terms of protection - which can be ensured via ethical design practices and regulation.

For **future studies**, we propose the following research agenda:

- To reduce this limitation by gathering additional evidence from journalistic and academic sources. We intend to conduct systematic mapping studies on specific platforms such as TikTok or Roblox to assess the risks they pose and the parental mediation tools they offer. This would allow us to contextualize our findings within the broader literature, combining CGI.br consultation data with insights from recent Computer Science research. Including academic literature will help corroborate, complement, or even challenge the arguments from the consultation.
- To foster collaboration with partner institutions such as Fairplay (UK), presenting our findings in ways that could lead to new conclusions or even the development of guidelines or requirements for such tools on platforms.
- Finally, we plan to design prototypes of parental mediation features to be tested with children and caregivers (thereby, not only refining our research findings but also promoting digital literacy).

Ethical considerations

This study does not include any activities involving human participants.

References

Albuquerque, N., Valença, G., e Falcão, T. P. (2024). Investigating manipulative design on social media platforms-the case of kidinfluencers. *Journal on Interactive Systems*, 15(1):860–874.

Baroni, L. A. e Pereira, R. (2024). Deceptive patterns under a sociotechnical view. In *XXIII Brazilian Symposium on Human Factors in Computing Systems*, pages 1–13.

Baughan, A., Fu, Y., Izenman, E., Schwamm, S., Alsabeh, D., Powell, N., Hunt, E., Rich, M., Bickham, D., Radesky, J., et al. (2024). Investigating attention and normative dissociation in children's social video games. In *Proceedings of the 23rd annual ACM interaction design and children conference*, pages 30–43.

Cao, J., Das, A., Emami-Naeini, P., et al. (2024). Understanding parents' perceptions and practices toward children's security and privacy in virtual reality. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 1554–1572. IEEE.

Castro, E. G. d. e Macedo, S. C. (2019). Estatuto da criança e adolescente e estatuto da juventude: interfaces, complementariedade, desafios e diferenças. *Revista Direito e Práxis*, 10(2):1214–1238.

Committee, C. et al. (2021). General comment no. 25 on children's rights in relation to the digital environment. `https://tinyurl.com/467wjb8j`. Accessed: 2025-05-09.

Cruzes, D. S. e Dyba, T. (2011). Recommended steps for thematic synthesis in software engineering. In *2011 international symposium on empirical software engineering and measurement*, pages 275–284. IEEE.

de Oliveira, L. C., Amaral, M. A., Bim, S. A., Valença, G., Almeida, L. D. A., Salgado, L. C. d. C., Gasparini, I., e da Silva, C. B. R. (2024). Grandihc-br 2025-2035-gc3: Plurality and decoloniality in hci. In *Proceedings of the XXIII Brazilian Symposium on Human Factors in Computing Systems*, pages 1–19.

de Paula Albuquerque, O., Fantinato, M., Kelner, J., e de Albuquerque, A. P. (2020). Privacy in smart toys: Risks and proposed solutions. *Electronic Commerce Research and Applications*, 39:100922.

Domingos, L. (2017). Telas e crianças: Conheça os mitos e riscos desta exposição. `https://tinyurl.com/mrxyy4e7`. Accessed: 2025-05-09.

dos Santos Madeira, F. N., de Souza Rosa, M., Ferreira, A. G. N., Dias, I. C. C. M., e Bezerra, J. M. (2023). Análise de aplicativos móveis voltados para controle parental: revisão narrativa. *Arquivos de Ciências da Saúde da UNIPAR*, 27(3):1457–1476.

Geržičáková, M., Dedkova, L., e Mỳlek, V. (2023). What do parents know about children's risky online experiences? the role of parental mediation strategies. *Computers in Human Behavior*, 141:107626.

Ghedin, R. (2024). Controle parental não é a resposta. `https://tinyurl.com/mm27b5w4`. Accessed: 2025-05-09.

Gray, C. M., Santos, C., Bielova, N., e Mildner, T. (2024). An ontology of dark patterns knowledge: Foundations, definitions, and a pathway for shared knowledge-building. In *2024 CHI Conference on Human Factors in Computing Systems*, pages 1–22.

Horkoff, J. e Yu, E. (2016). Interactive goal model analysis for early requirements engineering. *Requirements Engineering*, 21:29–61.

Iftikhar, Z., Haq, Q. R. u., Younus, O., Sardar, T., Arif, H., Javed, M., e Shahid, S. (2021). Designing parental monitoring and control technology: A systematic review. In *IFIP Conference on Human-Computer Interaction*, pages 676–700. Springer.

NIC.BR (2024). Tic kids online brasil - 2024. `https://tinyurl.com/3m3crruy`, note = Accessed: 2025-05-09.

Nouwen, M., JafariNaimi, N., e Zaman, B. (2017). Parental controls: reimagining technologies for parent-child interaction. In *15th European Conference on Computer-Supported Cooperative Work-Exploratory Papers*, volume 2017, pages 18–34.

Ofcom (2022). Research into risk factors that may lead children to harm online. `https://tinyurl.com/yc3tj2tk`. Accessed: 2025-05-09.

Pasquale, L., Zippo, P., Curley, C., O'Neill, B., e Mongiello, M. (2020). Digital age of consent and age verification: can they protect children? *IEEE software*, 39(3):50–57.

Silva, V. H. (2023). O ex-diretor do instagram que viu sua própria filha sofrer assédio na rede social. `https://tinyurl.com/yc4yy335`. Accessed: 2025-05-09.

United Nations (1989). Convention on the rights of the child. `https://tinyurl.com/yc3tj2tk`. Accessed: 2025-05-09.

Winther, D. K., Livingstone, S., Saeed, M., et al. (2019). Growing up in a connected world. `https://tinyurl.com/bdz4bjha`. Accessed: 2025-05-09.

Wisniewski, P., Ghosh, A. K., Xu, H., Rosson, M. B., e Carroll, J. M. (2017). Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety? In *ACM Conf. on Computer Sup. Cooperative Work and Social Comp.*, pages 51–69.

Yao, Y., McCollum, S., Sun, Z., e Zhang, Y. (2025). Easy as child's play: An empirical study on age verification of adult-oriented android apps. In *Proceedings of the 34th USENIX Security Symposium*.

Zaman, B., Nouwen, M., Vanattenhoven, J., De Ferrerre, E., e Looy, J. V. (2016). A qualitative inquiry into the contextualized parental mediation practices of young children's digital media use at home. *J. of Broadcasting & Elec. Media*, 60(1):1–22.