

Avaliação da Competência Parental na Gestão da Privacidade dos Filhos em Ambientes Digitais

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

¹Programa de Pós-Graduação em Informática (PPGIa)
Pontifícia Universidade Católica do Paraná (PUCPR)
80.215-901 - Curitiba - PR

{mykaele.abreu, eduardo.viegas, santin, jgeremias}@ppgia.pucpr.br

Resumo. *A disseminação do uso de plataformas digitais por crianças intensificou as preocupações quanto à adequação das proteções de privacidade existentes. A legislação atribui aos pais a responsabilidade de gerenciar a privacidade das crianças, pressupondo seu conhecimento para decisões informadas. Diante disso, este trabalho avalia a maturidade parental na gestão da privacidade dos filhos nas plataformas sociais. Primeiramente, identificamos os principais atributos de privacidade relevantes para a proteção de dados online de crianças, com base na análise das leis e regulamentações vigentes, como a GDPR, a COPPA e a LGPD. Na segunda etapa, entrevistamos 77 pais e responsáveis para avaliar seu nível de maturidade no gerenciamento de medidas relacionadas à privacidade. Os resultados revelam uma discrepância significativa entre o conhecimento percebido e o conhecimento real, indicando que muitos pais podem não estar adequadamente preparados para desempenhar o papel exigido pelas regulamentações vigentes.*

1. Introdução

A proteção da privacidade online das crianças é essencial devido a diversas ameaças, como a coleta inadequada de dados pessoais, a publicidade direcionada e as interações online potencialmente prejudiciais. [Alomar and Egelman 2022]. Recentemente, o número de crianças e adolescentes que utilizam plataformas de mídia social como TikTok, YouTube, Facebook e Instagram aumentou consideravelmente, com quase uma em cada quatro crianças utilizando a Internet antes dos seis anos de idade. [CGI.br 2024]. Entre os jovens de 9 a 17 anos, 93% possuem perfis digitais, com 88% utilizando YouTube, 78% WhatsApp, 66% Instagram, e 63% TikTok. O uso generalizado de plataformas digitais expõe os jovens usuários a uma coleta intensa de dados e à publicidade direcionada, gerando preocupações significativas sobre privacidade e segurança. [Ekambaranathan et al. 2023]. Apesar desses riscos, apenas 28% dos pais ou responsáveis implementam filtros ou configurações para limitar a exposição à publicidade online.

Como resultado, foram estabelecidas várias leis para proteger dados pessoais, incluindo disposições específicas voltadas para as crianças. [Ismagilova et al. 2020]. Alguns exemplos, como a General Data Protection Regulation (GDPR) [Zaeem and Barber 2020] da Europa, a General Data Protection Law (LGPD) [Neitzke et al. 2023] do Brasil, e Children's Online Privacy Protection Act (COPPA) [Vlajic et al. 2018] dos Estados Unidos. Em vigor desde 2018, a GDPR unifica e fortalece a proteção de dados de toda a União Europeia. A LGPD, que entrou em vigor no ano 2020, estabelece diretrizes

para a proteção de dados pessoais no Brasil. A COPPA concentra-se especificamente na proteção de dados online de crianças. Ambas as regulamentações buscam garantir práticas responsáveis de coleta, manuseio e armazenamento de dados para indivíduos de todas as idades, incluindo menores. [Albuquerque et al. 2020]. Por sua vez, a COPPA, promulgada no ano de 1998, foca na proteção da privacidade de crianças com menos de 13 anos, oferecendo aos pais maior controle sobre as informações que sites e aplicativos podem coletar de seus filhos. Além disso, a COPPA aborda questões relacionadas ao marketing direcionado e promove a conscientização sobre segurança online.

A privacidade das crianças tornou-se uma preocupação crescente à medida que o uso de tecnologias online e dispositivos móveis por menores se torna cada vez mais comum. Essa crescente interação com ambientes digitais normalizou a coleta e o processamento de dados por provedores de serviços, ao mesmo tempo em que expôs as crianças a riscos significativos em termos de privacidade. [Simioni et al. 2025b]. As crianças são reconhecidas como vulneráveis devido ao seu desenvolvimento físico e cognitivo em curso, à capacidade ainda limitada de tomar decisões de forma autônoma e à sensibilidade emocional e psicológica. [Etzel 2020]. As legislações nacionais e internacionais reconhecem essa vulnerabilidade e garantem direitos especiais às crianças, ressaltando a importância da supervisão ativa de pais, responsáveis e cuidadores na proteção de sua privacidade.

Os pais e responsáveis possuem um papel essencial, para garantir que as crianças compreendam os riscos do compartilhamento de dados e estejam protegidas de potenciais ameaças. [Abreu et al. 2024]. No entanto, a falta de transparência nas políticas das redes sociais e nas práticas de tratamento de dados dificultam a capacidade de avaliar e escolher adequadamente por parte dos adultos. Um dos principais desafios é a variação no grau de maturidade entre pais e responsáveis, definida neste contexto como a capacidade de identificar riscos online e adotar medidas eficazes de proteção à privacidade. [Jain et al. 2021]. A ausência de padronização nos mecanismos de proteção de dados voltados para menores agrava ainda mais esse cenário [Filho et al. 2025]. Regulamentações como a LGPD, a COPPA e a GDPR apresentam diferenças em relação à definição de quem é considerado menor, o que gera ambiguidades jurídicas e limita a eficácia da aplicação dessas normas. [Dorfleitner et al. 2023]. Muitos provedores de serviços digitais não adotam mecanismos eficazes, como a verificação robusta do consentimento parental ou controles de segurança mais rigorosos. Além disso, há pouca compreensão sobre como os pais percebem esses recursos e sobre sua capacidade de utilizá-los de maneira eficaz. Para abordar essa lacuna, é preciso uma compreensão mais profunda da maturidade dos pais em relação à privacidade digital e o desenvolvimento de estratégias educacionais para aumentar a segurança online das crianças.

Um desafio significativo das regulamentações atuais é a premissa de que pais e responsáveis são os principais responsáveis por proteger a privacidade de seus filhos no uso de plataformas digitais. Isso pressupõe que eles tenham o conhecimento necessário sobre questões de privacidade digital e compreendam sobre as mais diversas regulamentações, como a GDPR, a COPPA e a LGPD. [Amon et al. 2022]. No entanto, essa expectativa frequentemente desconsidera os diferentes níveis de alfabetização e conscientização digital entre os pais e os responsáveis. Isso porque eles podem apresentar dificuldades em compreender configurações complexas de privacidade, políticas das plataformas e requisitos

legais. Embora o envolvimento parental desempenhe um papel crucial, a literatura ainda carece de uma compreensão aprofundada da maturidade dos pais na gestão da privacidade digital das crianças, especialmente no que diz respeito à sua capacidade de identificar riscos, interpretar obrigações regulatórias e implementar medidas de proteção eficazes. Essa lacuna evidencia a necessidade urgente de mais pesquisas sobre como os pais percebem e interagem com os mecanismos de privacidade, além do desenvolvimento de estratégias de apoio para fortalecer sua capacidade de desempenhar esse papel de forma eficaz.

Contribuição. Diante disso, este trabalho avalia a maturidade parental na gestão da privacidade das crianças em plataformas sociais. O estudo é realizado em duas fases. Na primeira fase, identificamos os principais atributos de privacidade essenciais para a proteção dos dados online das crianças analisando as principais leis e regulamentações, incluindo o GDPR, a COPPA e a LGPD. Estabelecemos uma linha de base regulatória para avaliar as responsabilidades e expectativas parentais. Na segunda fase, desenvolvemos e aplicamos uma pesquisa estruturada com 77 pais e responsáveis para avaliar sua maturidade, definida por sua conscientização sobre a implementação de medidas relacionadas à privacidade. A pesquisa abrange diferentes aspectos, incluindo o conhecimento sobre definições legais, a percepção das responsabilidades das plataformas, a compreensão das práticas de tratamento de dados e as atitudes em relação ao uso comercial dos dados das crianças. Essa abordagem permite uma análise detalhada da eficácia com que os pais conseguem proteger a privacidade de seus filhos nas redes sociais, além de evidenciar as possíveis lacunas entre o conhecimento percebido e o real.

Em resumo, as principais contribuições deste trabalho são:

- Definição de um conjunto estruturado de atributos de privacidade com base nas estruturas legais e regulatórias vigentes (GDPR, COPPA, LGPD), visando estabelecer uma referência para avaliar as responsabilidades parentais na proteção dos dados online das crianças
- Avaliação da maturidade parental por meio de uma pesquisa detalhada, examinando a conscientização, a compreensão e a capacidade prática dos pais em gerenciar as configurações de privacidade e proteger os dados de seus filhos em plataformas sociais. Os dados demonstram que a maioria dos pais ou dos responsáveis não possuem a conscientização ou a preparação necessárias para gerenciar eficazmente a privacidade de seus filhos nesses ambientes.

2. Contexto

2.1. Privacidade de Dados

Privacidade refere-se ao direito do indivíduo de controlar o acesso às suas informações pessoais, por meio de proteções legais e salvaguardas técnicas que garantam a confidencialidade, a autenticidade e a integridade dos dados. [Ismagilova et al. 2020]. O NIST destaca que os usuários muitas vezes não compreendem totalmente as implicações do compartilhamento de dados pessoais por meio de plataformas digitais. [Landis and Kroll 2024, de Oliveira et al. 2025]. Para ajudar as organizações a enfrentar esses desafios, o NIST desenvolveu o Privacy Risk Management Framework, que oferece orientação estruturada para identificar e gerenciar riscos de privacidade. Esses riscos nem sempre estão ligados a violações de segurança cibernética; muitas vezes, decorrem de consequências

não intencionais do processamento de dados em plataformas sociais. Por exemplo, algoritmos de recomendação de conteúdo ou de direcionamento de anúncios podem inferir interesses pessoais, hábitos e até estados emocionais, gerando uma sensação de vigilância constante. [Sun et al. 2023, Geremias et al. 2023]. Além disso, o simples cumprimento das normas regulatórias não é suficiente para eliminar os riscos à privacidade. Para enfrentar esses desafios, o NIST recomenda uma abordagem proativa de gerenciamento de privacidade por meio de cinco funções principais: *Identificar, Governar, Controlar, Comunicar, e Proteger*—ajudando as organizações a avaliarem e mitigarem melhor os riscos de privacidade decorrentes de interações em plataformas sociais.

2.2. Privacidade infantil nas redes sociais

A privacidade das crianças em plataformas sociais é uma preocupação específica e relevante, já que os menores são especialmente vulneráveis às consequências não intencionais da coleta e do processamento de dados. [Simioni et al. 2025a]. As redes sociais geralmente coletam grandes quantidades de informações pessoais, incluindo comportamento de navegação, dados de localização e interações de conteúdo, que podem ser usados para criação de perfis e publicidade direcionada. [Ekambaranathan et al. 2023]. Essas práticas expõem as crianças a riscos como manipulação, exploração e perda de autonomia sobre seus dados. Além disso, os estágios de desenvolvimento psicológico infantil limitam sua capacidade de compreender plenamente e consentir com o compartilhamento de informações, o que torna fundamental a adoção de salvaguardas mais robustas e adequadas às suas necessidades.

Diversas regulamentações foram criadas para enfrentar essas preocupações, como a COPPA nos Estados Unidos, o GDPR na União Europeia e a LGPD no Brasil. Essas regulamentações reconhecem a necessidade de uma proteção reforçada dos dados de crianças e, em muitos casos, exigem o consentimento dos pais para o seu tratamento. [Amon et al. 2022]. Essas regulamentações pressupõem que os pais ou responsáveis estejam adequadamente informados e capacitados para avaliar e gerenciar a privacidade digital de seus filhos. Entretanto, isso representa um desafio considerável, uma vez que muitos pais não possuem uma compreensão clara de como os riscos à privacidade se manifestam nas plataformas sociais nem sabem como configurar adequadamente as ferramentas de privacidade [Thammaratchuchai et al. 2023]. Como resultado, as crianças podem permanecer inadequadamente protegidas, apesar de estarem protegidas pela lei.

3. Trabalhos relacionados

A avaliação do nível de maturidade em privacidade é normalmente realizada por meio de pesquisas que utilizam questionários estruturados. Essas ferramentas ajudam a avaliar a compreensão, as atitudes e os comportamentos dos indivíduos em relação às práticas de privacidade, permitindo que os pesquisadores identifiquem lacunas na conscientização e áreas que precisam ser aprimoradas. Por exemplo, A. L. Salgado *et al.* [Salgado et al. 2020] avaliaram as expectativas dos usuários em relação à privacidade por meio de uma pesquisa com 50 indivíduos. Os autores identificaram que a maioria dos indivíduos desconhece os problemas de segurança associados à privacidade no contexto automotivo. O. Albuquerque *et al.* [Albuquerque et al. 2020] teve como objetivo identificar os requisitos de privacidade associados a aplicativos voltados para crianças. O autor destacou os

desafios associados à definição de mecanismos adequados de controle parental e a falta de propostas aplicáveis. M. J. Amon *et al.* [Amon et al. 2022] investiga a preocupação dos pais com a privacidade ao postar fotos de seus filhos pequenos nas redes sociais. A pesquisa, realizada com mais de 400 pessoas, mostrou que os pais geralmente não se importam com os riscos à privacidade associados aos dados de seus filhos. S. Thammarchuchai *et al.* [Thammarchuchai et al. 2023] investigaram a conscientização dos pais sobre a privacidade dos filhos nas redes sociais. Os autores aplicaram um questionário a 96 indivíduos por meio de uma escala Likert. Os resultados indicaram que os pais têm consciência moderada dos efeitos negativos de compartilhar as atividades dos filhos nas redes sociais. Entretanto, o estudo ignorou a maturidade dos pais em lidar com a privacidade dos filhos e as regulamentações associadas. Costuma-se atribuir aos pais o papel principal na proteção da privacidade digital das crianças. No entanto, muitos aplicativos desenvolvidos para o público infantil promovem o uso autônomo, o que dificulta a supervisão efetiva dos responsáveis sobre a coleta de dados e as configurações de privacidade. Essa lacuna levanta dúvidas sobre a eficácia de depender exclusivamente dos pais para proteger a privacidade online dos menores. Como exemplo, R. Sun *et al.* [Sun et al. 2023] investigou as questões de privacidade de aplicativos móveis voltados para crianças. Os autores revelaram que 80% dos aplicativos familiares utilizam rastreadores que não são permitidos em aplicativos voltados para crianças.

A literatura existente ressalta de forma consistente a preocupação dos pais com a privacidade de seus filhos em ambientes online. No entanto, apesar dessa conscientização, ainda há uma lacuna significativa em pesquisas que investiguem especificamente o grau de preparo e maturidade dos pais na gestão e proteção da privacidade infantil. A maioria dos estudos concentra-se no comportamento online das crianças ou nas funcionalidades técnicas das plataformas, oferecendo poucos insights sobre a capacidade dos pais de compreender normas de privacidade, identificar riscos e adotar medidas eficazes de proteção. Essa carência de investigação limita o desenvolvimento de estratégias direcionadas para apoiar e capacitar os pais nesse papel.

4. Avaliação da maturidade parental na gestão da privacidade infantil

Para enfrentar esse desafio, nossa proposta visa avaliar a maturidade dos pais na gestão da privacidade dos filhos em plataformas sociais. A proposta é conduzida de duas etapas.

A primeira etapa irá identificar os principais atributos de privacidade descritos nos principais marcos regulatórios, incluindo o GDPR, a COPPA e a LGPD. Analisamos como essas regulamentações definem os direitos de proteção de dados das crianças, as responsabilidades atribuídas aos pais ou responsáveis e as obrigações impostas aos provedores de serviços digitais. Esta análise serve como base para a identificação dos aspectos críticos da privacidade que os pais devem compreender e gerenciar em ambientes digitais.

Na segunda etapa, elaboramos e implementamos uma pesquisa estruturada para avaliar a maturidade parental. A pesquisa utiliza uma escala Likert para captar o grau de conhecimento dos pais sobre conceitos e princípios regulatórios relacionados à privacidade. As redes sociais são adotadas como o principal caso de uso devido à sua relevância na vida digital das crianças. A pesquisa é estruturada para estabelecer conexões entre o conhecimento autorrelatado pelos pais sobre as regulamentações de proteção de dados e sua familiaridade com as políticas de privacidade e os termos de uso das plataformas com as

Tabela 1. Principais aspectos de privacidade definidos pelas regulamentações e leis atuais de privacidade de criança (GDPR, COPPA, LGPD).

Aspectos de Privacidade	Definição
Dados Pessoais	Dado pessoal é qualquer informação relacionada à pessoa natural identificada ou identificável, já o dado pessoal sensível é aquele vinculado a identificação da pessoa.
Definição de Criança	Idades definidas para a necessidade do consentimento dos responsáveis sobre a proteção de dados.
Consentimento dos Pais ou Responsáveis	O tratamento de dados pessoais deve ser realizado com o consentimento dos pais ou tutores legais
Transparência do uso de Informações	As informações deverão estar públicas, contendo o tipo de dado que foi coletado, para que este dado será utilizado e acesso aos dados para realizar procedimentos
Finalidade Limitada	Os dados das crianças só podem ser coletados para finalidades determinadas, específicas e legítimas.
Minimização de Dados	A coleta de dados deve ser limitada ao mínimo necessário para atingir a finalidade específica.
Coleta de Dados sem o Consentimento dos Pais	De maneira geral, os dados só poderão ser coletados quando for para contactar os pais e os responsáveis.
Aviso de Tratamento de Dados	O aviso de tratamento de dados deve estar de forma simples, clara e acessível.
Direito de Revisar os Dados Fornecidos	A qualquer momento os dados poderão ser revisados e ou apagados.
Desing Orientado à Privacidade	Organizações devem considerar e incorporar medidas de privacidade desde o início do desenvolvimento de produtos e serviços.
Confidencialidade das Informações Coletadas	As empresas devem proteger os dados pessoais que receberam e, caso os compartilhem com terceiros, devem assegurar que esses terceiros adotem o mesmo nível de proteção.

quais seus filhos interagem. Essa abordagem permite identificar lacunas de compreensão e destacar áreas que podem se beneficiar de estratégias educacionais complementares

4.1. Atributos de privacidade

A definição dos atributos de privacidade pertinentes ao nosso estudo foi guiada por três principais marcos regulatórios: COPPA, GDPR e LGPD. Esses regulamentos descrevem requisitos específicos para a coleta, o processamento e a proteção de dados pessoais de crianças. Apesar das diferenças de escopo e definições — como limites de idade variados para definir uma criança — eles compartilham princípios comuns que visam proteger a privacidade das crianças em ambientes digitais

A avaliação das legislações pertinentes destacou aspectos essenciais, como a definição de dados pessoais e sensíveis, o papel e os requisitos do consentimento dos pais ou responsáveis, além das implicações legais do processamento de dados de crianças

sem a devida autorização. Por exemplo, embora o GDPR exija o consentimento dos pais para o processamento de dados de crianças menores de 16 anos (podendo ser modificador de acordo com a legislação local), A COPPA irá se aplicar para crianças menores que 13 anos e exige consentimento parental verificável. A LGPD inicialmente refletia essa necessidade, mas foi recentemente revisada para permitir bases mais flexíveis para o processamento de dados, desde que os melhores interesses da criança sejam respeitados. Essas mudanças evidenciam a complexidade de garantir proteções de privacidade consistentes em nível global, destacando a necessidade de abordagens de conformidade mais integradas.”

As exigências legais vão além de questões como consentimento e idade, abrangendo outros atributos essenciais de privacidade. Entre eles, destaca-se a transparência no uso de dados — exigindo que as empresas comuniquem de forma clara e acessível como os dados são coletados, armazenados e compartilhados.—, bem como o direito dos usuários de acessar e corrigir seus dados pessoais. Outro princípio fundamental é o da minimização de dados, que restringe a coleta a apenas aquilo que for estritamente necessário. Além disso, consideramos a importância da privacidade desde a concepção, que determina a incorporação de mecanismos de proteção de dados desde as fases iniciais do desenvolvimento de sistemas e produtos. Todas as três legislações analisadas reforçam esses princípios como pilares para a construção da confiança dos usuários e a garantia de uma gestão responsável e ética das informações pessoais.

Ao reunir esses elementos, consolidamos um conjunto unificado de atributos de privacidade que refletem os padrões legais e éticos essenciais para a proteção de dados de crianças. Esses atributos funcionam como critérios de avaliação no modelo desenvolvido em nosso estudo, permitindo-nos medir até que ponto os pais compreendem e aplicam os princípios de privacidade no contexto das plataformas sociais. A tabela 1 1 apresenta um conjunto consolidado de aspectos de privacidade, extraídos das principais regulamentações de proteção de dados relativas a crianças. Ela define o que são dados pessoais e sensíveis, estabelece limites de idade que exigem o consentimento dos pais ou responsáveis e reforça a necessidade de transparência sobre como os dados são coletados, utilizados e acessados. Entre os princípios-chave, destacam-se a limitação de finalidade, a minimização da coleta de dados e a exigência de avisos claros e acessíveis sobre o processamento das informações. A estrutura também enfatiza o direito de revisar ou excluir dados, a importância da privacidade desde a concepção — incorporada desde as fases iniciais do desenvolvimento do sistema —, e a obrigação de garantir a confidencialidade das informações compartilhadas, inclusive quando envolvem a transferência de dados a terceiros.

4.2. Modelo de maturidade

Os Modelos de Maturidade são fundamentados na premissa de que pessoas, organizações, áreas funcionais e processos evoluem através de um processo contínuo de desenvolvimento e crescimento, avançando em direção a níveis mais avançados de maturidade. Neste trabalho, será utilizado o SANS Security Awareness Maturity Model, de forma análoga, para se estabelecer os níveis de maturidade dos pais em relação à privacidade e segurança digital de seus filhos. Esse modelo de maturidade foi criado para avaliar o nível de conscientização e prática de segurança dentro das organizações, categorizando em diferentes estágios de desenvolvimento.

Tabela 2. Perguntas em uma Escala Likert para avaliar a maturidade dos responsáveis no gerenciamento da privacidade dos filhos em plataformas sociais.

Atributos de Priv.	Conhecimento Autodeclarado	Métrica do conhecimento
Definição de idade	Como você classificaria seu conhecimento da definição de ' <i>criança</i> ' de acordo com os regulamentos aplicáveis?	Considerando o trecho dos termos de uso de uma rede social: " <i>...Você deve ter pelo menos 13 anos para usar o serviço...</i> " O quanto você acredita que esta declaração está em conformidade com os regulamentos?
Cons. dos Pais	Qual é o seu nível de conhecimento em relação às exigências legais de idade e autorização parental, especialmente, considerando a criação de contas por crianças sem permissão dos pais?	Considerando o trecho retirado do termo de uso de uma rede social: " <i>...Se você é pai/mãe ou responsável legal de um usuário menor de 18 anos, ao permitir o uso do Serviço pelo seu filho, você fica sujeito aos termos deste Contrato e é responsável pelas atividades do seu filho no YouTube...</i> ", o quanto você concorda que está ciente e entende os termos de uso da rede social que seu filho usa?
Transp. dos Dados	Como você avaliaria seu nível de concordância com a afirmação: " <i>Sinto-me adequadamente informado sobre como os dados do meu filho são coletados e usados pelas redes sociais</i> "?	Até que ponto você concorda que é apropriado que as redes sociais usem dados de crianças para avaliar a eficácia dos anúncios e veicular publicidade personalizada com base nos interesses e atividades delas na plataforma?
Minimização dos dados	O quanto você concorda com a quantidade de dados que as redes sociais coletam de crianças?	Considerando este trecho de uma rede social: " <i>Ao criar uma conta em uma rede social e aceitar os Termos de Uso, você concorda com a coleta de informações sobre sua localização aproximada, incluindo dados do cartão SIM e/ou endereço IP.</i> " Isso implica que você está autorizando a disponibilização de informações como a localização atual da criança. Qual é o seu nível de concordância com a coleta de dados de localização ao aceitar os Termos de Uso?

Revisão de dados	Como você avaliaria seu conhecimento sobre se as redes sociais permitem a revisão (atualização) dos dados do seu filho na plataforma a qualquer momento, conforme exigido por lei?	Este trecho de uma rede social menciona: <i>“incluindo o direito de acessar, excluir, atualizar ou corrigir seus dados, ser informado sobre o processamento de dados, registrar reclamações junto às autoridades e potencialmente outros direitos.”</i> Isso significa que você pode, por exemplo, modificar os dados da criança, como idade e interesses, a qualquer momento. Se você precisasse revisar os dados da criança para interromper anúncios direcionados, qual é o seu nível de conhecimento sobre como fazer essa alteração?
Finalidade Limitada	Como você avaliaria a transparência da rede social que seu filho utiliza em relação à forma como suas informações pessoais são coletadas, utilizadas e compartilhadas?	Este trecho dos termos de uso de uma rede social menciona: <i>“Também podemos divulgar suas informações a terceiros: se vendermos ou comprarmos qualquer negócio ou ativo”</i> . Isso significa que as informações da criança podem ser compartilhadas com outras empresas sem o seu conhecimento e aprovação prévios. Qual é o seu nível de concordância com a prática de divulgar suas informações a terceiros?
Conf. das Informações	Como você avalia sua concordância com a forma como as redes sociais usam dados para veicular anúncios direcionados a crianças?	Ao aceitar os Termos de Uso em uma rede social, você concorda com a coleta de informações sobre os vídeos assistidos pela criança, termos de pesquisa e outras interações com conteúdo e anúncios no aplicativo. Isso significa que a rede social pode exibir anúncios com base no histórico de vídeos da criança, mas não é responsável pela coleta de dados por outros sites visitados após clicar nesses anúncios. Qual é o seu nível de concordância com essa prática?

Aviso de Tratamento de Dados	Como você avalia sua concordância com a clareza e a transparência do aviso de tratamento de dados fornecido pelas redes sociais em relação às informações de crianças?	Ao aceitar os Termos de Uso de uma rede social, você se sente informado sobre os seguintes tópicos: quais informações são coletadas, como as informações são usadas, onde são armazenadas, seus direitos e escolhas, a segurança das suas informações e por quanto tempo elas são retidas. Qual é o seu nível de concordância sobre a clareza dessas informações quando você criou a conta?
------------------------------	--	---

No nosso contexto, será realizado um questionário para que possamos definir esse nível de conhecimento dos pais e assim criar mecanismos para proteger a privacidade das crianças. O Modelo de maturidade SANS, serão divididos em 5 níveis de programas de conscientização, desde a conscientização inexistente até uma cultura de segurança profundamente enraizada, que foi readaptado neste contexto para refletir o engajamento dos pais com a privacidade digital.

O modelo de maturidade parental proposto avaliará a conscientização e as ações tomadas para proteger os dados pessoais das crianças em plataformas digitais. No Nível 1, os pais desconhecem os riscos online e não tomam medidas de proteção. O Nível 2 reflete uma conscientização mínima com pouca aplicação prática. No Nível 3, há uma compreensão moderada, com medidas de proteção esporádicas, como ajustar as configurações de privacidade ou oferecer orientação básica às crianças. No Nível 4, os pais implementam consistentemente práticas proativas de privacidade e se envolvem em educação contínua com seus filhos. O Nível 5 representa pais que não apenas são informados e protetores, mas também defendem os direitos digitais das crianças.

Este modelo de maturidade avalia as principais dimensões da privacidade digital infantil, com ênfase no conhecimento dos pais ou responsáveis sobre a coleta e o uso de dados pessoais, seu envolvimento na criação e gestão dos perfis digitais dos filhos, e nas medidas adotadas para protegê-los. O objetivo é medir o nível de maturidade em relação aos princípios fundamentais da privacidade, como consentimento, transparência, minimização de dados e o direito de acesso e revisão das informações. (Vide Tabela 1. Foi distribuído um questionário aos pais ou responsáveis para realizar esta avaliação (posteriormente apresentado na Seção 5.1). Com base nas respostas, será atribuído um nível de maturidade, refletindo sua compreensão e envolvimento na proteção das informações pessoais de seus filhos. As perguntas abrangem aspectos como idade para consentimento, requisitos de consentimento parental, compreensão de dados pessoais e seu uso, práticas de minimização de dados, direito de revisão de dados, transparência no processamento de dados e princípios de confidencialidade.

As perguntas foram estrategicamente formuladas e divididas em duas etapas para fornecer uma visão detalhada sobre o envolvimento dos pais na proteção da privacidade online de seus filhos. O primeiro tipo concentra-se no , **conhecimento autodeclarado** fo correspondente , capturando sua percepção do que sabem ou acreditam sobre um deter-

minado tópico de privacidade. Já no segundo tipo é *métrica do conhecimento*, avaliando se sua compreensão está alinhada com práticas, definições ou requisitos legais precisos. Essa abordagem identifica possíveis lacunas entre o conhecimento percebido e o real, oferecendo uma visão mais confiável da maturidade dos pais em relação à privacidade digital dos filhos. Tabela 2 apresenta o conjunto completo de perguntas e os aspectos específicos de privacidade que cada uma visa validar.

5. Avaliação baseada em pesquisa

Nossa pesquisa conduzida tem como objetivo responder às seguintes perguntas de pesquisa (RQs):

- (RQ1) *Qual é o conhecimento autodeclarado dos pais sobre como gerenciar a privacidade dos filhos em plataformas sociais?*
- (RQ2) *Existe uma discrepância significativa entre o conhecimento mensurado e o autodeclarado pelos pais em relação ao gerenciamento da privacidade digital dos filhos?*
- (RQ3) *Os pais podem gerenciar a privacidade dos filhos nas plataformas sociais?*

5.1. Aplicação de pesquisa

A pesquisa foi realizada por meio de um questionário online elaborado para avaliar a compreensão e as práticas dos pais e responsáveis em relação à privacidade digital das crianças. Além das questões apresentadas na Tabela 2, também foram incluídas perguntas de perfil para identificar o gênero e a faixa etária dos respondentes. Antes da distribuição, o questionário foi revisado e aprovado pelo comitê de ética da universidade, assegurando a conformidade com os padrões éticos de pesquisa. A pesquisa foi disponibilizada por meio de um link público e amplamente divulgada por meio de redes sociais e plataformas de mensagens, com o objetivo de alcançar um público diversificado. Ao total 77 pessoas responderam ao questionário, informando seu nível de conscientização, envolvimento e medidas tomadas para proteger os dados de seus filhos em plataformas digitais. As respostas coletadas foram então analisadas para determinar o nível de maturidade de cada participante, com base em seu conhecimento e comportamentos alinhados aos principais princípios de privacidade.

Figura 1 apresenta o perfil dos entrevistados. A análise dos dados revelou que a maioria dos entrevistados tinha entre 26 e 45 anos. (86%). Em relação à escolaridade, observou-se um predomínio de pessoas com ensino superior completo, sendo (83%). Este perfil indica um grupo com razoável acesso à informação, o que é favorável às discussões sobre privacidade digital e proteção de dados. A distribuição por gênero pendeu para o masculino, com 69% se identificando como homem e 31% como mulher. A maioria das crianças tinha entre 2 e 5 anos (49%), uma fase marcada por intenso desenvolvimento e interação precoce com tecnologias digitais. Percentuais menores foram encontrados entre os grupos de 6 a 9 e 10 a 12 anos, sugerindo que a exposição digital começa antes da idade típica para o uso independente de dispositivos. Notavelmente, 23% das crianças tinham seus próprios perfis em plataformas digitais, apesar de muitas estarem abaixo da idade mínima exigida. Essa presença precoce nas redes sociais apresenta riscos, como exposição a conteúdo inapropriado, uso indevido de dados e publicidade direcionada. YouTube Kids foi a plataforma mais utilizada (56%), seguida pelo tiktok (17%), Instagram (IG) (10%), e YouTube (9%), com outras plataformas contando em 9%.

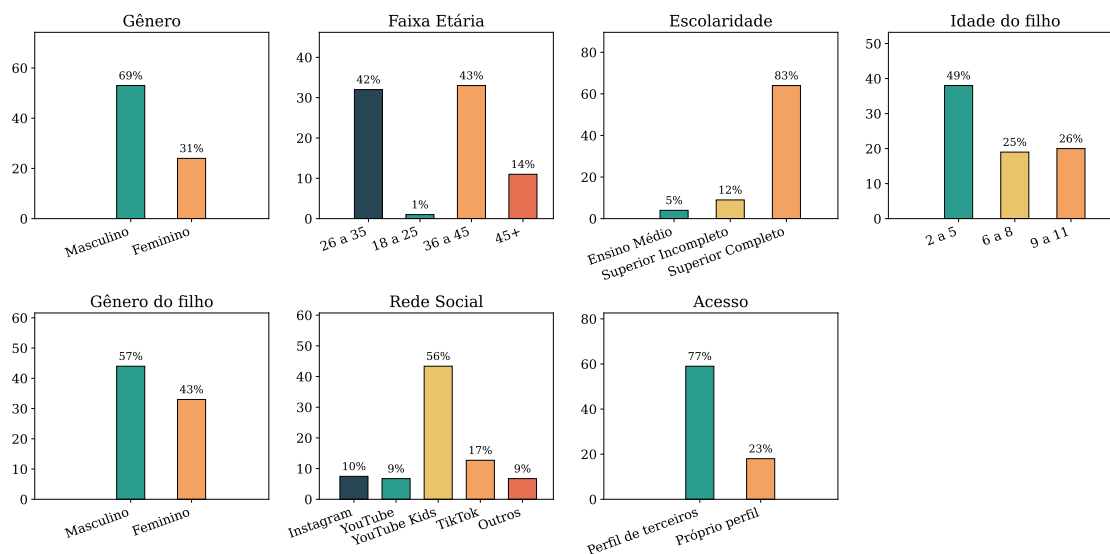


Figura 1. Visão geral do perfil dos entrevistados da pesquisa

5.2. A Maturidade Parental na Privacidade Infantil

Para responder à Pergunta 1, analisamos o conhecimento autodeclarado dos pais sobre a gestão da privacidade dos filhos em plataformas sociais, com base nas respostas a uma escala Likert aplicada às questões listadas na Tabela 2 (*Conhecimento autodeclarado*). O objetivo é investigar como os pais se avaliam quanto à gestão da privacidade dos filhos nas plataformas sociais. A Figura 2 apresenta as distribuições de respostas para cada atributo de privacidade avaliado com base na escala Likert. A análise do conhecimento autodeclarado revelou que muitos entrevistados acreditam estar familiarizados com os marcos legais que regulam a privacidade de crianças em ambientes digitais. Metade (50%) afirmou saber que a LGPD define criança como alguém com menos de 12 anos, enquanto 35% não tinham certeza e 14% admitiram abertamente que não sabiam. Da mesma forma, 65% dos participantes afirmaram estar cientes da exigência legal de autorização dos pais para o uso de redes sociais por crianças, e 55% afirmaram saber que os pais ou responsáveis são legalmente responsáveis pelas atividades online de seus filhos.

Quando questionados sobre sua compreensão do papel das plataformas digitais, a grande maioria expressou concordância de que as plataformas devem solicitar autorização dos pais, mesmo que a criança seja tecnicamente capaz de criar um perfil de forma independente. No entanto, apenas 22% os entrevistados afirmaram que os avisos de privacidade apresentados pelas plataformas são claros, enquanto 40% os consideraram pouco claros ou nada claros. Embora essa percepção não mensure o conhecimento real, ela reflete uma postura crítica em relação à transparência das práticas atuais de processamento de dados. Por fim, apesar da desaprovação dos participantes em relação às práticas comerciais envolvendo dados de crianças—56% se opuseram ao seu uso para publicidade e rastreamento de geolocalização—essas opiniões, como indicadores autodeclarados, revelam uma sensibilidade geral às preocupações com a privacidade e um alinhamento expresso com os princípios de proteção de dados de crianças.

Para abordar o RQ2, examinamos a lacuna entre o conhecimento autodeclarado pelos pais e a métrica do conhecimento. Conforme detalhado na tabela 2, essa métrica

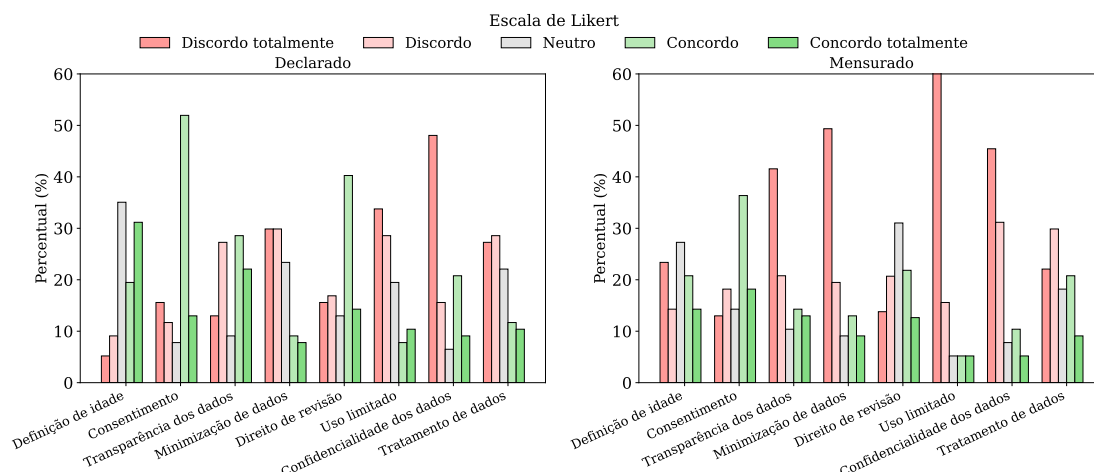


Figura 2. Distribuição das respostas da pesquisa de acordo com cada atributo de privacidade avaliado (Tabela 1).

de conhecimento irá refletir o grau de alinhamento entre as respostas dos pais e as atuais estruturas legais e sociais que regem a privacidade infantil. Ao comparar a concordância demonstrada com essas diretrizes com a familiaridade autodeclarada, é possível avaliar de forma mais precisa o nível de maturidade e a real preparação dos pais para gerenciar a privacidade digital de seus filhos. A figura 2 apresenta uma visão geral do conhecimento autodeclarado *vs.* o conhecimento medido dos entrevistados. A análise destaca uma discrepância consistente entre o que os pais acreditam saber e sua compreensão das responsabilidades relacionadas à privacidade de acordo com as regulamentações atuais. Embora 50% dos entrevistados tenham afirmado estar familiarizados com a definição legal de criança de acordo com a LGPD, a maioria desse grupo discordou da restrição de idade mínima de 13 anos estabelecida por grandes plataformas como Instagram e TikTok. Isso indica que muitos responsáveis que afirmam ter conhecimento legal podem não compreender ou internalizar totalmente as implicações dessas regulamentações.

Ao avaliar responsabilidades mais específicas, como a responsabilidade parental pelas ações dos filhos online, apenas 51% dos participantes reconheceram essa obrigação, e uma parcela significativa negou conhecimento ou expressou incerteza. Mesmo entre aqueles que afirmaram conhecer as práticas de processamento de dados, poucos demonstraram uma compreensão completa de como seus dados — e os de seus filhos — são coletados, usados ou compartilhados. A percepção dos avisos de privacidade fornecidos pelas plataformas digitais demonstra ainda mais essa lacuna, visto que 25% os consideraram claros e apenas 16% dentre esse grupo, poucos demonstraram uma compreensão consistente dos princípios fundamentais de proteção de dados, o que indica a eficácia limitada dos atuais mecanismos de consentimento. Essas descobertas indicam que muitos pais acreditam ser capazes de gerenciar a privacidade digital de seus filhos, mas seu preparo é limitado. Os legislações atuais assumem que os pais podem proteger efetivamente os dados de seus filhos e garantir os padrões de privacidade.

Para responder à Pergunta 3, é necessário aprofundar a análise dos resultados da pesquisa. As evidências indicam que os pais não estão totalmente preparados para gerenciar de maneira consistente e eficaz a privacidade digital de seus filhos em plataformas sociais. Embora muitos entrevistados afirmem estar familiarizados com as definições,

requisitos e responsabilidades legais relacionadas à presença online das crianças, suas respostas a perguntas específicas, baseadas em conhecimento, revelam discrepâncias significativas entre o que acreditam saber e o que realmente compreendem. Além disso, embora muitos pais apoiem a ideia de responsabilidade legal pelas ações digitais de seus filhos, frequentemente não têm clareza sobre como os dados são coletados, compartilhados e processados pelas plataformas, especialmente em relação ao rastreamento por terceiros e à publicidade direcionada. Essa discrepância entre o conhecimento autodeclarado e o efetivamente demonstrado levanta preocupações sobre a eficácia de depender exclusivamente da supervisão parental para garantir a privacidade digital das crianças.

6. Conclusão

O uso generalizado de plataformas digitais por crianças tem intensificado as preocupações sobre a adequação das proteções de privacidade. A legislação atual atribui aos pais e responsáveis a responsabilidade de gerenciar a privacidade das crianças, assumindo que eles possuam o conhecimento necessário para tomar decisões informadas. Para tratar essa questão, propomos uma abordagem em duas fases. Primeiramente, identificamos os principais atributos de privacidade relevantes para a proteção de dados de crianças, com base no GDPR, COPPA e LGPD, estabelecendo uma base normativa sólida. Em seguida, entrevistamos 77 pais e responsáveis para avaliar sua maturidade, definida pela conscientização, compreensão e capacidade de aplicar medidas relacionadas à privacidade. Nossas descobertas revelam uma lacuna significativa entre o conhecimento autodeclarado e o real, indicando que muitos responsáveis podem não estar totalmente preparados para cumprir as responsabilidades de privacidade previstas pela legislação.”

Agradecimentos

Este trabalho foi parcialmente patrocinado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), por meio das bolsas nº 304990/2021-3, 407879/2023-4, 302937/2023-4 e 442262/2024-8.

Referências

- Abreu, M. F., Viegas, E. K., and Santin, A. O. (2024). *A Review of Social Network Regulations and Mechanisms for Safeguarding Children’s Privacy*, page 427–438. Springer Nature Switzerland.
- Albuquerque, O. d. P., Fantinato, M., Eler, M. M., Peres, S. M., and Hung, P. C. K. (2020). A study of parental control requirements for smart toys. In *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, page 2215–2220. IEEE.
- Alomar, N. and Egelman, S. (2022). Developers say the darnedest things: Privacy compliance processes followed by developers of child-directed apps. *Proceedings on Privacy Enhancing Technologies*, 2022(4):250–273.
- Amon, M. J., Kartvelishvili, N., Bertenthal, B. I., Hugenberg, K., and Kapadia, A. (2022). 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*, 6(CSCW1):1–30.
- CGI.br (2024). Microdata ict kids online brazil 2024 - children and adolescents.

- de Oliveira, V. M., de Oliveira, H. M., Santos, G. M., Geremias, J., and Viegas, E. K. (2025). A big data framework for scalable and cross-dataset capable machine learning in network intrusion detection systems. *IEEE Access*, 13:129419–129431.
- Dorfleitner, G., Hornuf, L., and Kreppmeier, J. (2023). Promise not fulfilled: Fintech, data privacy, and the gdpr. *Electronic Markets*, 33(1).
- Ekambaranathan, A., Zhao, J., and Van Kleek, M. (2023). How can we design privacy-friendly apps for children? using a research through design process to understand developers’ needs and challenges. *Proceedings of the ACM on Human-Computer Interaction*, (CSCW2):1–29.
- Etzel, R. A. (2020). The special vulnerability of children. *International Journal of Hygiene and Environmental Health*, 227:113516.
- Filho, A. G., Viegas, E. K., Santin, A. O., and Geremias, J. (2025). A dynamic network intrusion detection model for infrastructure as code deployed environments. *Journal of Network and Systems Management*, 33(4).
- Geremias, J., Viegas, E. K., Santin, A. O., Britto, A., and Horschulhack, P. (2023). Towards a reliable hierarchical android malware detection through image-based cnn. In *2023 IEEE 20th Consumer Communications amp; Networking Conference (CCNC)*, page 242–247. IEEE.
- Ismagilova, E., Hughes, L., Rana, N. P., and Dwivedi, Y. K. (2020). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, 24(2):393–414.
- Jain, A. K., Sahoo, S. R., and Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex amp; Intelligent Systems*, 7(5):2157–2177.
- Landis, C. B. and Kroll, J. A. (2024). Mitigating inference risks with the nist privacy framework. *Proceedings on Privacy Enhancing Technologies*, 2024(1):217–231.
- Neitzke, C., Mendes, J., Rivero, L., Teixeira, M., and Viana, D. (2023). Enhancing lgpd compliance: Evaluating a checklist for lgpd quality attributes within a government office. In *Proceedings of the XXII Brazilian Symposium on Software Quality, SBQS ’23*, page 218–227. ACM.
- Salgado, A. d. L., Singh, B., Hung, P. C. K., Jiang, A., Liu, Y.-H., Wheler, A. P. d. A., and Gaber, H. A. (2020). Preliminary tendencies of users’ expectations about privacy on connected-autonomous vehicles. In *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, page 296–301. IEEE.
- Simioni, J., Viegas, E. K., Santin, A., and Horschulhack, P. (2025a). An early exit deep neural network for fast inference intrusion detection. In *Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing, SAC ’25*, page 730–737. ACM.
- Simioni, J. A., Viegas, E. K., Santin, A. O., and de Matos, E. (2025b). An energy-efficient intrusion detection offloading based on dnn for edge computing. *IEEE Internet of Things Journal*, 12(12):20326–20342.

- Sun, R., Xue, M., Tyson, G., Wang, S., Camtepe, S., and Nepal, S. (2023). Not seen, not heard in the digital world! measuring privacy practices in children’s apps. In *Proceedings of the ACM Web Conference 2023*, WWW ’23, page 2166–2177. ACM.
- Thammaratchuchai, S., Nutsuda, N., and Jantori, P. (2023). The awareness of child privacy of thai parents on social media. *Human Behavior, Development and Society*, 24(3):1–10.
- Vlajic, N., El Masri, M., Riva, G. M., Barry, M., and Doran, D. (2018). 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*, CCS ’18. ACM.
- Zaeem, R. N. and Barber, K. S. (2020). The effect of the gdpr on privacy policies: Recent progress and future promise. *ACM Transactions on Management Information Systems*, 12(1):1–20.