Evaluating Parental Readiness to Manage Children's Privacy Across Social Media Platforms

Mykaele F. Abreu, Eduardo K. Viegas, Altair O. Santin, Jhonatan Geremias

***Abstract*— Children's widespread use of digital platforms has intensified concerns about the adequacy of privacy protections. Current legislation places the responsibility for managing children's privacy on parents and guardians, assuming they possess the necessary knowledge to make informed decisions. In light of this, this work assesses parental maturity in managing children's privacy on social platforms. First, we identify the main privacy attributes relevant to children's online data protection by analyzing existing laws and regulations, including the GDPR, COPPA, and LGPD. This phase establishes a regulatory baseline for evaluating parental responsibilities and expectations. In the second phase, we surveyed 77 parents and guardians to assess their level of maturity in managing privacy-related measures and to evaluate how effectively they can protect their children's data in digital environments. Our results reveal a significant discrepancy between perceived and actual knowledge, suggesting that many parents may not be adequately prepared to fulfill the role expected by current regulations. These findings support the need for clearer policies and a shared responsibility model between platforms and guardians to ensure child privacy.**

I. Introduction

Several legal frameworks have been established in recent years to protect personal data, with specific provisions for children [1]. Notable examples include the General Data Protection Regulation (GDPR) [2] in Europe, the General Data Protection Law (LGPD) [3] in Brazil, and Children's Online Privacy Protection Act (COPPA) [4] in the United States. Enforced since 2018, the GDPR unifies and strengthens data protection across the EU. The LGPD, in effect since 2020, governs personal data processing in Brazil. COPPA focuses specifically on protecting children's online data. Both regulations seek to ensure responsible data collection, handling, and storage practices for individuals of all ages, including minors [5]. In contrast, COPPA, enacted in 1998, focuses on protecting the privacy of children under the age of 13 by granting parents greater control over the information websites and applications may collect from their children. It also addresses concerns related to targeted marketing and encourages awareness of online safety.

Children's privacy has become increasingly critical as the use of online technologies and mobile devices by minors continues to grow. This rising exposure to digital environments has normalized the collection and processing of their data by service providers, while simultaneously exposing them to significant privacy risks [6]. Children are considered inherently vulnerable due to their ongoing physical and cognitive development, limited decision-making capacity, and psychological and emotional fragility [7]. International and national frameworks establish special rights for children to address this vulnerability, emphasizing the need for active supervision by parents, guardians, and caregivers to safeguard their privacy.

Their role is essential in ensuring children understand the risks of data sharing and are protected from potential threats [8]. However, a lack of transparency in social network policies and data handling practices hinders their decision-making. A key issue is the varying degree of maturity among parents and guardians, defined here as their capacity to recognize online risks and apply effective privacy measures [9]. The absence of standardization in data protection mechanisms for minors compounds this challenge. Regulations such as the LGPD, COPPA, and GDPR differ in defining who qualifies as a minor, leaving room for legal ambiguity and limiting enforcement [10]. Many digital service providers fail to implement mechanisms like robust parental consent verification or stricter security controls. Moreover, little is known about how parents perceive these mechanisms or their ability to utilize them effectively. Addressing this gap requires a deeper understanding of parental maturity regarding digital privacy and the development of educational strategies to enhance children's online safety.

A significant challenge in current regulatory frameworks is the assumption that parents or guardians are primarily responsible for safeguarding their children's privacy while using social platforms [11]. This presumes they possess adequate knowledge of digital privacy issues and understand how regulations, such as the GDPR, COPPA, and LGPD, define and enforce children's data protection [12]. However, this expectation often overlooks the varying levels of digital literacy and awareness among parents, who may struggle to comprehend complex privacy settings, platform policies, and legal requirements. Despite the critical role of parental involvement, the literature still lacks a comprehensive understanding of parental maturity in managing children's digital privacy, specifically, their ability to recognize risks, interpret regulatory obligations, and implement effective protective measures.

Contribution. In light of this, this work evaluates parental maturity in managing children's privacy on social platforms. The study is carried out in two phases. In the first phase, we identify the key privacy attributes critical to protecting children's online data by analyzing major laws and regulations, including the GDPR, COPPA, and LGPD. It establishes a

[1]Mykaele F. Abreu, Eduardo K. Viegas, Altair O. Santin, and Jhonatan Geremias are with the Graduate Program in Computer Science (PPGIa) at Pontifical Catholic University of Parana (PUCPR), Brazil {mykaele.abreu, eduardo.viegas, santin, jhonatan.geremias}@ppgia.pucpr.br

regulatory baseline for assessing parental responsibilities and expectations. In the second phase, we design and conduct a structured survey with 77 parents and guardians to assess their maturity as defined by their awareness of implementing privacy-related measures. The survey explores multiple dimensions, such as their knowledge of legal definitions, their perception of platform responsibilities, their understanding of data handling practices, and their attitudes toward the commercial use of children's data. In summary, the main contributions of this work are:

- We define a structured set of privacy attributes based on current legal and regulatory frameworks to establish a baseline for evaluating parental responsibilities in safeguarding children's online data;
- We assess parental maturity through a comprehensive survey, analyzing parents' awareness, understanding, and practical ability to manage privacy settings and protect their children's data on social platforms. Our findings reveal that most parents lack sufficient awareness to effectively manage their children's privacy;

II. Related Works

The assessment of privacy maturity is typically conducted through surveys using structured questionnaires [13]. These tools help evaluate individuals' understanding, attitudes, and behaviors regarding privacy practices, enabling researchers to identify gaps in awareness and areas for improvement [14], [15]. For example, A. L. Salgado *et al.* [16] assessed the users' expectations on privacy through a survey with 50 individuals. The authors identified that most individuals are not aware of security issues associated with privacy in the automotive context. O. Albuquerque *et al.* [5] aimed to identify the privacy requirements associated with children-oriented applications. The authors highlighted the challenges associated with defining adequate parental control mechanisms and the lack of applicable proposals. M. J. Amon *et al.* [12] investigates the parent privacy concern while posting their young children's photos on social media. The survey conducted with over 400 individuals showed that parents do not usually care about privacy risks associated with their child's data. S. Thammaratchuchai *et al.* [17] investigated the parents' awareness of child privacy on social media. The authors applied a questionnaire to 96 individuals through a Likert scale. The results indicated that parents are moderately aware of the negative effects of sharing their children's activities on social media. Unfortunately, the study overlooked the parents' maturity in managing child privacy and the associated regulations. R. Sun *et al.* [18] investigated the privacy issues of children-oriented mobile apps. The authors revealed that up to 80% of Family apps use trackers that are not allowed for children-oriented applications. A. Ekambaranathan *et al.* [19] surveyed 20 children's app developers to investigate the challenges of designing privacy-friendly apps. The results revealed that fully adhering to privacy concerns may involve financial risks, as implementing comprehensive privacy protections often requires significant investment in technology, personnel, and ongoing compliance efforts.

III. Assessing Parental Maturity in Managing Child Privacy

To address such a challenge, our proposal aims to assess parental maturity in managing children's privacy on social platforms. The proposal is conducted twofold.

The first step involves identifying the main privacy attributes outlined in major regulatory frameworks, including the GDPR, COPPA, and LGPD. We analyze how these regulations define children's data protection rights, the responsibilities assigned to parents or guardians, and the obligations imposed on digital service providers. This analysis serves as the foundation for identifying the critical aspects of privacy that parents should understand and manage in digital environments.

In the second step, we design and implement a structured survey to evaluate parental maturity. The survey uses a Likert scale to capture the extent of parents' awareness of privacy-related concepts and regulatory principles. Social platforms are adopted as the primary use case due to their relevance in children's digital lives. The survey is structured to draw connections between parents' self-reported knowledge of data protection regulations and their familiarity with the privacy policies and terms of use of the platforms their children engage with. This approach allows us to identify gaps in understanding and areas where further educational strategies may be needed.

A. Privacy Attributes

To define the privacy attributes relevant to our study, we first analyzed three major regulatory frameworks: COPPA, GDPR, and LGPD. These regulations outline specific requirements for collecting, processing, and protecting children's personal data. Despite differences in scope and definitions—such as varying age thresholds for defining a child—they share common principles that aim to safeguard children's privacy in digital environments.

This legal review identified key aspects such as the definition of personal and sensitive data, the role and requirements for parental or guardian consent, and the implications of processing children's data without proper authorization. For instance, while GDPR requires parental consent for data processing of subjects under 16 (with allowances for national adjustments), COPPA applies to children under 13 and demands verifiable parental consent. LGPD originally mirrored this need but was recently revised to allow broader bases for processing, provided that the child's best interests are upheld. These variations highlight the complexity of enforcing consistent privacy protections globally and the need for harmonized compliance approaches.

Beyond consent and age thresholds, we also examined other critical privacy attributes mandated by these laws. These include transparency in data usage—requiring companies to clearly explain how data is collected, stored, and shared—along with the right to access and correct

TABLE I: Key privacy aspects defined by current regulations and legislation on child privacy (GDPR, COPPA, LGPD).

Privacy Aspect	Definition
Personal Data	Personal data is any information related to an identified or identifiable natural person. Sensitive personal data is that which is tied to the identification of the person.
Definition of a Child	Define ages that require parental or guardian consent for data protection purposes.
Parental or Guardian Consent	The processing of personal data must be carried out with the parents' or legal guardians' consent.
Transparency in the Use of Information	Collected and processed information must be available to parents, indicating the data collected, its intended use, and user access for procedures such as correction or deletion.
Limited Purpose	Children's data can only be collected for specific, explicit, and legitimate purposes.
Data Minimization	Data collection must be limited to the minimum necessary to achieve the purpose.
Parental Consent for Data Collection	Data may only be collected with parents' or guardians' consent.
Notice of Data Processing	Notices of data processing must be simple, clear, and accessible.
Right to Review Provided Data	At any time, the data may be reviewed or deleted.
Privacy by Design	Organizations must consider and incorporate privacy measures during product and service development.
Confidentiality of Information	Companies must protect the shared personal data and ensure that any third party they share it with provides the same level of protection.

information, and the principle of data minimization, which limits the collection of unnecessary data. Additionally, we considered the importance of privacy-by-design, which calls for integrating data protection mechanisms from the earliest stages of system development. All three laws emphasize these principles as necessary to build trust and ensure responsible data stewardship.

By synthesizing these elements, we consolidated a unified set of privacy attributes representing the foundational legal and ethical standards for child data protection. These attributes serve as the evaluation metrics for our study's assessment model, enabling us to evaluate how well parents understand and apply privacy principles in the context of social platforms. Table I presents a consolidated set of privacy aspects derived from major data protection regulations concerning children. It defines personal and sensitive data, highlights the age thresholds that require parental or guardian consent, and the need for transparency in how data is collected, used, and accessed. Key principles include limited purpose, data minimization, and the necessity of clear, accessible notices about data processing [20]. The framework also emphasizes the right to review or delete data, the importance of privacy-by-design from the outset of system development, and the obligation to maintain the confidentiality of shared information, including when data is transferred to third parties.

B. Maturity Model Assessment

In this study, the Security Awareness Maturity Model (SANS), which was originally designed to assess organizational security awareness, will be adapted to evaluate parents' maturity levels in protecting their children's privacy and digital safety. A questionnaire will be used to assess parents' knowledge, perceptions, and behaviors regarding online privacy to identify gaps and tailor interventions. The SANS model comprises five levels, from non-existent awareness to a deeply embedded culture of security, which has been repurposed in this context to reflect parental engagement with digital privacy.

The proposed parental maturity model will assess awareness and actions taken to safeguard children's personal data on digital platforms. At Level 1, parents are unaware of online risks and take no protective actions. Level 2 reflects minimal awareness with little practical application. At Level 3, there is a moderate understanding, with sporadic protective measures such as adjusting privacy settings or offering basic guidance to children. At Level 4, parents consistently implement proactive privacy practices and engage in ongoing education with their children. Level 5 represents parents who are not only informed and protective but also advocate for children's digital rights.

The goal is to evaluate their maturity level concerning core privacy principles such as consent, transparency, data minimization, and the right to review data (see Table I. A questionnaire was distributed to parents or guardians to conduct this evaluation (later presented at Section IV-A). Based on their responses, a maturity level will be assigned, reflecting their understanding and involvement in protecting their children's personal information. The questions cover aspects such as age for consent, parental consent requirements, understanding of personal data and its usage, data minimization practices, the right to review data, data processing transparency, and confidentiality principles.

To ensure a comprehensive and credible assessment, the questionnaire was structured to evaluate each privacy aspect using two complementary types of questions. The first type focuses on the respondent's ***self-declared knowledge***, capturing their perception of what they know or believe about a given privacy topic. The second type targets their ***measured knowledge***, assessing whether their understanding aligns with accurate practices, definitions, or legal requirements. This approach identifies potential gaps between perceived and actual knowledge, offering a more reliable view of parents' maturity regarding children's digital privacy. Table II presents the complete set of questions and the specific privacy aspects each one aims to validate.

IV. Survey-Based Assessment

Our conducted survey aims at answering the following Research Questions (RQs):

- *(RQ1) What is the self-declared knowledge of parents on managing child privacy on social platforms?*
- *(RQ2) Does the measured knowledge of parents on managing child privacy significantly differ from their*

TABLE II: Survey questions to assess the parental maturity in managing child privacy on social platforms. We measure *self-declared knowledge* and compare it with *measured knowledge* answers on a Likert scale.

Privacy Attribute	Self-declared Knowledge Questions	Measured Knowledge Questions
Age definition	How would you rate your knowledge of the definition of a '*child*' according to applicable regulations?	Considering the excerpt from the terms of use of a social network: "*...You must be at least 13 years old to use the Service...*" How much do you believe this statement complies with the regulations?
Consent	How would you rate your knowledge of the legal age requirements and parental authorization rules, particularly in cases where children create accounts without parental consent?	Considering the excerpt from the terms of use of a social network: "*...If you are a parent or legal guardian of a user under the age of 18, by allowing your child to use the Service, you are subject to the terms of this Agreement and are responsible for your child's activities on YouTube...*", how much do you agree that you are aware and understand the terms of use of the social network your child uses?
Data transparency	How would you rate your level of agreement with the statement: "*I feel adequately informed about how my child's data is collected and used by social networks*"?	How much do you agree that it is appropriate for social networks to use children's data to assess ad effectiveness and deliver personalized advertising based on their interests and activities on the platform?
Data minimization	How much do you agree with the amount of data social networks collect from children?	Considering this excerpt from a social network: "*By creating an account on a social network and accepting the Terms of Use, you agree to the collection of information about your approximate location, including SIM card and/or IP address-based data*." This implies that you are authorizing the availability of information such as the child's current location. What is your level of agreement with collecting location data when accepting the Terms of Use?
Revision right	How would you rate your awareness of whether social networks allow the revision (updating) of your child's data on the platform at any time, as required by law?	This excerpt from a social network mentions: "*including the right to access, delete, update, or correct your data, be informed about data processing, file complaints with authorities, and potentially other rights*." This means you can, for example, modify the child's data, such as age and interests, at any time. If you needed to review the child's data to stop targeted ads, what is your level of knowledge about how to make this change?
Limited use	How would you rate the transparency of the social network your child uses regarding how their personal information is collected, used, and shared?	This excerpt from the terms of use of a social network mentions: "*We may also disclose your information to third parties: if we sell or buy any business or asset*" This means the child's information may be shared with other companies without your prior knowledge and approval. What is your level of agreement with the practice of disclosing your information to third parties?
Data confidentiality	How would you rate your agreement with how social networks use data to deliver targeted ads to children?	By accepting the Terms of Use on a social network, you agree to the collection of information about the videos the child watches, search terms, and other interactions with content and ads in the app. This means the social network can display ads based on the child's video history, but it is not responsible for the data collection by other websites visited after clicking on these ads. What is your level of agreement with this practice?
Data treatment	How would you rate your agreement with the clarity and transparency of the data processing notice provided by social networks regarding children's information?	By accepting the Terms of Use of a social network, do you feel informed about the following topics: what information is collected, how the information is used, where it is stored, your rights and choices, the security of your information, and how long your information is retained. What is your level of agreement on how clear this information was when you created the account?

self-declared counterpart?

- *(RQ3) Can parents manage child privacy on social platforms?*

A. Survey Application

The survey was conducted through an online questionnaire designed to assess parents' and guardians' understanding and practices regarding children's digital privacy. In addition to the questions shown on Table II, we also applied profile-related questions to identify the respondent's gender and age profile. Before distribution, the university's ethics committee reviewed and approved the questionnaire to ensure compliance with ethical research standards. The survey was made available via a public link and disseminated through social networks and messaging platforms to reach diverse respondents. A total of 77 individuals completed the questionnaire, providing their level of awareness, involvement, and actions taken to protect their children's data on digital platforms. The collected responses were then analyzed to determine each participant's maturity level, based on their knowledge and behaviors aligned with key privacy principles.

Figure 1 overviews the profile of the survey respondents. The data analysis revealed that most respondents were between 26 and 45 years old (86%), with a high level of education—83% had completed higher education. This profile indicates a group with reasonable access to

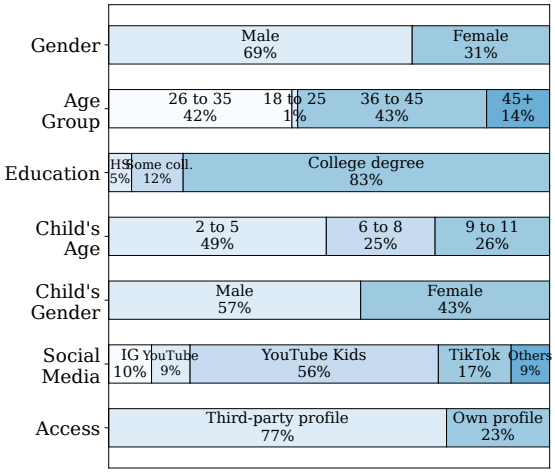

Fig. 1: Overview of the survey respondents' profile.

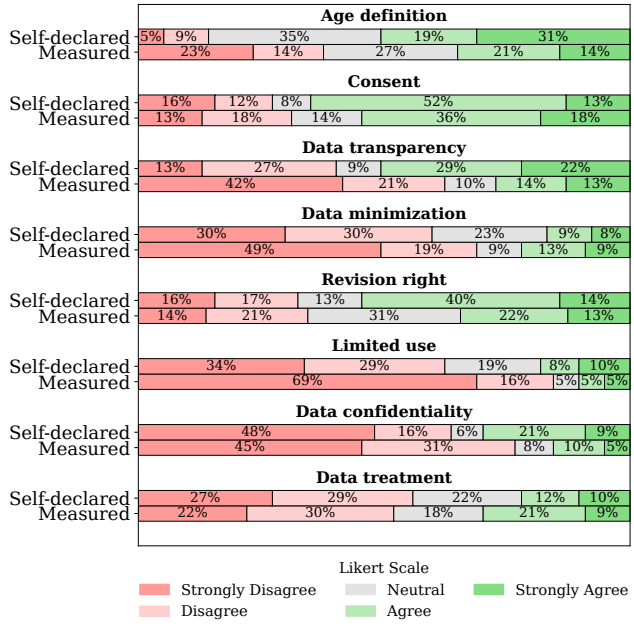

Fig. 2: Survey answer distribution according to each evaluated privacy attribute (Table I).

information, which is favorable for discussions about digital privacy and data protection. The gender distribution leaned toward male, with 69% identified as male and 31% as female. Most children were between 2 and 5 years old (49%), a stage marked by intense development and early interaction with digital technologies. Smaller percentages were found among the 6 to 9 and 10 to 12-year-old groups, suggesting that digital exposure begins before the typical age for independent device use. Notably, 23% of children had their own profiles on digital platforms, despite many being under the required minimum age.

B. The Parental Maturity on Child Privacy

To answer RQ1, we further investigate the self-declared knowledge of parents in managing child privacy on social platforms. To achieve such a goal, we assess the answers on a Likert scale for each question listed on Table II (*Self-declared Knowledge*). The goal is to investigate how the parents evaluate themselves regarding the management of child privacy on social platforms. Figure 2 shows the distributions of answers for each evaluated privacy attribute based on the Likert scale. The analysis of self-declared knowledge revealed that many respondents believe they are familiar with the legal frameworks that regulate children's privacy in digital environments. Half (50%) stated that they knew the LGPD defines a child as someone under the age of 12, while 35% were unsure and 14% openly admitted they did not know. Similarly, 65% of participants claimed to be aware of the legal requirement for parental authorization when children use social networks, and 55% said they knew that parents or guardians are legally responsible for their children's online activities.

When asked about their understanding of the role of digital platforms, the vast majority expressed agreement that platforms should request parental authorization, even if the child is technically able to create a profile independently. However, only 22% of respondents stated that the privacy notices presented by platforms are clear, while 40% found them unclear or not clear at all. Although this perception does not measure actual knowledge, it reflects a critical stance toward the transparency of current data processing practices. Finally, while participants expressed strong disapproval of commercial practices involving children's data—56% opposed its use for advertising and geolocation tracking—these opinions, as self-declared indicators, reveal a general sensitivity to privacy concerns and an expressed alignment with child data protection principles.

To address RQ2, we examine the gap between parents' self-declared knowledge and their measured knowledge. As detailed in Table II, the measured knowledge reflects how well parents' responses align with the current legal and social frameworks governing children's privacy. By comparing their expressed agreement with these established guidelines against their self-declared familiarity, we are able to assess their actual maturity and preparedness in managing their children's digital privacy. Figure 2 overviews the self-declared knowledge $vs.$ the measured knowledge of respondents. The analysis highlights a consistent mismatch between what parents believe they know and their understanding of privacy-related responsibilities under current regulations. While 50% of respondents claimed to be familiar with the legal definition of a child according to the LGPD, the majority of this group disagreed with the minimum age restriction of 13 years set by major platforms such as Instagram and TikTok. This indicates that many guardians who assert legal awareness may not fully comprehend or internalize the implications of these regulations. Similarly, 66% of respondents reported awareness of the legal requirements concerning age and parental consent. Yet, this self-assessment did not always align with their support for enforcing or practically applying these requirements.

When evaluating more specific responsibilities, such as parental liability for children's actions online, only 51% of

participants acknowledged this obligation, and a significant portion either denied knowledge or expressed uncertainty. Even among those who claimed awareness of data processing practices, only a small subset demonstrated a comprehensive understanding of how their data—and that of their children—is collected, used, or shared. The perception of privacy notices provided by digital platforms further shows this gap given that 25% found them clear, just 16% of this group showed consistent understanding of essential data protection principles, pointing to a limited effectiveness of current consent mechanisms. These findings suggest that many parents believe they can handle their children's digital privacy, but their preparedness is limited.

To answer RQ3, we must further investigate the survey findings. The evidence suggests that parents are not fully equipped to manage their children's privacy on social platforms consistently and informally. While many respondents declared familiarity with legal definitions, requirements, and responsibilities regarding children's online presence, their answers to specific knowledge-based questions reveal notable discrepancies between what they believe they know and what they understand. Furthermore, although many parents supported being legally responsible for their children's digital actions, they often lacked clarity on how data is collected, shared, and processed by platforms, especially in third-party tracking and targeted advertising cases. This disconnect between self-declared and demonstrated knowledge raises concerns about the effectiveness of relying solely on parental oversight to safeguard children's digital privacy.

V. Conclusion

The widespread use of digital platforms by children has intensified concerns about the adequacy of privacy protections. Current legislation places the responsibility for managing children's privacy on parents and guardians, assuming they possess the necessary knowledge to make informed decisions. To address this, we proposed a two-phase approach. First, we identified the core privacy attributes relevant to children's data protection based on GDPR, COPPA, and LGPD, establishing a normative foundation. Second, we surveyed 77 parents and guardians to assess their maturity, defined by awareness, understanding, and ability to apply privacy-related measures. Our findings reveal a substantial gap between self-declared and actual knowledge, indicating that many guardians may not be fully equipped to meet the privacy responsibilities expected by law.

Acknowledgment

This work was partially sponsored by the Brazilian National Council for Scientific and Technological Development (CNPq), grants nº 407879/2023-4, 442262/2024-8, and 302937/2023-44, Araucária Foundation, the Secretariat of Science, Technology and Higher Education (SETI) and the Coordination for the Improvement of Higher Education Personnel (CAPES).

References

[1] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework," *Information Systems Frontiers*, vol. 24, no. 2, p. 393–414, Jul. 2020.

[2] R. N. Zaeem and K. S. Barber, "The effect of the gdpr on privacy policies: Recent progress and future promise," *ACM Transactions on Management Information Systems*, vol. 12, no. 1, p. 1–20, Dec. 2020.

[3] C. Neitzke, J. Mendes, L. Rivero, M. Teixeira, and D. Viana, "Enhancing lgpd compliance: Evaluating a checklist for lgpd quality attributes within a government office," in *Proc. of the XXII Brazilian Symposium on Software Quality*, ser. SBQS '23. ACM, Nov. 2023, p. 218–227.

[4] N. Vlajic, M. El Masri, G. M. Riva, M. Barry, and D. Doran, "Online tracking of kids and teens by means of invisible images: Coppa vs. gdpr," in *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*, ser. CCS '18. ACM, Jan. 2018.

[5] O. d. P. Albuquerque, M. Fantinato, M. M. Eler, S. M. Peres, and P. C. K. Hung, "A study of parental control requirements for smart toys," in *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, Oct. 2020, p. 2215–2220.

[6] R. Ribeiro, A. Santin, V. Abreu, J. Marynowski, and E. Viegas, "Providing security and privacy in smart house through mobile cloud computing," in *2016 8th IEEE Latin-American Conference on Communications (LATINCOM)*. IEEE, Nov. 2016, p. 1–6.

[7] R. A. Etzel, "The special vulnerability of children," *International Journal of Hygiene and Environmental Health*, vol. 227, p. 113516, Jun. 2020.

[8] G. Aridor, Y.-K. Che, and T. Salz, "The effect of privacy regulation on the data industry: Empirical evidence from gdpr," in *Proceedings of the 22nd ACM Conference on Economics and Computation*, ser. EC '21. ACM, Jul. 2021.

[9] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," *Complex amp; Intelligent Systems*, vol. 7, no. 5, p. 2157–2177, Jun. 2021.

[10] G. Dorfleitner, L. Hornuf, and J. Kreppmeier, "Promise not fulfilled: Fintech, data privacy, and the gdpr," *Elec. Markets*, vol. 33, Jul. 2023.

[11] V. M. de Oliveira, H. M. de Oliveira, G. M. Santos, J. Geremias, and E. K. Viegas, "A big data framework for scalable and cross-dataset capable machine learning in network intrusion detection systems," *IEEE Access*, vol. 13, p. 129419–129431, 2025.

[12] M. J. Amon, N. Kartvelishvili, B. I. Bertenthal, K. Hugenberg, and A. Kapadia, "Sharenting and children's privacy in the united states: Parenting style, practices, and perspectives on sharing young children's photos on social media," *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CSCW1, p. 1–30, Mar. 2022.

[13] M. F. Abreu, E. K. Viegas, and A. O. Santin, *A Review of Social Network Regulations and Mechanisms for Safeguarding Children's Privacy*. Springer Nature Switzerland, 2024, p. 427–438.

[14] A. G. Filho, E. K. Viegas, A. O. Santin, and J. Geremias, "A dynamic network intrusion detection model for infrastructure as code deployed environments," *Journal of Network and Systems Management*, 2025.

[15] E. Viegas, A. Santin, J. Bachtold, D. Segalin, M. Stihler, A. Marcon, and C. Maziero, "Enhancing service maintainability by monitoring and auditing sla in cloud computing," *Cluster Computing*, vol. 24, no. 3, p. 1659–1674, Nov. 2020.

[16] A. d. L. Salgado, B. Singh, P. C. K. Hung, A. Jiang, Y.-H. Liu, A. P. d. A. Wheler, and H. A. Gaber, "Preliminary tendencies of users' expectations about privacy on connected-autonomous vehicles," in *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, Oct. 2020, p. 296–301.

[17] S. Thammaratchuchai, N. Nutsuda, and P. Jantori, "The awareness of child privacy of thai parents on social media," *Human Behavior, Development and Society*, vol. 24, no. 3, p. 1–10, 2023.

[18] R. Sun, M. Xue, G. Tyson, S. Wang, S. Camtepe, and S. Nepal, "Not seen, not heard in the digital world! measuring privacy practices in children's apps," in *Proceedings of the ACM Web Conference 2023*, ser. WWW '23. ACM, Apr. 2023, p. 2166–2177.

[19] A. Ekambaranathan, J. Zhao, and M. Van Kleek, "How can we design privacy-friendly apps for children? using a research through design process to understand developers' needs and challenges," *Proc. of the ACM on Human-Computer Interaction*, no. CSCW2, p. 1–29, 2023.

[20] P. Horchulhack, E. K. Viegas, A. O. Santin, and J. A. Simioni, "Network-based intrusion detection through image-based cnn and transfer learning," in *2024 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, May 2024, p. 386–391.