Journal of the Brazilian Computer Society, 2026, 32:1, doi: 10.5753/jbcs.2026.8248
This work is licensed under a Creative Commons Attribution 4.0 International License.

Unsafe by Design? Examining Age Assurance Mechanisms and Child Protection on Digital Platforms

André de Andrade Theodoro [**Federal Rural University of Pernambuco** | ***andre.theodoro@ufrpe.br***]
George Valença [**Federal Rural University of Pernambuco** | ***george.valenca@ufrpe.br***]
Átila Rodrigues [**Federal Rural University of Pernambuco** | ***atila.rodrigues@ufrpe.br***]

Department of Computing, Universidade Federal Rural de Pernambuco, Praça Farias Neves, 2, Dois Irmãos, Recife, PE, 52171-900, Brazil.

Received: 18 May 2026 • **Accepted:** 26 October 2026 • **Published:** 12 November 2026

Abstract. Given the ease of unsupervised access and the growing risks faced by minors online, safeguarding children's digital rights has become increasingly urgent. As personal data becomes a major economic asset, governments worldwide are enforcing stricter age assurance requirements for digital platforms. This study investigates age assurance mechanisms on the social media platforms most frequently used by Brazilian children and adolescents. First, we created test accounts and analyzed the terms of use and age assurance procedures of YouTube, TikTok, Instagram, and WhatsApp. Second, we examined contributions submitted to a public consultation on platform regulation conducted by the *Comitê Gestor da Internet no Brasil* (CGI.br) to identify expert concerns and expectations regarding age assurance. Third, we conducted a systematic mapping study of age verification research published between 2020 and 2025, examining categories of age verification methods, data modalities, evaluation approaches, and evidence regarding their effectiveness. Our findings indicate that platforms in Brazil largely mirror patterns observed in previous international studies, relying on mechanisms that can be easily circumvented. The literature similarly reveals the absence of a universally effective solution, highlighting trade-offs between robustness, privacy, and inclusion. Rather than proposing a new age-assurance mechanism, we provide a contextual and integrative examination of existing approaches within the Brazilian regulatory and child-protection context. Taken together, the results suggest that age assurance should not be understood solely as a technical challenge, but as a broader socio-technical issue involving child protection, data governance, and digital rights.

Keywords: Age Assurance, Social Media Platforms, Child Online Safety, Regulation.

1 Introduction

In 2025, the global social media user figure had exceeded 5 billion [Kemp, 2025]. Today, they extend far beyond communication tools, increasingly functioning as spaces to identity construction, self-expression, and professional development, including the emergence of child influencers and "sharenting" as a practice [Albuquerque *et al*., 2024; Ngai *et al*., 2015].

In this context, children and adolescents are increasingly accessing digital platforms independently, often without adult supervision [Pasquale *et al*., 2022; Jarvie and Renaud, 2024]. In Brazil, 93% of individuals aged 9 to 17 are Internet users, representing approximately 24.5 million young people, many of whom access digital platforms several times a day [Cetic.br and NIC.br, 2024]. This intensive participation suggests that childhood is increasingly experienced through digital interactions, which can generate significant consequences for children's and adolescents' everyday lives and well-being [Farthing *et al*., 2021].

Users under the age of 18 account for approximately one-third of Internet users in Brazil [Cetic.br and NIC.br, 2024]. Studies have associated excessive engagement with digital platforms with dependency, reduced participation in offline activities, and potential impacts on physical and psychological well-being [Ngai *et al*., 2015]. The constant pressure to maintain and update online profiles may also contribute to stress and emotional burden, while young users can be exposed to unethical design practices, including manipulative and deceptive design [Albuquerque *et al*., 2024]. Taken together, this evidence indicates that, as access to digital platforms becomes increasingly widespread, children and adolescents may be exposed to a broad range of online risks.

Studies have documented multiple risks faced by children and adolescents across digital platforms. In community- or forum-based environments, such as Discord, young users may experience cyberbullying, with potentially severe and long-lasting psychological consequences [Slonje *et al*., 2013]. Other studies have shown how social media platforms can be used to target children through personalized advertising [Carvalho and Marques-Neto, 2024] and, in more severe cases, facilitate the dissemination of child sexual abuse material [Coelho and de Oliveira, 2021]. In environments where content moderation practices are more flexible, users may also be exposed to harassment, adult content, and online scams [Faraz *et al*., 2022]. Taken together, this evidence suggests that inadequate access control and protection mechanisms may increase children's vulnerability to harmful content, interactions, and practices in digital environments.

Therefore, children's and teenagers' online browsing presents a dilemma for researchers, families, and regulatory entities, among other stakeholders involved in the digital protection of this group. These platforms offer numerous

opportunities for developing educational, communication, and creative skills [Hasebrink *et al*., 2008]. However, they pose risks to physical health and psychological well-being [Staksrud and Livingstone, 2009].

In this article, we evaluate the age assurance mechanisms employed by social media platforms that are part of the everyday digital experiences of children and adolescents in Brazil. Platform selection was informed by findings from the *Tecnologias de Informação e Comunicação* (TIC) Kids Online Brasil 2024 survey, conducted annually by the *Comitê Gestor da Internet no Brasil* (Brazilian Internet Steering Committee, CGI.br) [Cetic.br and NIC.br, 2024]. Our analysis replicates previous studies that investigated the robustness of access control mechanisms in popular applications used by young users in Ireland [Pasquale *et al*., 2022; Curley, 2020]. Additionally, we examine expert perspectives on this topic through contributions submitted to the CGI.br public consultation on platform regulation conducted in 2024 [Comitê Gestor da Internet no Brasil (CGI.br), 2025].

This article extends and revises our WebMedia 2025 paper [Theodoro and Valença, 2025]. The extension introduces a systematic mapping study and provides a broader socio-technical integration of the empirical platform evaluation, expert consultation data, and literature evidence. The empirical platform evaluation is designed as a contextual replication and extension of previous international studies on age assurance [Pasquale *et al*., 2022; Curley, 2020]. Because these previous evaluations were conducted using Irish versions of the applications, their findings are geographically bounded and may not reflect age-assurance practices under different regulatory and data-protection contexts. We therefore apply and adapt this established approach to platforms operating in Brazil, examining how these mechanisms are implemented within the country's regulatory and child-protection context.

Our findings indicate that the age assurance procedures used by platforms in Brazil are similar to those found in Ireland and can be easily circumvented by users. Although some platforms have introduced initiatives for stronger protection or more inclusive forms of supervised access, these mechanisms remain limited and frequently rely on self-reported information. The mapping study reveals a growing research interest in age assurance and a broad range of proposed approaches, particularly document-based and biometric methods. However, the literature highlights the absence of a universally effective solution, pointing instead to persistent trade-offs between robustness, privacy, and inclusion. Our results suggest that age assurance should not be treated solely as a technical challenge, but rather as a socio-technical issue involving child protection, data practices, and regulatory concerns.

The contribution of this study does not lie in proposing a novel age-assurance mechanism, for example. Instead, it combines a contextual replication of platform evaluations in Brazil with evidence from the CGI.br public consultation and a systematic mapping study. The mapping provides a structured synthesis of the age-assurance landscape by characterizing existing mechanisms, data modalities, evaluation practices, and recurring trade-offs. Together, these sources enable an integrated socio-technical analysis of age assurance and its implications for child protection, privacy, and inclusion.

2 Conceptual Background

2.1 Online Risks to Children

The **risks** to which children and young people are exposed online are commonly classified into at least three categories: *content*, *contact*, and *conduct* risks [Hasebrink *et al*., 2008; Staksrud and Livingstone, 2009]. *Content-related* risks involve exposure to potentially harmful material, including advertisements, spam, and violent, misleading, racist, or sexual content. *Contact-related* risks involve children's passive participation in online activities and include interactions with strangers, experiences of bullying or manipulation, tracking practices, and the collection of personal data.

Conduct risks, in contrast, assume a more active role by children and adolescents, involving behaviors such as participating in gambling activities, accessing illegal content, producing pornographic material, or encouraging self-destructive practices among peers [Staksrud and Livingstone, 2009; Livingstone and Stoilova, 2021; Faraz *et al*., 2022].

In addition to these categories, Livingstone and Stoilova [2021] identify a fourth type of risk associated with the relationship between digital service providers and children and adolescents. *Contractual* or *commercial* risks reflect the increasing commercialization of children's personal data and emerge when children accept providers' terms of service, either intentionally or unintentionally, often without fully understanding their implications [Mascheroni, 2020].

Digital platforms are frequently criticized for failing to provide terms and policies tailored to children and adolescents, instead relying on technical and legal language that can be difficult for young users to understand. As a result, these platforms often neglect the accessibility and usability of such information for younger audiences and fail to adopt strategies that actively promote family involvement in data privacy and protection of children and adolescents [Farthing *et al*., 2021].

Table 1 summarizes the 4C model and relates the four types of online risk to the roles assumed by children and adolescents in digital environments.

2.2 Age Assurance and Regulations

Given the ease of unsupervised access and the risks associated with digital platforms (particularly social media) the need for technology companies to safeguard children's and adolescents' rights by default becomes increasingly critical. This principle has recently been discussed under the concept of *Children's Rights by Design*, which advocates for embedding child protection considerations into the design of digital services from the outset [Livingstone and Stoilova, 2021; Farthing *et al*., 2021]. This concern becomes even more relevant considering that the large amount of personal data collected from young users through digital platforms has become a significant economic asset [Laterça, 2022].

This scenario has led governments worldwide to introduce stricter **regulations** requiring digital service providers to adopt more robust age assurance mechanisms [Jarvie and Renaud, 2024]. Legislative initiatives, including Brazil's Law No. 15,211/2025, the *Estatuto Digital da Criança e do Adolescente*, suggest different approaches to age assurance,

Table 1. 4C Model – Online Risks for Children and Adolescents (adapted from Livingstone and Stoilova [2021]).

	Content *Child as Recipient*	**Contact** *Child as Participant*	**Conduct** *Child as Actor*	**Contract** *Child as Consumer*
Aggressive	Exposure to violent, hateful, racist, or extremist material.	Harassment, stalking, and intrusive or excessive surveillance.	Bullying, hate speech, and social exclusion.	Identity theft, fraud, coercion, scams, and phishing.
Sexual	Exposure to sexual and/or pornographic material.	Sexual harassment; production, solicitation, or dissemination of child sexual abuse material; sextortion.	Sexual harassment, coercive threats of abuse, and sexually explicit communications.	Commercial live-streaming of child sexual abuse and trafficking for purposes of sexual exploitation.
Values	Exposure to misleading, manipulative, or ideologically biased content, including disinformation.	Extremist recruitment, ideological indoctrination, and processes of radicalization.	Participation in communities or networks associated with potential harm.	Gambling practices, algorithmic filter bubbles, and manipulative consumer targeting.

including the use of artificial intelligence techniques such as facial analysis and age estimation based on photographs [Brasil, 2025; Jarvie and Renaud, 2024]. Digital platforms have adopted different age-assurance approaches, including age verification based on official identification documents and age estimation based on facial images, such as photo or video selfies [Cetic.br, 2026].

A related study conducted by Jarvie and Renaud [2024] analyzes major legal frameworks concerning online age assurance worldwide. Their findings identify significant regulatory progress in regions such as the European Union and the United States, mapping initiatives designed to protect children from harmful online content. Although several European countries had previously implemented laws concerning online child protection, a broader legal framework for personal data protection was only established in 2018 through the General Data Protection Regulation (GDPR) [GDPR.info, 2016]. The study also highlights broader initiatives, such as the multinational *EU Kids Online* research network [Hasebrink *et al*., 2008], which investigates risks and benefits related to children's digital participation, including issues related to privacy, data protection, and age assurance.

In the United States, the *Children's Online Privacy Protection Act* (COPPA) represents an important milestone in the protection of children's personal data [Federal Trade Commission, 1998]. COPPA [Federal Trade Commission, 1998], enacted in 1998, considered the concept of the *digital age of consent*, establishing restrictions on the collection and use of personal data from children under the age of 13 and effectively defining this threshold as the minimum age for many digital services and social media environments [Pasquale *et al*., 2022]. China has likewise adopted highly restrictive measures concerning minors' access to online content. Enacted in 2019, the *Provisions on Cyber Protection of Personal Information of Children* (PCPPIC) established specific guidelines for children's data protection and defines the age threshold at 14, rather than the more conventional 18 or 21 years [Jarvie and Renaud, 2024].

In Brazil, children's personal data are protected by the *Lei Geral de Proteção de Dados Pessoais* (LGPD), which requires specific parental or guardian consent for the processing of children's data. However, this requirement does not extend to adolescents [Brasil, 2018]. In addition, the *Estatuto da Criança e do Adolescente* (ECA) establishes that the processing of children's data must occur according to the principle of the child's best interests [Brasil, 1990]. Laterça [2022] argues that, where the LGPD does not provide sufficient guidance, institutions such as the *Agência Nacional de Proteção de Dados* (ANPD)[1] may play an important complementary regulatory role. The author also highlights the international influence of COPPA, which has become a reference framework for child data protection practices in several countries, including Brazil Laterça [2022].

Across the jurisdictions discussed above, the literature points to increasing regulatory attention regarding the processing of children's personal data. Motivated by this scenario, Pasquale *et al*. [2022] and Curley [2020] investigated age assurance mechanisms in social media platforms to examine whether children and adolescents in Ireland had safe and supervised access to these environments. The present study builds upon and extends the protocol adopted in these studies.

To effectively manage age-related access and regulatory compliance, it is important to distinguish among the different approaches used to assess a user's age. According to the Brazilian National Data Protection Authority [ANPD, 2026], age-related assessment mechanisms can be organized into four interconnected concepts, which operate as distinct yet complementary components within the broader age assurance ecosystem, as illustrated in Figure 1.

Age Assurance is an umbrella framework encompassing different methodologies and systems designed to verify, estimate, or infer an individual's age or age group. This broader concept enables institutions to determine age eligibility with varying levels of confidence and precision. In this context, **age estimation** is a probabilistic approach that predicts a person's likely age based on the analysis of behavioral patterns or biometric characteristics. Common indicators include facial geometry, vocal attributes, and digital interaction behaviors.

In its turn, **age verification** is a process that seeks to confirm an individual's exact age using highly reliable and authoritative sources. Typical mechanisms include government-issued identification documents (e.g., passports or ID cards), financial credentials, and secure digital identity services (e.g.,

[1]Official ANPD website: `https://www.gov.br/anpd/`.

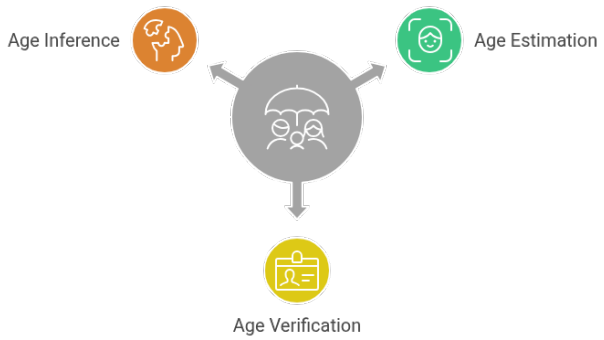


Figure 1. Age Assurance Components.

GOV.br). Finally, **age inference** is an indirect and complementary approach that estimates a user's likely age group through contextual indicators. Rather than relying on explicit proof, it uses variables such as browsing behavior, purchasing history, and educational information to support broader age assurance systems.

3 Research Method

This study was structured into three methodological stages: (i) an empirical evaluation of age assurance mechanisms on four digital platforms; (ii) an analysis of contributions submitted to the CGI.br public consultation on platform regulation; and (iii) a systematic mapping study of age assurance research published between 2020 and 2025. The following subsections describe the procedures adopted in each stage.

3.1 Age Assurance Mechanisms on Digital Platforms

Based on data from the *TIC Kids Online Brasil 2024* survey on Internet and social media use among children and adolescents aged 9 to 17 [Cetic.br and NIC.br, 2024], we selected the digital platforms most frequently used by this population in Brazil. The empirical evaluation followed the procedure adopted by Curley [2020] and discussed by Pasquale *et al*. [2022].

With regard to the online habits of Brazilian children and youth, the TIC Kids Online Brasil 2024 survey found that 93% of this age group accesses the internet primarily to listen to music and do school research (86%), watch videos or movies (84%), play games (76%) use social media, and send instant messages (76%). The most popular platforms used were WhatsApp, YouTube, Instagram, and TikTok, and 83% of them have their own profiles [Cetic.br and NIC.br, 2024].

Based on the online behavior of kids and teens and considering the specifics of Brazilian legislation on the processing of personal data (LGPD), this study examined the main apps used multiple times a day by kids and teens aged 9 to 17 in Brazil: WhatsApp, YouTube, Instagram, and TikTok Cetic.br and NIC.br [2024]. On these platforms — one messaging app (WhatsApp) and three social media and entertainment platforms (YouTube, Instagram, and TikTok), — we evaluated the main age assurance mechanisms used by analyzing their terms of service (to assess criteria such as "minimum age") and the procedures for children's and adolescents' profiles (by creating fictitious profiles with ages of 12, 13, and 16). Hence, no real children participated and no personal data from children were collected.

Thus, this study on age assurance mechanisms was guided by two research questions (RQs) proposed by Pasquale *et al*. [2022]:

- RQ1 - Do the application's terms of use incorporate the age limits established by data protection regulations?
- RQ2 - Do applications implement robust age assurance mechanisms for their users?

The tests were conducted between March and May 2025 using the mobile applications available at the time on iOS. We analyzed the mobile versions of each app, given that 81% of accesses are made via mobile devices Cetic.br and NIC.br [2024]. In Table 2, we outline the protocol, consisting of seven questions, used to evaluate the applications.

Table 2. Management of Underage Users in Online Platforms.

#	Question
1	What is the minimum age stated in the Terms of Use?
2	Is it mandatory to input the age on sign-up?
3	If the answer to the previous question is yes, what happens if age 12 is entered?
4	If age 13 is entered, are there any additional assurance processes (e.g., e-mailing a parent)?
5	Is it possible to bypass the existing age assurance process?
6	If age 16 is entered on sign-up, is there any age assurance process enabled?
7	At any point, is the minimum age made clear to the user?

In Europe, the minimum age at which children can consent to the processing of their personal data may vary between 13 and 16 years across Member States [Pasquale *et al*., 2022]. Therefore, the tests considered both age thresholds. Although Brazilian legislation does not establish the same distinction, we replicated all steps of the original evaluation protocol to preserve consistency with the previous study.

During this process, we considered the guiding questions listed in Table 2. Question 1 pertains to the terms of use, while questions 2 through 6 are based on practical tests. Finally, question 7 combines the results of both. All questions were addressed during the testing phase, with one researcher responsible for conducting the review and a second researcher analyzing and discussing the evidence obtained. Hence, the empirical platform evaluation was conducted by one researcher and subsequently reviewed by a second researcher.

3.2 Challenges and Expectations for Regulating Age Assurance on Digital Platforms

To provide additional insights into the age assurance mechanisms of the platforms evaluated, we examined consultation data from CGI.br regarding platform regulation, which received approximately 1,400 contributions from individuals

and organizations in the government, nonprofit, and corporate sectors, as well as input from the scientific community [Comitê Gestor da Internet no Brasil (CGI.br), 2025].

The results of the consultation were published by CGI.br in multiple formats, including a website, CSV file, and PDF report [Comitê Gestor da Internet no Brasil (CGI.br), 2025]. We searched the PDF using Portuguese terms related to age assurance, including terms corresponding to "age verification" and "assessment." The retrieved passages were inspected and retained when they substantively addressed age restrictions, age-assurance mechanisms, their limitations, or proposals for improving age assurance on digital platforms. This process resulted in a corpus of 14 excerpts, which were transferred to a text file for qualitative analysis.

Google NotebookLM was used as an AI-assisted analytical support tool to generate and organize candidate themes from the 14 excerpts. The multiple interactions with the tool were conducted during the analysis, with instructions that resulted in the thematic organization. The candidate themes generated with the support of NotebookLM were subsequently reviewed against the original excerpts by the researchers, who assessed their coherence and correspondence with the source material. The researchers then validated the final categorization, resulting in four themes: *age restrictions as a mitigation strategy*, *limitations of current age restrictions*, *suggestions for more effective age assurance*, and *challenges of rigorous age assurance*. Thus, NotebookLM supported the initial organization of candidate themes, while their interpretation and final validation remained the responsibility of the researchers.

This study did not recruit, contact, or interact with human participants. The consultation analysis relied exclusively on contributions previously made publicly available by CGI.br as part of its public regulatory consultation. No attempt was made to re-identify contributors beyond the information contained in the public dataset.

3.3 Systematic Mapping Study

The systematic mapping study was guided by the recommendations of Petersen *et al*. [2015]. These guidelines informed the organization of the mapping into four main activities: definition and calibration of the search strategy, screening of retrieved studies according to the eligibility criteria, structured extraction of data from the included studies, and synthesis of the extracted evidence according to the research questions.

The systematic mapping study aimed to answer the following **research questions**:

- RQ3: What age assurance categories are discussed in the literature?
- RQ4: What modalities and data types are used?
- RQ5: How are age assurance mechanisms evaluated?
- RQ6: What conclusions are reported regarding effectiveness?

Then, we conducted a comprehensive search across six digital libraries: IEEE Xplore (`ieeexplore.ieee.org`, accessed December 27, 2025), Google Scholar (`scholar.google.com`, accessed February 19, 2026), ACM Digital Library (`dl.acm.org`, accessed January 24, 2026), ScienceDirect (`sciencedirect.com`, accessed February 11, 2026), Wiley Online Library (`onlinelibrary.wiley.com`, accessed February 11, 2026), and JSTOR (`jstor.org`, accessed February 11, 2026). The search targeted studies published between 2020 and 2025 and focused specifically on age assurance research. The final search string was defined through an iterative calibration process involving testing and refinement across the selected digital libraries: *Title:(age) AND Title:(verification OR assurance OR estimation OR assessment)*.

The mapping was restricted to English-language publications retrieved from the six selected digital libraries. This scope was adopted to maintain a consistent search strategy across the selected international databases and to ensure the feasibility of the screening and analysis process. Therefore, Portuguese search terms and regional sources, such as SBC OpenLib, were not included in the search strategy.

The initial search returned 889 records: 385 from IEEExplore, 100 from Google Scholar, 266 from ACM Digital Library, 79 from ScienceDirect, 11 from Wiley Interscience, and 48 from JSTOR. A multi-stage screening process was then applied to refine the corpus.

Then, we considered the following **inclusion criteria**:

- The study's primary contribution concerns the design, implementation, evaluation, or application of age assurance methods, systems, or policies;
- When multiple papers reported the same study, only the most complete version was included;
- When multiple studies appeared within a single paper, each relevant study was treated independently.

In addition, we had the following **exclusion criteria**:

- Studies not written in English;
- Papers outside the age assurance research domain;
- Studies for which the full text was unavailable or could not be accessed in PDF or Microsoft Word format;
- Duplicate records indexed across multiple digital libraries.

In the first screening stage, titles were reviewed to identify and remove false positives, resulting in the exclusion of 536 articles outside the scope of this study. Most excluded papers were related to clinical medicine and age assessment examinations rather than technical age assurance systems. This stage retained 165 articles from IEEE, 47 from Google Scholar, 104 from ACM, 23 from ScienceDirect, 2 from Wiley, and 12 from JSTOR. Subsequently, the abstracts of the remaining studies were analyzed, leading to the exclusion of an additional 37 articles (15 from IEEE, 7 from Google Scholar, 13 from ACM, and 2 from ScienceDirect).

Following title and abstract screening, a deduplication process was performed to ensure that only unique records remained. This step removed 51 duplicate entries indexed across multiple databases, resulting in a consolidated set of 265 unique studies. Efforts were then made to obtain full-text versions of all identified articles, including direct contact with authors and requests through academic networks such as ResearchGate. While 245 studies were successfully retrieved, 20 remained inaccessible. The resulting corpus of 245 articles formed the basis for data extraction and subsequent analysis. The complete selection process is illustrated in Figure 2.

The mapping did not adopt a dedicated grey literature search strategy. The corpus was retrieved exclusively through the six digital libraries described above, according to the predefined search string and selection criteria. Hence, non-peer-reviewed materials indexed by these sources, such as institutional reports, policy documents, and technical publications, could be included when they met the eligibility criteria. However, we did not conduct complementary searches targeting grey literature repositories, governmental websites, NGO publications, industry reports, or other sources outside the selected databases. Therefore, the mapping should not be interpreted as providing systematic coverage of grey literature.

3.3.1 Data extraction

Following the final selection of 245 accessible articles, a structured data extraction process was conducted to collect the information necessary to address the research questions of this systematic mapping study. To ensure consistency and completeness, a standardized extraction framework was applied to all studies. Table 3 summarizes the extracted data.

Table 3. Data extraction fields and descriptions applied to the final corpus of articles.

Data Field	Description
Functional Technical Implementation	Does the paper propose a functional implementation of an AV method?
AV Category Developed / Addressed	The broad approach used to verify age, such as analyzing physical traits, reviewing ID cards.
Specific Technology / Algorithm	The specific tools or logic powering the system, such as artificial intelligence.
Modality	The type of information the system looks at to make a decision, like photos of a face.
Datasets Used	The collections of information used to teach the system or test if it works correctly, such as public photo galleries or private collections of user data.
Evaluation Framework / Method	The setting or method used to see if the proposed system actually works, like a controlled laboratory experiment, real-world testing, or theoretical analysis.
Evaluation Metrics	The criteria used to judge the obtained results, can be used to obtain quantitative results or give more insights to the conclusions.
Quantitative Results	The numerical results from the testing phase, showing the actual performance scores or error margins of the system.
Conclusions on Effectiveness	A short summary of the authors' final thoughts on how well their AV methods behave in practice based on their insights.

The primary goal of collecting these data was to understand the theoretical foundations of age assurance approaches and their practical feasibility and real-world applicability.

3.3.2 Thematic Synthesis

During the thematic synthesis phase, the extracted data were used to organize the studies into a hierarchical taxonomy aimed at characterizing the research landscape, as illustrated in Figure 3. The first level of classification relied on the *Functional Technical Implementation* attribute, dividing the corpus into two primary branches: studies proposing practical, operational systems (*Has technical implementation*) and studies without a technical implementation (*No technical implementation*). This initial distinction separated hands-on engineering and system development research from broader theoretical, policy-oriented, or review-based studies.

The second level of categorization relied on the *Age Assurance Category Developed / Addressed* attribute to further refine these branches according to their technological focus. Studies with technical implementations were subdivided into biometric-based approaches and other implementation categories. In contrast, studies without technical implementations were grouped according to the scope of their analysis, resulting in categories such as biometric-focused analyses, comparative studies examining multiple age Assurance categories, and broader conceptual discussions of age assurance. This structure provides a clearer view of the current distribution of research efforts and highlights trends within the field.

3.3.3 Data Analysis

The scope of this analysis focused on studies that simultaneously evaluate multiple age assurance categories. This decision was motivated by future research directions identified in our previous work [Theodoro and Valença, 2025], which highlighted the need to systematically examine a broad range of age assurance mechanisms, including self-declaration approaches, hard identifiers, and commercial and technical solutions. The goal was not only to assess the robustness of these alternatives but also to understand implementation trade-offs, particularly those involving personal data processing and privacy risks.

By concentrating on studies that compare multiple age assurance categories, the present research addresses this previously identified gap. Studies limited to isolated technical implementations or broad conceptual discussions cannot provide the comparative evidence necessary to evaluate trade-offs across different approaches. Therefore, focusing on the category *Analysis of Many Age Assurance Categories* enables a broader assessment of robustness, privacy implications, practical considerations, and legal or regulatory requirements associated with age assurance mechanisms.

4 Age Assurance in Digital Platforms

This section addresses the research questions by describing the mechanisms and terms of use for age assurance on the selected platforms, as assessed during the tests conducted.

4.1 WhatsApp

According to WhatsApp's Terms of Service, the platform is intended for users who are at least 13 years old, though this age

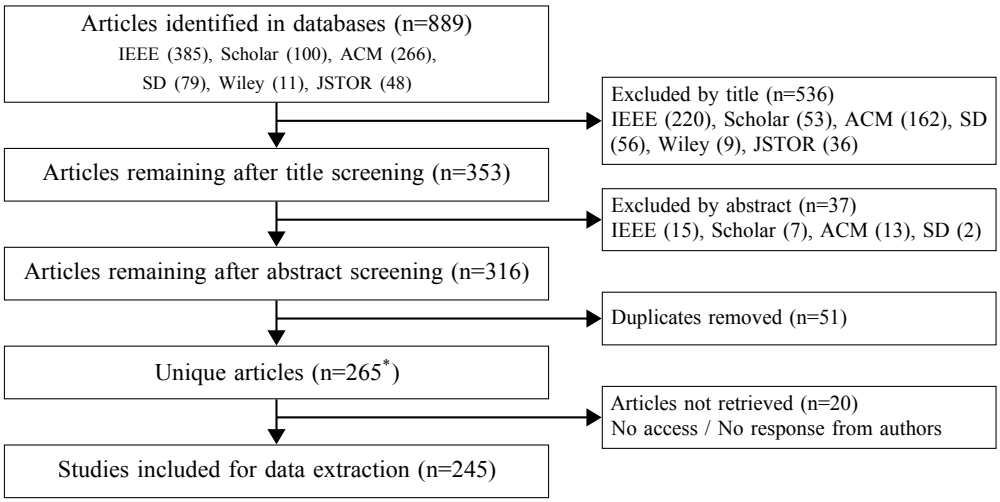


Figure 2. Study selection flow diagram for the systematic mapping study.

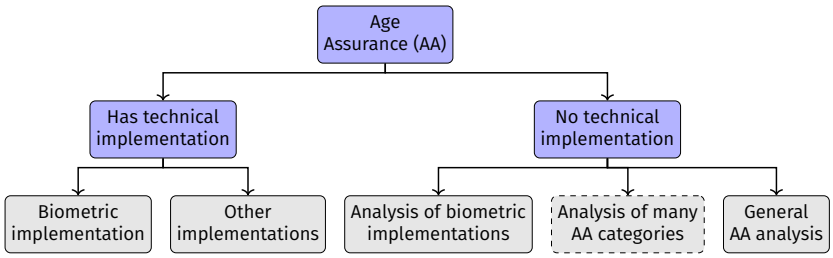


Figure 3. Article categorization

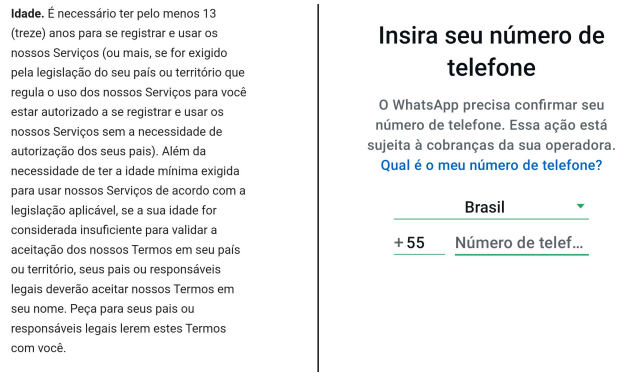


Figure 4. WhatsApp – Portuguese Terms of Service and account creation. Relevant text translated from Portuguese: "You must be at least 13 years old to use our Services, or older if required in your country."

may be higher depending on the laws governing the service in the user's jurisdiction. The Terms also require parental consent if the user's age is considered insufficient to accept them under the applicable legislation. Although WhatsApp is clear about age restrictions for its users, the platform does not employ any type of age assurance mechanism. Simply entering a phone number is sufficient to create an account (cf. Figure 4).

4.2 YouTube

YouTube's Terms of Service set the minimum age for accessing its services at 13 and require parental consent for users under 18. The platform stands out for offering a version of its services tailored for children, YouTube Kids, which requires registration by parents or guardians. This approach is noteworthy for creating an inclusive and age-appropriate environment that minimizes exposure risks while encouraging the positive use of technology in children's development [Livingstone and Sylwander, 2025]. However, this version of the platform was not mentioned in the original study and is not among the four main platforms highlighted in the *TIC Kids Online Brasil 2024* survey [Cetic.br and NIC.br, 2024]. Therefore, we are considering the standard version of YouTube.

The platform is integrated with Google, which means that users must have a Google account to access YouTube services. For this reason, our tests were conducted through Google (Figure 5), in accordance with its terms of service and registration procedures. For teenagers, parental controls become optional. Since YouTube offers the Family Link feature, children can invite their parents or guardians to monitor their access. However, this option is not presented during account creation and must be actively sought out in the settings, which could be interpreted as misleading design (since child protection is not the default setting) [Albuquerque *et al.*, 2024].

4.3 Instagram

Instagram's Terms of Use also establish that users must be at least 13 years old or the minimum legal age in their country of residence, as shown in Figure 6.

Whenever a user attempts to create an account, the app asks for their date of birth. If the user enters an age of 12, the app blocks the registration process. For users aged 13 and 16, accounts are automatically created in "teen" mode. No request for parental consent is made, although Instagram applies different policies based on the age stated. (Figure 7).

User accounts for children under 16 have recently adopted a design that is more focused on protecting children's rights

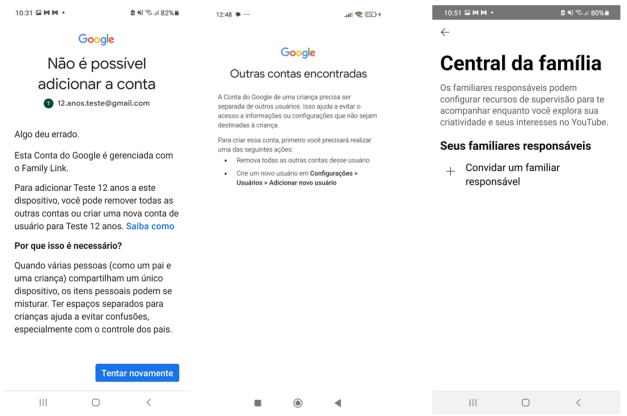


Figure 5. YouTube/Google – Age restrictions and parental supervision for users under 13. Relevant text translated from Portuguese: "The account cannot be added" and "Responsible family members can configure resources for supervision and monitor the use of Google services."

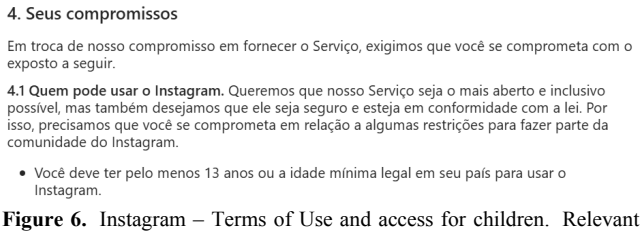


Figure 6. Instagram – Terms of Use and access for children. Relevant text translated from Portuguese: "You must be at least 13 years old or the minimum legal age in your country to use Instagram."



Figure 7. Instagram – Preventing account registration by users under 13. Relevant text translated from Portuguese: "We couldn't create an account for you. We couldn't sign you up for Instagram."

through the *Instagram Teen Accounts* [2]. These accounts are set to private mode by default and can only be switched to public mode with the consent of a registered guardian. Starting at age 16, users can adjust their privacy settings themselves, although supervision by a guardian remains optional.

4.4 TikTok

TikTok sets the minimum age at 13 and states that it removes accounts belonging to users under this age (cf. Figure 8).



Figure 8. TikTok – Terms of Use and Children's Access. Relevant text translated from Portuguese: "The Services are intended exclusively for persons aged 13 or older (subject to any additional limitations established in the Region-Specific Supplemental Terms)."

During registration, the app asks users to enter their date of birth. If an age under 13 is entered, the account creation process is immediately blocked (Figure 9). When a user enters the age of 13, the platform allows them to proceed but displays a notification requesting consent from their parents or guardians (Figure 10). However, the user can simply click *Continue* to skip the verification process. When attempting to register as a user under the age of 13, we observed that the platform restricts the creation of new accounts (even if a new age is entered) unless the app's cache is cleared or the app is reinstalled. This mechanism is intended to prevent attempts to circumvent the rule, although it can be easily bypassed: after reinstalling the app and entering "16 years old," the user can complete the registration without any additional steps.



Figure 9. TikTok – Account creation feature blocking the sign-up process for child users. Relevant text translated from Portuguese: "It looks like you're not eligible for TikTok."

[2] "Introducing Instagram Accounts for Teens" - `https://familycenter.meta.com/br/our-products/instagram/?utm_source=about-meta&utm_medium=referral&utm_content=ig-tech-pg`. Access in 2025-01-08.

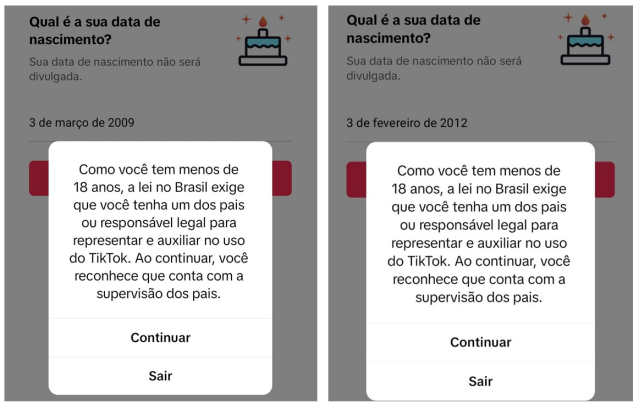


Figure 10. TikTok – Parental consent and supervision notice during account registration. Relevant text translated from Portuguese: "Since you are under 18, Brazilian law requires you to have a legal guardian represent or assist you in registering and using TikTok. By continuing, you acknowledge that your account will be supervised by your parent or guardian."

5 Reflections on Age Assurance: CGI.br Public Consultation

As described in Section 3.2, this analysis draws on the CGI.br public consultation on platform regulation, whose original dataset comprised approximately 1,400 contributions from different sectors and organizations. We searched the consultation report using the predefined Portuguese terms related to age assurance and included 14 excerpts that substantively addressed the topic in the qualitative analysis.

According to participants in the CGI.br consultation on platform regulation, age restrictions are one of the key measures that platforms should implement to protect children and adolescents [Comitê Gestor da Internet no Brasil (CGI.br), 2025]. Establishing appropriate age limits for access to certain services and content can ensure that this audience does not encounter inappropriate material. Despite the definition of 13 as the common minimum age on many platforms, some comments advocate for a total ban on individuals under 18 creating profiles (*"It would be important to prohibit the creation of profiles and the use of social media by individuals under 18 on any platform"*).

Many responses emphasized the limitations of the age restrictions currently in place, a point that was also noted in the previous phase of the study. Participants point out that restriction mechanisms are easily circumvented (*"However, in many cases, it ends up being easy to get around this system, so other measures should be adopted"*). In this way, participants reinforce the need to develop new strategies, as they believe that, otherwise, restrictions based solely on age will remain ineffective. Simply stating in the Terms of Use that there is an age restriction is considered insufficient, especially given the reality of children's access to digital platforms: 60% of children aged 9 to 10 have profiles on platforms such as WhatsApp, Instagram, TikTok, and Discord [Cetic.br and NIC.br, 2024].

To improve the design of age assurance mechanisms, we identified five measures based on our analysis of the data, which are summarized graphically in Figure 11:

- Implement age assurance that **prevent children from misrepresenting their age when creating accounts**.

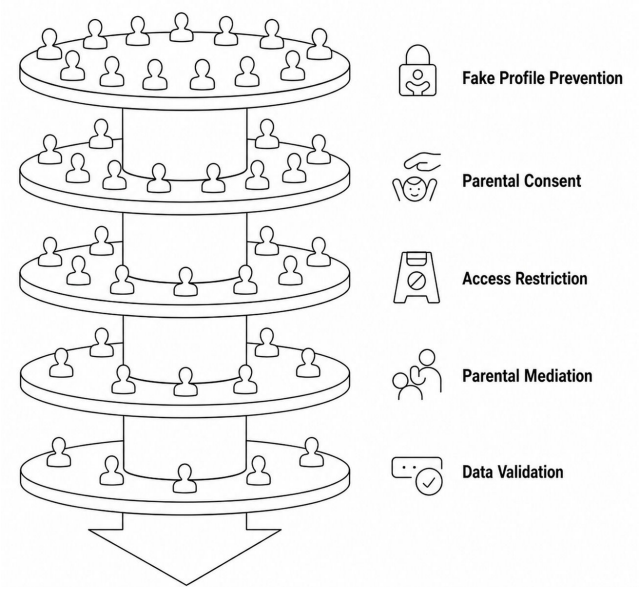


Figure 11. Key recommendations to improve age assurance on platforms.

- Develop mechanisms that **do not rely exclusively on parental consent** for users under 13.
- Ensure that age assurance tools prevent **access to products and services that are illegal for children**.
- **Link user accounts of individuals under 16 to a responsible adult** for parental mediation.
- **Validate user registrations through official databases** (using secure identification methods).

Finally, we noted that participants highlighted a dilemma regarding stricter age assurance: more effective versions of these mechanisms may require companies to authenticate all users. This raises privacy concerns and could encourage tracking and excessive data collection (*"such requirements may inadvertently encourage organizations to collect different types of data and share them across platforms, websites, and services after age assurance"*), contrary to data minimization principles set forth in legislations such as LGPD and GDPR.

6 Systematic Mapping Study Results

The following analyses focus on the subset of 33 studies that compare multiple age assurance categories, selected from the 245 articles included in the systematic mapping study. We first analyzed the demographic profile of the publications in order to map the broader research landscape. In terms of the **publication year**, our analysis of the primary studies (cf. Figure 12) revealed a significant recent increase in the literature on age verification. We identified 13 papers published in 2024 and 9 articles in 2025, in contrast to the period from 2020 to 2023, which ranged between 2 and 3 publications per year. These findings suggest that the debate has recently gained prominence, possibly driven by emerging global regulations, such as European Parliament and Council of the European Union [2022], published in October 2022.

Publications evaluating multiple age assurance categories are distributed across several **disciplinary domains and publication types**, reflecting the highly interdisciplinary nature of the topic. Most of the identified literature consists of jour-

nals and magazines, particularly in the fields of law, ethics, and social sciences, including venues such as the *Stanford Technology Law Review* (S19), *Columbia Journal of Law & Social Problems* (S12), *The International Journal of Children's Rights* (S10), and *Feminist Studies* (S11).

Computer science and cybersecurity are also represented through academic conferences, technical publications, and standards, including venues such as the *USENIX Security Symposium* (S28), *Communications of the ACM* (S25, S26), IEEE publications (S21, S22) and standards (S23), as well as the *Internet Engineering Task Force* (S7).

Beyond traditional academic routes, the research is frequently published through media outlets, think tanks, and official government or policy reports. Venues in this category include the European Parliamentary Research Service (S9), the Australian eSafety Commission (S16), New America (S27), and mainstream platforms like The Wall Street Journal (S18) and CNBC TV18 (S14).

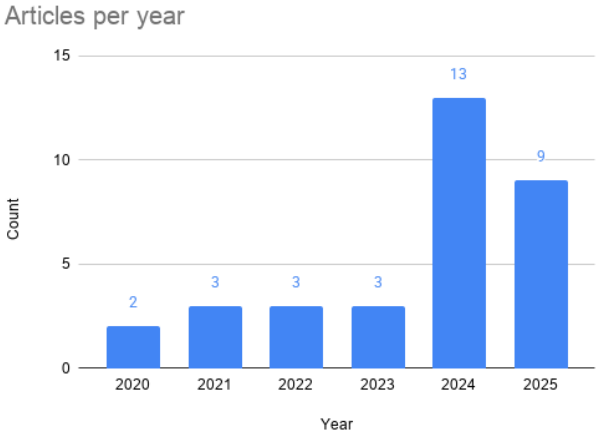


Figure 12. Distribution of the analyzed studies by publication year.

In the following subsections, we analyze specific aspects related to the topic itself, including age assurance categories (6.1), data modalities (6.2), assessment methods, metrics and findings (6.3), and conclusions regarding the effectiveness of existing approaches (6.4). These sections answer RQ3-6.

6.1 Categories

When examining the categories (cf. Figure 13), **document/ID verification** (present in 29 studies) and **biometric methods** (24 studies) emerged as the most frequently analyzed and compared approaches. A second tier includes studies focused on **third-party verification** (16), **self-declaration** (16), and **credit card verification** (14). The frequent presence of self-declaration in comparative studies generally reflects its role as an ineffective baseline against which other age assurance technologies are evaluated.

6.2 Data Modalities

Regarding the modality of the evaluated methods, the analyzed studies examined the specific types of data used by these

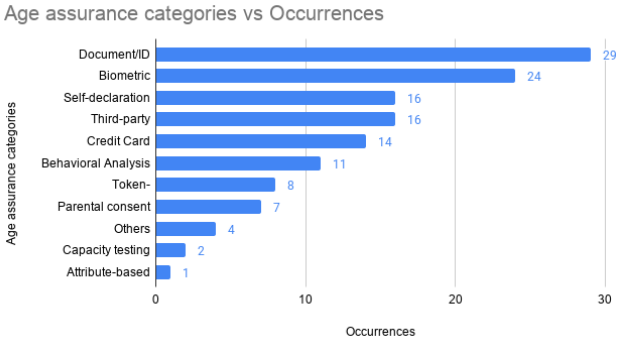


Figure 13. Occurrences of age assurance categories across the studies.

systems to confirm a user's age, which directly map to distinct age assurance categories. The most common data types rely on **physical images and biometric features**, such as static facial photos, facial videos, active liveness checks, and voice recordings, corresponding to the Biometric verification category (e.g., S1, S2, S3, S10, S28, S29).

These methods are frequently evaluated alongside the scanning of **official government documents**, such as passports, birth certificates, and ID cards, which represent the Document/ID Verification category (e.g., S1, S2, S24, S28, S29).

Additionally, some studies explored alternative approaches based on the collection and analysis of **dynamic behavioral data**, including browsing history, typing patterns, and device interactions. These modalities correspond to the Behavioral Analysis category (e.g., S1, S3, S10, S23, S29, S33), which seeks to estimate or verify users' ages through behavioral patterns rather than formal identity documents.

Overall, the identified modalities reinforce the predominance of document-based and biometric approaches, while also revealing a diverse set of inputs, including voice data, browsing behavior, and physical or digital identifiers.

6.3 Evaluation and Findings

The studies evaluating multiple age assurance categories predominantly relied on **empirical, risk-based, and qualitative evaluation frameworks** rather than strictly technical or algorithmic testing. Because many of these works approached the problem from socio-technical or regulatory perspectives, their methodologies frequently involved hands-on audits of existing applications, the creation of simulated child or teenager accounts, and assessments of platforms against established privacy and security standards.

Instead of analyzing source code or model performance alone, researchers focused on the practical implementation of these systems, examining how easily users could bypass age gates, the level of friction introduced during account creation, and the extent to which platform practices aligned with data protection regulations.

For example, the study *"Easy As Child's Play: An Empirical Study on Age Verification of Adult-Oriented Android Apps"* (S28) employed a large-scale empirical framework to evaluate the real-world adoption of age verification mechanisms across the mobile ecosystem. The researchers deployed an automated detection tool to analyze more than 31,000 adult-oriented Android applications, complementing the automated

analysis with manual verification procedures.

Their evaluation measured the prevalence of different verification mechanisms and the detection tool's accuracy through false positive and false negative rates. The results revealed substantial shortcomings: only 3.67% of the analyzed applications implemented any form of age assurance. Among those that did, self-declaration mechanisms were the most common, accounting for nearly 32% of implementations, while biometric verification appeared in fewer than 9% of cases.

Other studies adopted similar practical evaluation frameworks to demonstrate the widespread inadequacy of age assurance systems across different sectors. In *"The digital loophole: evaluating the effectiveness of child age verification methods on social media,"* researchers applied a qualitative framework composed of nine verification checks, including the blocking of disposable email addresses and resistance to browser refresh bypasses, while also mapping the results to IEEE standards. Their findings showed that major social media platforms consistently achieved the lowest levels of verification robustness, whereas financial services demonstrated substantially stricter compliance.

6.4 Effectiveness

The analyzed studies conclude that self-declaration, currently the most widely adopted age assurance method, is ineffective, as children can easily bypass such restrictions. A broader examination of the literature indicates a consensus that there is currently no "silver bullet" technology capable of simultaneously satisfying all necessary requirements. Instead, the literature highlights persistent trade-offs between security, privacy, and inclusivity.

Methods considered technically effective at preventing underage access, such as government ID submission and biometric facial scanning, are frequently criticized for being highly privacy-invasive, vulnerable to data breaches, and structurally exclusionary toward populations lacking formal documentation. Conversely, approaches that preserve privacy and reduce user friction, such as self-declaration or simple tick-boxes, are widely characterized as ineffective mechanisms that minors can easily circumvent.

Taken together, these findings highlight a persistent tension between protecting children from harmful online access and preserving user privacy, while also reinforcing the limitations of many existing age assurance approaches.

6.5 Cross-cutting Gaps in Current Age-Assurance Research

Beyond the findings reported for individual age-assurance categories, data modalities, and evaluation approaches, our mapping study reveals broader gaps in the current research landscape. First, the field appears to be expanding rapidly but remains relatively heterogeneous in terms of disciplinary perspectives, methodological approaches, and objects of evaluation. The studies range from technical assessments of biometric and document-based mechanisms to platform audits, regulatory analyses, and privacy-oriented evaluations. While this diversity reflects the socio-technical nature of age assurance, it also makes direct comparison across studies and approaches difficult.

Second, the evidence indicates a gap between the development or assessment of age-assurance mechanisms and their evaluation under real-world conditions. Some studies examine technical properties (e.g., accuracy or the ability to correctly estimate or verify age), whereas others evaluate practical aspects (e.g., circumvention, user friction, regulatory compliance, or implementation) in existing services. Therefore, technical performance alone provides limited evidence of how effectively a mechanism protects children when deployed by current platforms.

Finally, the literature reveals a recurring separation between robustness and other dimensions relevant to the practical adoption of age assurance. Approaches based on official documents or biometric data may provide stronger barriers against age misrepresentation. At the same time, they raise concerns regarding privacy, accessibility, inclusion, and data protection. Conversely, less intrusive approaches may reduce data collection and user friction while providing weaker protection against circumvention by children or teenagers.

These findings suggest that the maturity of age-assurance research should not be assessed solely via improvements in technical accuracy or robustness, but also through the extent to which evaluation frameworks jointly consider effectiveness, privacy, usability, accessibility, and inclusion in realistic deployment contexts.

7 Discussion

Our findings should be interpreted as a contextual and integrative extension of existing evidence on age assurance rather than as the validation of a new mechanism or evaluation method. By examining previous approaches in the Brazilian context and triangulating the platform evaluation with consultation data and systematic literature evidence, the study highlights how recurring technical limitations and trade-offs manifest within a specific regulatory and child-protection environment.

In this section, we interpret our findings from two complementary perspectives. First, we examine the age assurance mechanisms adopted by digital platforms in light of current child online protection regulations (Section 7.1). Second, we analyze the age assurance methods identified in the literature, representing the current state of the art in digital protection, through a risk-based lens. This perspective assumes that platforms should implement prevention and mitigation measures proportionate to the risks inherent in their products and services, as outlined in the ECA Digital[3]

7.1 Age Assurance Methods on Digital Platforms Through a Regulatory Lens

In Table 3, we summarize the results of the tests conducted on the four platforms, addressing the previously defined guiding questions. YouTube's approach aligns with the concept of "evolving capabilities," which seeks to ensure the inclusion

[3]ANPD. *Mecanismos Confiáveis de Aferição de Idade: Orientações Preliminares*. Brasília, DF, 2026. Available at: https://tinyurl.com/23en83dt

of children based on their level of maturity and social context, under the supervision of responsible adults. In contrast, the approach adopted by the other platforms is more restrictive and exclusionary, preventing children from exploring digital features in a safe and supervised manner. The results also reinforce the arguments of Farthing *et al*. [2021] regarding the complexity of the terms of use and how they are not tailored to this audience's level of understanding.

Overall, Google's approach has proven to be a good example of how to structure age assurance mechanisms. The platform provides clear instructions for parents and guardians to manage children's accounts, restricts access on devices shared with other users, and seeks to create an environment conducive to child development. Variations such as YouTube Kids help minimize risks while promoting the positive use of technology. However, the platform also has limitations. Google does not require mandatory assurance steps or specific settings for the creation of accounts by teenagers, and although YouTube offers supervision mechanisms for this audience, they are neither mandatory nor prominently promoted, which requires proactive action and digital literacy on the part of parents and guardians.

Instagram, on the other hand, does not allow the creation of children's accounts, but offers a recent and specific set of features designed for teenagers. When a teenager's account is created, parental supervision is encouraged through a built-in invitation feature. This kind of feature was also frequently mentioned in the public consultation conducted by CGI.br Comitê Gestor da Internet no Brasil (CGI.br) [2025] because it allows guardians to supervise and restrict children's and teenagers' access to certain content. In this scenario, platforms can take the lead in improving age assurance mechanisms, while families simultaneously contribute to the protection of minors. Thus, a shared responsibility is established to ensure the concept of *"children's rights by design"* Hartung [2020].

TikTok also restricts access to children under the age of 13. Although it allows use by teenagers and offers parental supervision tools through Family Sync [4], the platform lacks features specifically designed for this age group. As a result, teenagers are exposed to a wide range of digital risks. Although TikTok imposes functional restrictions (such as blocking account creation after an age that is not permitted is entered), these measures can be easily circumvented by reinstalling the app.

The platforms analyzed rely on self-reported age as the sole verification method, an approach that is highly susceptible to manipulation. As highlighted in a related study by Eltaher *et al*. [2025], the design of this type of age classification complies with COPPA but shifts the responsibility for age assurance onto the children themselves and their guardians [Federal Trade Commission, 1998]. This reality demonstrates the need for robust legislation requiring the implementation of effective age assurance methods. One alternative currently under discussion, for example, is that companies behind social media platforms (such as the one analyzed in this study) could develop age assurance features using facial recognition Hymas [2024]. However, this approach still poses a risk to data protection, given the use of children's sensitive data. Additionally, it would require a new level of consent (explicit and distinguishable) from guardians, as provided for in the LGPD [Brasil, 2018].

Furthermore, the terms of use of the analyzed platforms are often lengthy and written in complex legal language, making them difficult for both children and their guardians to understand. These characteristics may be interpreted as forms of deceptive design, particularly *Visual Interference* and *Obstruction*. Extensive terms presented with low readability features, such as small fonts, poor visual contrast, or layouts that are difficult to navigate, may contribute to user fatigue and parental exhaustion, increasing the likelihood that users abandon the reading process and become more susceptible to manipulative practices[5].

Although Brazilian law explicitly requires parental consent for children to access digital platforms, not all apps implement practical measures to ensure that parents are aware of their children's or teenagers' online profiles [Brasil, 2018]. On the one hand, Google offers tools such as Family Link, YouTube Kids, and device usage restrictions, as well as clear and accessible instructions for parents to monitor children's access. On the other hand, when it comes to teenagers, the same level of effort is not observed. For this audience, parental controls are optional and must be enabled by the user.

Even though platforms may display notifications requesting parental consent, they do not verify this authorization through direct contact. This is also the case with TikTok and Instagram. This practice reflects the current state of Brazilian legislation on the protection of children's and teenagers' data, since the LGPD does not guarantee the same level of protection for both groups, which makes it easier for platforms to access teens' personal information [Brasil, 2018; Laterça, 2022].

7.2 Mapping Age Assurance Methods in Literature to Child Online Risk Categories

The categories of age verification methods identified in the literature (Section 6) can be interpreted not only from a technical perspective, but also according to the types of online risks they are intended to mitigate. Drawing on the frameworks proposed by Hasebrink *et al*. [2008] and Livingstone and Stoilova [2021], we observed different ways in which age assurance methods may contribute to reducing content, contact, conduct, and contractual/commercial risks for children. However, these mechanisms can simultaneously introduce new and specific risks, particularly regarding privacy, surveillance, and data processing practices.

Self-declaration methods, which are still widely adopted across digital environments such as gaming and adult-content platforms, have been consistently identified as ineffective because they are easily circumvented [Cruz, 2025]. Their limited robustness significantly reduces their ability to prevent children's exposure to *content risks* (e.g., violent or sexual material), *contact risks* (e.g., interactions with strangers), and

[4]Family Sync: `https://support.tiktok.com/pt_BR/safety-hc/account-and-user-safety/family-pairing`. Access in: 2025-01-08.

[5]Types of Deceptive Patterns. `https://www.deceptive.design/types`. Accessed: 2025-01-08.

Table 4. Age restrictions and assurance across platforms.

Question	WhatsApp	Instagram	YouTube	TikTok
Minimum age (Terms)	13+	13+ or legal age	13+ or with a guardian	13+
Requests age?	No	Yes	Yes	Yes
Blocks minors?	N/A	Yes	Yes (parental email)	Yes
Additional verification at 13?	N/A	Teen mode	No	Requires consent
Is it possible to bypass?	N/A	Yes (edit age)	Yes (edit age)	Yes ("Continue")
Additional verification at 16?	N/A	Teen mode	No	Warning if under 13 attempted before
Minimum age visible?	Yes (Terms)	Yes (Terms)	Yes (Terms)	Yes (Terms)

conduct risks (e.g., access to gambling or adult-oriented services). Consequently, these mechanisms frequently operate more as symbolic barriers than as effective protection measures. This limitation has also been recognized in regulatory initiatives. In Brazil, for example, Law No. 15,211/2025, the *Estatuto Digital da Criança e do Adolescente* (ECA Digital), no longer considers self-declaration mechanisms sufficient for age assurance purposes [Brasil, 2025].

Document/ID verification and **biometric** methods potentially offer stronger protection against *conduct* and *content-related risks* by creating more robust barriers to age-restricted services. These mechanisms may reduce children's exposure to inappropriate environments and improve compliance with legal age requirements. However, they simultaneously raise concerns associated with *contractual* or *commercial risks*, since they frequently require the collection and processing of highly sensitive personal data, including government-issued documents and biometric information.

In their turn, **Behavioral** and **inference-based** methods introduce a different trade-off. Instead of relying on explicit identification, they estimate users' age through browsing behavior, interaction patterns, or digital traces. While potentially less intrusive than hard identifiers, such approaches may intensify tracking practices and expand commercial profiling, reinforcing concerns regarding the datafication of children's online activities.

Overall, we observed that no category identified in the literature appears capable of simultaneously maximizing protection while minimizing privacy and inclusion concerns. Our findings suggest that age assurance should not be interpreted exclusively as a technical challenge but as a socio-technical balancing process involving safety, privacy, proportionality, and children's rights.

8 Conclusion

In terms of **contribution**, the empirical platform evaluation reinforces the findings reported by Curley [2020], demonstrating that social media platforms still lack robust age assurance and parental supervision mechanisms for children and adolescents. As a result, existing measures remain relatively easy to circumvent. Furthermore, the contrasting approaches adopted by platforms such as TikTok and Instagram, which primarily restrict children's access, and YouTube, which provides an adapted and supervised environment for younger users, further contribute to the ongoing debate identified by Livingstone and Sylwander [2025] regarding appropriate ages for Internet use and the digital rights of children. In this context, YouTube's approach appears to provide comparatively more extensive mechanisms for balancing inclusion, supervision, and child safety.

Moreover, the evaluation revealed the presence of extensive terms of use containing detailed policies, data protection clauses, usage rules, and other legal provisions. None of the analyzed platforms provided simplified or child-friendly versions of these documents. Among the evaluated services, Google comes closest to addressing this limitation by sending guidance and informational emails to the guardians of child users, although this practice is not consistently implemented across all of its services.

With the exception of WhatsApp, which does not implement age assurance or parental consent mechanisms, the evaluated platforms generally maintain policies aligned with current Brazilian regulations. These platforms either restrict children's access or provide alternative mechanisms and, to some extent, attempt to encourage supervision for adolescent users. Nevertheless, both regulatory frameworks and platform practices still present important gaps that may compromise the effective protection of personal data and the broader digital safety of younger users.

Taken together, this study contributes to the age-assurance literature through three complementary elements: a contextual replication of previous international platform evaluations in the Brazilian context; a systematic synthesis of evidence on age-assurance mechanisms, data modalities, evaluation practices, and reported effectiveness; and the integration of these findings with perspectives from the CGI.br public consultation. This combined analysis highlights persistent tensions between child protection, robustness, privacy, and inclusion.

To address these challenges and mitigate the negative impacts associated with social media use, future policies should establish clearer definitions of the roles and responsibilities of both digital service providers and adults responsible for minors [Farthing *et al*., 2021]. At the same time, these regulations should provide more concrete guidance regarding the collection, processing, and protection of children's personal data. Regulators must also seek an appropriate balance between normative principles such as child welfare and autonomy, a central challenge in the development of frameworks such as *Child Rights by Design*[6], which aim to protect young users while respecting cross-cultural and social differences.

The systematic mapping revealed a rapidly expanding

[6] 5Rights Foundation. `https://childrightsbydesign.5rightsfoundation.com/`. Accessed: 2025-01-08.

and highly interdisciplinary research landscape around age assurance. It identified document-based and biometric approaches as the most frequently studied mechanisms. The review also demonstrated that current research extends beyond purely technical solutions, involving legal, ethical, and policy-oriented perspectives. Furthermore, our findings indicate that self-declaration mechanisms, despite being the most widely deployed approaches in practice, are consistently described as ineffective and easily circumvented. At the same time, methods considered more robust, such as document-based and biometric verification, introduce important concerns related to privacy, accessibility, and inclusion.

The integration of the mapping findings with the empirical platform evaluation and the CGI.br consultation enables us to interpret age assurance mechanisms from a risk-based perspective centered on child online protection. This analysis shows that these mechanisms may simultaneously reduce exposure to harmful environments while creating new risks involving surveillance, profiling, and personal data processing. Therefore, our findings reinforce the need to understand age assurance as a broader socio-technical challenge rather than solely as a technical verification problem.

This study presents **limitations** that also suggest opportunities for **future work**. First, the platform evaluation was conducted based on services, configurations, and regulatory contexts specific to Brazil. Age assurance mechanisms may vary across countries due to differences in legislation and platform policies. Google, in particular, presents substantial variations in age-related restrictions and supervision features across regions. This creates opportunities for comparative studies examining how age assurance and child protection mechanisms are implemented under different regulatory contexts.

Another limitation concerns the data collection process, which was conducted by a single researcher. Although the results and interpretations were subsequently reviewed and discussed by two authors, this may reduce the reliability and reproducibility of the evaluation process. Although this procedure provided an additional layer of analysis, the absence of independent parallel coding may reduce reliability and reproducibility of our study. Future replications should involve independent evaluators during platform testing and thematic coding, enabling the use of inter-rater agreement measures such as Cohen's Kappa when methodologically appropriate.

In addition, the empirical analysis relied primarily on two sources of evidence: platform documentation and the creation of test accounts. The inclusion of additional sources, such as interviews with industry professionals or technical analyses of platform ecosystems, could enable stronger triangulation and provide a broader understanding of age assurance practices.

The systematic mapping study also presents some limitations related to the scope of the review. The selected timeframe (2020–2025) may have excluded earlier studies relevant to the historical evolution of age assurance technologies. The mapping was also restricted to English-language publications across the six selected digital libraries. This introduces potential language and database coverage bias and may have underrepresented research disseminated locally in Brazil. Future extensions should therefore incorporate Portuguese search terms and regional sources, such as SBC OpenLib. In addition, the review did not conduct a dedicated search for grey literature beyond the selected digital libraries, which may have limited the coverage of government reports, policy documents, and technical publications relevant to the implementation and regulation of age assurance mechanisms. Hence, in future work we aim to compare identical platform configurations and age-assurance flows across jurisdictions, particularly Brazil under the LGPD, ECA Digital and European jurisdictions under the GDPR/DSA framework, to examine how regulatory contexts influence implementation and robustness.

In upcoming studies we also intend to incorporate these additional sources, including materials produced by nongovernmental organizations (NGOs) dedicated to protecting children and adolescents online, such as Alana Institute and SaferNet, both from Brazil.

Declarations

Authors' Contributions

Conceptualization: George Valença.

Methodology: André de Andrade Theodoro, George Valença, and Átila Rodrigues.

Investigation: André de Andrade Theodoro and Átila Rodrigues.

Data Curation: André de Andrade Theodoro and Átila Rodrigues.

Formal Analysis: André de Andrade Theodoro, George Valença, and Átila Rodrigues.

Writing - Original Draft: André de Andrade Theodoro and George Valença.

Writing - Review & Editing: André de Andrade Theodoro, George Valença, and Átila Rodrigues.

Supervision: George Valença.

All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Availability of data and materials

The datasets generated and analyzed during the current study will be made available upon reasonable request to the authors.

Use of Artificial Intelligence

Google NotebookLM was used as an AI-assisted tool during the qualitative analysis to support the thematic organization of the excerpts collected from the CGI.br public consultation (cf. Section 3.2). The interpretation and validation of the resulting categories remained authors' responsibility.

References

Albuquerque, N., Valença, G., and Falcão, T. P. (2024). Investigating manipulative design on social media platforms-the case of kidinfluencers. *Journal on Interactive Systems*, 15(1):860–874. DOI: 10.5753/jis.2024.4271.

ANPD (2026). Age assurance mechanisms. Technology radar, n.5, ANPD, Brasília, DF. Available at: https://www.gov.br/anpd/pt-br Accessed: 2026-05-07.

Brasil (1990). Lei nº 8.069, de 13 de julho de 1990: Estatuto da criança e do adolescente. Available at: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm.

Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018. lei geral de proteção de dados pessoais (lgpd). Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709compilado.htm.

Brasil (2025). Lei nº 15.211, de 17 de setembro de 2025: Estatuto digital da criança e do adolescente. Available at: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm.

Carvalho, R. G. L. and Marques-Neto, H. T. (2024). Crianças e propagandas no TikTok: identificando publicidade infantil na rede social TikTok. In *Proceedings of the 30th Brazilian Symposium on Multimedia and the Web (WebMedia 2024)*, pages 98–105. Sociedade Brasileira de Computação. DOI: 10.5753/webmedia.2024.242912.

Cetic.br (2026). Estudo inédito mapeia práticas de aferição de idade em serviços digitais no brasil. Available at: https://cetic.br/pt/noticia/estudo-inedito-mapeia-praticas-de-afericao-de-idade-em-servicos-digitais-no-brasil/ Accessed: 2026-09-14.

Cetic.br and NIC.br (2024). Tic kids online brasil 2024: principais resultados. Technical report, Núcleo de Informação e Coordenação do Ponto BR (NIC.br). Available at: https://cetic.br/media/analises/tic_kids_online_brasil_2024_principais_resultados.pdf Accessed: 2026-09-14.

Coelho, R. R. and de Oliveira, J. (2021). How twitter has been used for share pedophilia content in 2020. In *Proceedings of the Brazilian Symposium on Multimedia and the Web*. 27 September 2021. DOI: 10.1145/3470482.3479473.

Comitê Gestor da Internet no Brasil (CGI.br) (2025). Diálogos cgi.br: Consulta sobre regulação de plataformas digitais. Available at: https://dialogos.cgi.br/documentos/debate/consulta-plataformas/ Accessed: 2026-09-14.

Cruz, M. F. d. (2025). O enriquecimento de dados de crianças e adolescentes na regulamentação das plataformas de mídia social: entre a proteção da privacidade e os desafios regulamentares. Trabalho de Conclusão de Curso (Graduação em Direito), Universidade Federal de Santa Catarina. Available at: https://repositorio.ufsc.br/handle/123456789/266677.

Curley, C. (2020). 2020 technical report: A review of age verification mechanism for 10 social media apps. *CyberSafeIreland*. DOI: 10.21427/n1ja-1626.

Eltaher, F., Gajula, R. K., Miralles-Pechuán, L., Thorpe, C., and McKeever, S. (2025). The digital loophole: Evaluating the effectiveness of child age verification methods on social media. In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP)*, volume 2, pages 213–222. SciTePress. DOI: 10.5220/0013248300003899.

European Parliament and Council of the European Union (2022). Regulation (eu) 2022/2065 of the european parliament and of the council of 19 october 2022 on a single market for digital services and amending directive 2000/31/ec (digital services act). Available at: http://data.europa.eu/eli/reg/2022/2065/oj Accessed: 2026-09-14.

Faraz, A. *et al*. (2022). Child safety and protection in the online gaming ecosystem. *IEEE Access*, 10:115895–115913. DOI: 10.1109/ACCESS.2022.3218415.

Farthing, R. *et al*. (2021). Age appropriate digital services for young people: Major reforms. *IEEE Consumer Electronics Magazine*, 10(4):40–48. DOI: 10.1109/MCE.2021.3053772.

Federal Trade Commission (1998). Children's online privacy protection rule (coppa). Available at: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa Accessed: 2025-07.

GDPR.info (2016). Gdpr information portal. Available at: https://gdpr-info.eu/ Accessed: 2025-07.

Hartung, P. (2020). The children's rights-by-design standard for data use by tech companies. Good governance of children's data project, issue brief no. 5, UNICEF Office of Global Insight and Policy. Available at: https://www.unicef.org/innocenti/reports/childrens-rights-design-standard-data-use-tech-compar Accessed: 2026-09-14.

Hasebrink, U., Livingstone, S., Haddon, L., and Ólafsson, K. (2008). Comparing children's online opportunities and risks across europe: Cross-national comparisons for eu kids online. Deliverable d3.2, 2nd edition, EU Kids Online, London School of Economics and Political Science. Available at: https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/reports-and-findings Accessed: 2026-09-14.

Hymas, C. (2024). Social media firms to be forced to 'drive out' under-age users. Available at: https://www.telegraph.co.uk/news/2024/12/22/social-media-firms-to-be-forced-to-drive-out-under-a Accessed: 2025-01-08.

Jarvie, C. and Renaud, K. (2024). Online age verification: Government legislation, supplier responsibilization, and public perceptions. *Children*, 11(9):1068. DOI: 10.3390/children11091068.

Kemp, S. (2025). Digital 2025: Global overview report. Available at: https://datareportal.com/reports/digital-2025-global-overview-report Accessed: 2026-09-14.

Laterça, P. (2022). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Obliq Press, Rio de Janeiro, RJ. Available at:https://somos.itsrio.org/livro-privacidade-e-protecao-de-dados-de-criancas.

Livingstone, S. and Stoilova, M. (2021). The 4cs: Classifying online risk to children. *Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE – Children Online: Research and Evidence*, page 14. DOI: 10.21241/ssoar.71817.

Livingstone, S. and Sylwander, K. R. (2025). There is no right age! the search for age-appropriate ways to support chil-

dren's digital lives and rights. *Journal of Children and Media*, 19(1):6–12. DOI: 10.1080/17482798.2024.2435015.

Mascheroni, G. (2020). Datafied childhoods: Contextualising datafication in everyday life. *Current Sociology*, 68(6):798–813. DOI: 10.1177/0011392118807534.

Ngai, E. W. T., Tao, S. S. C., and Moon, K. K. L. (2015). Social media research: Theories, constructs, and conceptual frameworks. *International Journal of Information Management*, 35(1):33–44. DOI: 10.1016/j.ijinfomgt.2014.09.004.

Pasquale, L., Zippo, P., Curley, C., O'Neill, B., and Mongiello, M. (2022). Digital age of consent and age verification: Can they protect children? *IEEE Software*, 39(3):50–57. DOI: 10.1109/MS.2020.3044872.

Petersen, K., Vakkalanka, S., and Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, 64:1–18. DOI: 10.1016/j.infsof.2015.03.007.

Slonje, R., Smith, P. K., and Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. *Computers in Human Behavior*, 29(1):26–32. DOI: 10.1016/j.chb.2012.05.024.

Staksrud, E. and Livingstone, S. (2009). Children and online risk: Powerless victims or resourceful participants? *Information, Communication & Society*, 12(3):364–387. DOI: 10.1080/13691180802635455.

Theodoro, A. and Valença, G. (2025). Entre o acesso e a proteção - um estudo sobre verificação de idade e segurança infantil em plataformas digitais. In *Proceedings of the 31st Brazilian Symposium on Multimedia and the Web*, pages 211–219, Porto Alegre, RS, Brasil. SBC. DOI: 10.5753/webmedia.2025.16050.

Table 5. Appendix A: Analysis of many AV categories

ID	Paper information
S1	Sas M., Mühlberg J. T. Trustworthy age assurance. The Greens Cluster: Social & Economy, Location: The European Parliament. 2024.
S2	Eltaher F., et al. The digital loophole: evaluating the effectiveness of child age verification methods on social media. Technological University Dublin. 2025.
S3	Jarvie C., Renaud K. Are you over 18? A snapshot of current age verification mechanisms. 2021 Dewald Roode Workshop. 2021.
S4	Williams R. S., et al. Age verification and online sales of little cigars and cigarillos to minors. Tobacco regulatory science. 2020.
S5	Van Der Hof S. Age assurance and age appropriate design: what is required? London School of Economics and Political Science, Parenting for a Digital Future. 2021.
S6	Holland J. Age Verification in the Crosshairs: How NetChoice v. Bonta Complicates Legislators' Ability to Protect Children Online. University of Chicago Law Review Online. 2024.
S7	Celi S., et al. Private and Decentralized Age Verification Architecture. Internet Engineering Task Force. 2025.
S8	Radtke T. Mandatory Age Verification for Online Services under GDPR—The protection of children according to data protection law in the light of EDPB's Binding Decision regarding TikTok. Computer Law Review International. 2023.
S9	Del Mar N. A. M. Online age verification methods for children. European Parliamentary Research Service. 2023.
S10	Livingstone S., et al. Children's Rights and Online Age Assurance Systems. THE INTERNATIONAL JOURNAL OF CHILDREN'S RIGHTS. 2024.
S11	Colliver S. Porn vilification and age verification: Regulating online pornography and sex work. Feminist Studies. 2024.
S12	Anduze D. S. Obscenity Revisited: Defending Recent Age-Verification Laws Against First Amendment Challenges. Columbia Journal of Law & Social Problems. 2024.
S13	Köhler-Dauner F., et al. Digital child protection in social networks: age verification and age-tiered regulation in Europe. Springer, Child and Adolescent Psychiatry and Mental Health. 2025.
S14	Bhushan G. V. KYC for children's age verification—will this be a misguided missile in child protection. CNBC TV18. 2024.
S15	Murray A., et al. Cyber risk, privacy, and the legal complexities of age verification for adult content platforms. Issues in Information Systems. 2025.
S16	eSafety Commission. Age verification roadmap consultations (2022). Australian eSafety Commission. 2022.
S17	Stardust Z., et al. QUT Digital Media Research Centre submission in response to the eSafety Commission call for evidence regarding age verification and restricted access systems. Queensland University of Technology. 2021.
S18	Renaud K. Why age verification is so difficult for websites. The Wall Street Journal. 2022.
S19	Goldman E. The "Segregate-and-Suppress" Approach to Regulating Child Safety Online. Stanford Technology Law Review. 2025.
S20	Kishk Y. A. State-Based Online Restrictions: Age-Verification and the VPN Obstacle in the Law. International Journal of Law, Ethics, and Technology. 2024.
S21	Pasquale L. Digital Age of Consent and Age Verification: Can They Protect Children? IEEE Software. 2022.
S22	Adib A. Improvising Age Verification Technologies in Canada: Technical, Regulatory and Social Dynamics. 2023 IEEE International Humanitarian Technology Conference (IHTC). 2023.
S23	IEEE. IEEE Standard for Online Age Verification. IEEE Std 2089.1-2024. 2024.
S24	Jamaludin A. Age verification regulation in social media platform usage: Preventive measures against online child sexual violence. Jurnal Bina Mulia Hukum. 2024.
S25	Grimmelmann J. The Return of Age Verification Laws. Commun. ACM, Communications of the ACM, Volume 67, Issue 5. 2024.
S26	Scheffler S. Age Verification Systems Will Be a Personal Identifiable Information Nightmare. Commun. ACM, Communications of the ACM, Volume 67, Issue 7. 2024.
S27	Forland S., et al. Age Verification: The Complicated Effort to Protect Youth Online. New America. 2024.
S28	Yao Y., et al. Easy As Child's Play: An Empirical Study on Age Verification of Adult-Oriented Android Apps. 34th USENIX Security Symposium (USENIX Security 25). 2025.
S29	van der Hof S. Mapping age assurance typologies and requirements. EUROPEAN COMMISSION. 2024.
S30	Lin Y. V., et al. Carded by the Internet: Measuring User Responses to Online Age Assurance Mechanisms. USENIX SOUPS Poster. 2025.
S31	Xiao L. Y. Video Game Age Rating, Age Assurance, and Identity Verification Policy Implementation in Mainland China: Content Analysis of Popular iPhone Games. Open Science Framework. 2025.
S32	Pasquale L., Zippo P. A review of age verification mechanism for 10 social media apps. CyberSafe Ireland. 2020.
S33	Khalid Ranjha H. Children and the Digital Environment: Best Interests, Age Assurance, and Free Expression. Social Science Research Network. 2025.