

Mykaele Fortes Abreu

**A PRIVACIDADE INFANTIL EM REDES SOCIAIS
BASEADA NA CONSCIENTIZAÇÃO DOS RESPONSÁVEIS**

**MESTRADO EM
INFORMÁTICA
PUCPR**

**CURITIBA
2025**

MYKAELE FORTES ABREU

**A PRIVACIDADE INFANTIL EM REDES SOCIAIS BASEADA NA
CONSCIENTIZAÇÃO DOS RESPONSÁVEIS**

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná, como requisito parcial à obtenção do título de mestre em Informática.
Área de Concentração: Ciência da Computação
Orientador: Prof. Dr. Altair Olivo Santin

Pontifícia Universidade Católica do Paraná
Programa de Pós-Graduação em Informática

CURITIBA

2025

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central

Bibliotecária: Luci Eduarda Wielganczuk – CRB 9/1118

A162p 2025	Abreu, Mykaele Fortes Abreu A privacidade infantil em redes sociais baseada na conscientização dos responsáveis / Mykaele Fortes Abreu ; orientador: Altair Olivo Santin. – 2025. 105 f. : il. ; 30 cm
	Dissertação (mestrado) – Pontifícia Universidade Católica do Paraná, Curitiba, 2025 Bibliografia: f. 91-99
	1. Informática. 2. Privacidade infantil. 3. Proteção de dados. 4. Parentalidade. 5. Segurança de computadores. 6. Redes sociais. 7. Internet e crianças. I. Santin, Altair Olivo. II. Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Informática. III. Título.
	CDD. 20. ed. – 004



Pontifícia Universidade Católica do Paraná
Escola Politécnica
Programa de Pós-Graduação em Informática

Curitiba, 22 de agosto de 2025.

91-2025

DECLARAÇÃO

Declaro para os devidos fins, que **MYKAELE FORTES ABREU** defendeu a dissertação de Mestrado intitulada “A Privacidade Infantil em Redes Sociais Baseada na Conscientização dos Responsáveis”, na área de concentração Ciência da Computação no dia 11 de julho de 2025, no qual foi aprovada.

Declaro ainda, que foram feitas todas as alterações solicitadas pela Banca Examinadora, cumprindo todas as normas de formatação definidas pelo Programa.

Por ser verdade, firmo a presente declaração.

Documento assinado digitalmente
gov.br JEAN PAUL BARDDAL
Data: 25/08/2025 09:28:53 -0300
Verifique em <https://validar.br.gov.br>

Prof. Dr. Jean Paul Barddal
Coordenador do Programa de Pós-Graduação em Informática

AGRADECIMENTOS

A Deus, por me conceder sabedoria para enfrentar cada etapa desta jornada.

Ao meu marido e aos meus filhos, por serem minha base e minha maior motivação.

Aos meus pais, por todo o incentivo e por sempre acreditarem em mim.

Ao Prof. Dr. Altair Olivo Santin, pela confiança depositada, pelas valiosas oportunidades durante o mestrado, pelos ensinamentos imprescindíveis e pela paciência ao longo dos desafios enfrentados.

Ao Prof. Dr. Eduardo Kugler Viegas, pela parceria e orientações em cada etapa deste processo. Aos professores do PPGIa, por compartilharem seu conhecimento e por contribuírem para minha formação acadêmica.

Agradeço à Pontifícia Universidade Católica do Paraná (PUCPR) pela estrutura e ambiente de aprendizado proporcionados durante o meu mestrado.

Ao Programa de Pós-Graduação em Informática (PPGIa), pela concessão do auxílio da comissão de bolsas. O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal Nível Superior – Brasil (CAPES) – Código do Financiamento 001.

RESUMO

A legislação vigente, como a LGPD, atribui aos pais a responsabilidade de gerenciar a privacidade das crianças, presumindo um nível de conhecimento das redes sociais que usam. Diante disso, este trabalho avalia o nível de proteção da privacidade infantil em redes sociais, com base no nível de conscientização de pais, responsáveis e tutores quanto ao conhecimento e uso dos recursos de privacidade. Primeiramente, identificamos os principais atributos de privacidade relevantes para a proteção de dados online de crianças, com base na análise das legislações vigentes, como a GDPR, a COPPA e a LGPD. Na etapa seguinte, avaliamos o nível de proteção da privacidade infantil por meio da análise do nível de conscientização de 77 pais e responsáveis, considerando aspectos práticos em relação às medidas de privacidade oferecidas pelas redes sociais. A maior parte, 77%, situa-se no nível Ausência de conscientização, sem conhecimento dos riscos digitais nem adoção de medidas de proteção ou no Nível de Conscientização limitada, com entendimento superficial e pouca ou nenhuma ação prática. Os resultados revelam uma discrepância significativa entre a autoavaliação de conhecimento e o real, indicando que é necessário preparar pais e responsáveis para atender às exigências das regulamentações vigentes.

Palavras-chave: Privacidade Infantil, Redes Sociais, Conscientização Parental, Proteção de dados, Configurações de Privacidade.

ABSTRACT

Current legislation, such as the LGPD, assigns parents the responsibility for managing children's privacy, assuming a level of knowledge of the social networks they use. In view of this, this work evaluates the level of protection of children's privacy on social networks, based on the level of awareness of parents, guardians and tutors regarding the knowledge and use of privacy resources. First, we identify the main privacy attributes relevant to the protection of children's online data, based on the analysis of current legislation, such as the GDPR, COPPA and the LGPD. In the next step, we evaluate the level of protection of children's privacy by analyzing the level of awareness of 77 parents and guardians, considering practical aspects regarding the privacy measures offered by social networks. The majority, 77%, are at the level of No Awareness, with no knowledge of digital risks or adoption of protective measures, or at the Level of Limited Awareness, with superficial understanding and little or no practical action. The results reveal a significant discrepancy between self-assessed knowledge and actual knowledge, indicating that it is necessary to prepare parents and guardians to meet the requirements of current regulations

Keywords: Children's Privacy, Social Networks, Parental awareness, Data Protection, Privacy Settings.

LISTA DE FIGURAS

Figura 1. Método Proposto	52
Figura 2. Visão geral do perfil dos entrevistados da pesquisa.....	78
Figura 3. Distribuição das respostas da pesquisa de acordo com cada atributo de privacidade avaliado (Tabela 2)	80
Figura 4. Distribuição dos respondentes por nível de conscientização	86

LISTA DE TABELAS

Tabela 1. Trabalhos relacionados comparados ao trabalho proposto.....	49
Tabela 2 . Sumarização dos atributos de privacidade de dados.....	58
Tabela 3. Sumarização dos Mecanismos de Privacidade das Redes Sociais.....	67
Tabela 4.Perguntas do Formulário.....	71

LISTA DE ABREVIATURAS E SIGLAS

COPPA	Children's Online Privacy Protection
GDPR	Regulamento Geral de Proteção de Dados
LGPD	Lei Geral de Proteção de Dados
TIC KIDS	Tecnologia da informação e comunicação por crianças e adolescentes
NIDS	Network Intrusion Detection System
PQ	Pergunta de Pesquisa

SUMÁRIO

CAPÍTULO 1 INTRODUÇÃO	14
1.1. Contextualização.....	14
1.2. Motivação	15
1.3. Objetivos.....	17
1.3.1. Objetivo Geral	17
1.3.2. Objetivos Específicos	17
1.4. Contribuições	18
1.5. Estrutura do Documento	19
CAPÍTULO 2 FUNDAMENTAÇÃO TEÓRICA.....	20
2.1. Privacidade de Dados.....	20
2.1.1. Função Identificar.....	21
2.1.2. Função Governar	22
2.1.3. Função Controlar	23
2.1.4. Função Comunicar.....	24
2.1.5. Função Proteger.....	26
2.2. Aspectos Legais de Privacidade	27
2.2.1. GDPR	29
2.2.2. LGPD.....	30
2.2.3. COPPA	31
2.3. Desafios de Privacidade para Crianças	32
2.4. Privacidade de Crianças	35
2.5. Modelo de Maturidade.....	37
CAPÍTULO 3 TRABALHOS RELACIONADOS	40
3.1. Privacidade em Redes Sociais	40
3.2. Privacidade de Crianças em Redes Sociais.....	43

3.3.	Discussão	49
CAPÍTULO 4 METODOLOGIA.....		52
4.1.	Aspectos de Privacidade	53
4.1.1	Sumarização.....	56
4.2	Mecanismos que são implementados nas redes sociais	61
4.2.3	Dados Pessoais	62
4.2.4	Idade, Consentimento dos pais ou dos responsáveis	63
4.2.5	Transparência do uso das informações e Direito de revisar os dados	64
4.2.6	Minimização de dados e Finalidade Limitada	65
4.2.7	Aviso de Tratamento de dados	65
4.2.8	Design Orientado à privacidade	66
4.3	Modelo de Conscientização Para Proteção de Privacidade das crianças	68
CAPÍTULO 5 COLETA E ANÁLISE DE DADOS		75
5.1	Aplicação da Pesquisa	75
5.2	Análise do Perfil dos Participantes	77
5.3.1	Definição de idade	81
5.3.2	Consentimento dos Pais	81
5.3.3	Transparência dos dados	81
5.3.5	Revisão dos Dados.....	82
5.3.7	Confidencialidade das Informações.....	83
5.3.8	Aviso de Tratamento de Dados.....	83
5.3.9	Perguntas de Pesquisa	84
5.4	A Conscientização Parental na Privacidade Infantil.....	85
5.5	Medidas de conscientização e educação de pais e responsáveis.....	87
6	CONCLUSÃO.....	90
6.1	Trabalhos futuros	92
6.2	Publicações Científicas	93
REFERÊNCIAS		94

7	ANEXOS	103
7.1	Parecer consubstanciado do CEP	103

Capítulo 1

Introdução

1.1. Contextualização

A ascensão da tecnologia digital e das redes sociais tem transformado a forma como as pessoas de todas as idades se comunicam, trazendo a luz preocupações significativas sobre a privacidade dos usuários, especialmente aqueles menores de idade. A privacidade de crianças e adolescentes é crucial na era digital devido às inúmeras ameaças existentes em um cenário digital, como a coleta inapropriada de informações, publicidade direcionada e interações suspeitas.

Nos últimos anos o número de crianças e adolescentes que fazem uso de redes sociais, tais como o TikTok, YouTube, Facebook e Instagram, tem crescido significativamente. De acordo com a 10ª edição da *TIC kids*, foram entrevistadas presencialmente 2.704 crianças e adolescentes, com idades entre 9 e 17 anos, assim como seus pais e responsáveis, em todo território nacional. A pesquisa revelou dados alarmantes: 24% dos entrevistados relataram ter começado a se conectar à Internet ainda na primeira infância, ou seja, até os 6 anos de idade. (TIC-online, 2024) A pesquisa também apresenta que 93% da população de 9 a 17 anos mantém um perfil em redes sociais. Dentre esses, 88% das crianças e dos adolescentes disseram que tem acesso a plataforma de vídeos Youtube, 78% disseram ter WhatsApp, 66% disseram ter Instagram e 63% disseram ter TikTok. Ainda, a plataforma mais utilizada entre as crianças de 9 a 12 anos é o Youtube. Logo, as crianças estão cada vez mais presentes no ambiente digital, expondo-as à coleta de dados pessoais e informações sensíveis, trazendo preocupações significativas sobre sua segurança e privacidade. Além disso, um dado alarmante é que destes usuários, apenas 28% das crianças e adolescentes de 9 a 17 anos têm pais, mães ou responsáveis que afirmam utilizar “filtros” ou configurações que restrinjam o contato com propaganda na rede. (TIC-online, 2024)

Devido à complexidade do tema, ao longo dos últimos anos foram promulgadas várias leis com o propósito de proteger os dados pessoais, abrangendo a proteção das

crianças, como o Regulamento Geral de Proteção de Dados (GDPR) na Europa e a Lei Geral de Proteção de Dados (LGPD) no Brasil, que tratam de forma geral da proteção de dados pessoais. Neste contexto, nos Estados Unidos, a Lei de Privacidade Online Infantil (COPPA) foi criada especificamente para abordar a proteção de dados das crianças. (UNICEF,2020)

A GDPR, em vigor desde 2018, foi estabelecida para fortalecer e harmonizar as leis de proteção de dados pessoais na União Europeia. A LGPD, implementada em 2020, segue uma abordagem semelhante, regulamentando o tratamento de dados pessoais. Em essência, ambas as leis compartilham o objetivo comum de orientar a aquisição, manipulação e armazenamento de informações pessoais, tanto de adultos quanto de crianças. Por outro lado, a COPPA, criada nos Estados Unidos em 1998, tem como principal finalidade a proteção da privacidade de crianças menores de 13 anos, proporcionando aos pais um maior controle sobre as informações que sites e aplicativos podem coletar de seus filhos. Além disso, aborda questões relacionadas ao marketing direcionado e promove a conscientização sobre a segurança online. Neste cenário, o constante avanço tecnológico das redes sociais gera diversos desafios para garantir a privacidade dos usuários, demandando adaptações regulatórias contínuas.

1.2. Motivação

A privacidade de crianças constitui um tema de extrema relevância, à medida que a adoção de tecnologias online e dispositivos móveis por parte de menores de idade apresenta um crescimento nos últimos anos. Esse aumento na exposição das crianças ao ambiente tecnológico tem gerado a habitual coleta e processamento de dados por parte dos provedores de serviço, porém, simultaneamente, tem exposto esse grupo etário a consideráveis riscos no que tange à sua privacidade.

Crianças podem ser categorizados como sujeitos vulneráveis em virtude de múltiplos fatores. Isso ocorre devido ao contínuo desenvolvimento físico e mental das crianças, com isso é necessário que adultos supervisionem e amparem para assegurar sua segurança e privacidade. Ademais, tal vulnerabilidade é corroborada pela sua inerente fragilidade física e psicológica, juntamente com a sua limitada capacidade de tomar decisões autônomas. Para tratar essa condição de vulnerabilidade das crianças, observa-se a existência de direitos especiais reconhecidos tanto em âmbito internacional quanto nacional. Além disso, essa vulnerabilidade irá exigir que haja uma supervisão

contínua dos pais, responsáveis e tutores para garantir a proteção da privacidade dos dados das crianças. (ONU, 1989)

O papel dos pais, responsáveis e tutores na proteção de privacidade de dados é crucial, já que eles são os principais responsáveis por garantir que as crianças compreendam os riscos de compartilhar os dados, bem como protegê-las. Entretanto, a prevalente falta de transparência nas redes sociais dificulta a compreensão adequada de suas políticas, práticas de coleta de dados e a implementação de mecanismos de segurança e privacidade.

Um aspecto fundamental consiste na avaliação do nível de proteção da privacidade de crianças em redes sociais, considerando o nível de conscientização de pais, responsáveis e tutores quanto ao conhecimento e uso dos mecanismos de privacidade e segurança disponibilizados por essas plataformas. Nesse contexto, definimos o conceito de “conscientização”, como a capacidade dos pais de reconhecerem os riscos associados ao uso de redes sociais, bem como a capacidade de identificar medidas de proteção eficaz para assegurar a privacidade e a segurança dos dados pessoais das crianças.

Outro fator a ser observado, é a falta de padronização em relação aos mecanismos de proteção de dados das crianças. Além disso, a LGPD, COPPA e GDPR não oferecem uma definição consensual sobre menores de idade no contexto das questões de privacidade, resultando em uma margem para interpretações jurídicas. Essa falta de padronização cria uma lacuna na proteção dos dados das crianças, no qual os responsáveis muitas vezes não sabem identificar ou exigir o cumprimento das regulamentações.

Apesar das leis existentes, os provedores de serviços digitais frequentemente não implementam mecanismos robustos para garantir a conformidade com essas normas, como a verificação eficaz do consentimento dos pais ou a aplicação de controles de segurança mais rigorosos. Além disso, pouco se sabe sobre a forma como os pais percebem esses mecanismos e sua capacidade de utilizá-los adequadamente para proteger os dados de seus filhos. Para preencher essa lacuna, é fundamental entender o nível de conscientização dos pais em relação à privacidade digital e as estratégias educacionais que podem ser implementadas para melhorar a segurança online para as crianças

1.3. Objetivos

1.3.1. Objetivo Geral

O objetivo geral deste trabalho é avaliar o nível de proteção da privacidade de crianças em redes sociais, a partir do nível de conscientização dos pais, responsáveis e tutores em relação ao conhecimento e à utilização dos mecanismos de privacidade e segurança oferecidos por essas plataformas.

1.3.2. Objetivos Específicos

Para alcançar o objetivo geral deste trabalho, as seguintes demandas devem ser atendidas:

1. Revisão da literatura dos aspectos de privacidade em redes sociais para menores de idade;
2. Avaliar o nível de proteção da privacidade de crianças em redes sociais;
3. Analisar o nível de conscientização dos pais e responsáveis sobre as políticas de privacidade e os mecanismos de segurança oferecidos pelas principais redes sociais utilizadas por crianças e adolescentes.
4. Propor medidas de conscientização e educação de pais e responsáveis com relação a privacidade de crianças em redes sociais.

1.3.3. Questões de Pesquisa

Com base nos objetivos apresentados, a pesquisa busca responder às seguintes questões:

RQ1: Qual é o conhecimento autodeclarado dos pais sobre como gerenciar a privacidade dos filhos em redes sociais?

RQ2: Existe uma discrepância significativa entre o conhecimento mensurado e o auto-declarado pelos pais em relação ao gerenciamento da privacidade digital dos filhos?

RQ3: Os pais são capazes de gerenciar a privacidade dos filhos nas redes sociais?

1.4. Contribuições

As contribuições deste trabalho concentram-se na análise da proteção da privacidade infantil em redes sociais, a partir da avaliação do nível de conscientização dos pais, responsáveis e tutores quanto ao conhecimento e uso dos mecanismos de privacidade e segurança disponíveis. Essa análise possibilita identificar lacunas de conhecimento que podem comprometer a efetividade dessa proteção, considerando que os responsáveis nem sempre estão plenamente cientes dos riscos aos quais as crianças estão expostas. Além de servir como base para orientar políticas públicas, isso porque quando avaliamos o nível de conscientização dos responsáveis, podemos indicar a necessidade de regulamentações mais claras e eficazes. Desta forma, de maneira mais detalhada, as contribuições são apresentadas a seguir:

- I. Análise crítica da proteção da privacidade infantil em ambientes digitais, considerando o contexto de uso de redes sociais por crianças e o papel mediador dos adultos em relação aos riscos e mecanismos de segurança disponíveis.
- II. O trabalho proporciona uma visão clara sobre o nível de conscientização e entendimento que os pais e responsáveis têm em relação aos mecanismos de privacidade nas redes sociais.
- III. Realização de uma análise comparativa das legislações nacionais e internacionais relevantes, destacando as melhores práticas e identificando lacunas na proteção atual.
- IV. Apoio à Educação e Conscientização: Criação de materiais educativos e programas de conscientização para crianças, pais e educadores sobre a importância da privacidade e como protegê-la nas redes sociais.

- V. Os resultados podem ser utilizados pelos legisladores para desenvolver regulamentações e diretrizes que protejam melhor a privacidade das crianças nas redes sociais.

1.5. Estrutura do Documento

O documento está organizado de forma que apresenta a introdução no Capítulo 1, a fundamentação teórica no Capítulo 2, tratando sobre os desafios da privacidade infantil, abordando os problemas principais deste tema. O Capítulo 3 aborda os trabalhos relacionados e como eles tratam o problema proposto no trabalho. O Capítulo 4 apresenta a Metodologia do trabalho. Depois, o capítulo 5 irá apresentar a coleta de dados e os resultados do trabalho. E, por fim, o capítulo 6 irá concluir o trabalho, juntamente com as considerações finais.

Capítulo 2

Fundamentação Teórica

Com o avanço tecnológico, tornou-se possível coletar, armazenar e analisar uma grande quantidade de dados. A privacidade de dados é um tema relevante e atual, já que as informações pessoais estão mais suscetíveis a serem coletadas e utilizadas para diversos fins. Dessa forma, este capítulo visa apresentar os conceitos de privacidade, os aspectos legais de privacidade, e os desafios relacionados a privacidade para crianças.

2.1. Privacidade de Dados

Atualmente, a privacidade de dados é um tema amplamente discutido na sociedade, devido aos seus impactos e a sua relevância. Com a evolução tecnológica, houve um aumento no número de pessoas que passaram a ter acesso à Internet. Como consequência, a combinação de diversas técnicas, tais como coleta, registro, processamento, cruzamento e transmissão de dados, possibilitou a obtenção de informações intrínsecas das pessoas.

A privacidade pode ser definida como a capacidade do indivíduo de controlar o acesso aos seus dados pessoais (NIST, 2020). Normalmente, a privacidade é analisada sob duas óticas: a primeira, é um direito fundamental do indivíduo de decidir sobre a coleta e o processamento dos seus dados, bem como o direito de ter a sua informação segura. A segunda, refere-se as medidas técnicas que devem ser implementadas para que possa garantir que as informações armazenadas e processadas pelos sistemas computacionais sejam autênticas, confidenciais e integras.

Nesse sentido, o NIST (*National Institute of Standards and Technology*) ressalta que os indivíduos podem não perceberem completamente as consequências da sua privacidade na medida que interagem com sistemas, produtos ou serviços. Assim, o NIST criou um Framework de Gerenciamento de Riscos de Privacidade, que possui um

conjunto de diretrizes e processos para orientar as organizações a identificarem, avaliarem e gerenciarem os riscos de privacidade.

Os riscos de privacidade ocorrem quando há um efeito adverso no processamento dos dados. Essa adversidade nem sempre é associada a incidentes de cibersegurança, como ataques cibernéticos que violam a confidencialidade, integridade ou disponibilidade. Por exemplo, no contexto de cidades inteligentes, foram desenvolvidos medidores inteligentes de energia que tinham a capacidade de coletar, registrar e distribuir informações sobre o uso de eletricidade residencial, com o objetivo de aumentar a eficiência energética. Essas informações permitiram inferir o comportamento das pessoas dentro das suas casas, fazendo com que as pessoas se sentissem vigiadas.

Além disso, é importante destacar que uma organização possui riscos de privacidade, mesmo que esteja em compliance com as leis, regulamentos, normas e padrões. Dessa maneira, as organizações podem mitigar os riscos adotando alguns procedimentos de gestão de riscos de privacidade. O Framework do NIST sugere a adoção de cinco funções fundamentais para apoiar a organização no gerenciamento de riscos de privacidade decorrente do processamento de dados, descritas a seguir (NIST, 2020).

2.1.1. Função Identificar

A função identificar refere-se à primeira etapa do processo de gerenciamento de risco de privacidade. Essa etapa é projetada para ajudar as organizações a entenderem o contexto em que operam, identificando e documentando as atividades relacionadas ao processamento de dados pessoais, envolvendo a coleta de informações essenciais sobre o tratamento de dados pessoais, incluindo:

1. **Escopo:** Definir claramente os limites do tratamento de dados pessoais dentro da organização. Isso inclui identificar os sistemas, processos, projetos ou atividades que envolvem a coleta, uso e/ou compartilhamento de dados pessoais.
2. **Categorias de Dados:** Identificar as categorias específicas de dados pessoais que estão sendo processadas. Essas categorias podem incluir dados de identificação pessoal, informações de saúde, dados financeiros, etc.

3. **Partes Interessadas:** Identificar as partes interessadas envolvidas no tratamento de dados pessoais, tanto internas quanto externas. Isso pode incluir os titulares dos dados, funcionários, parceiros de negócios, entre outros.
4. **Propósitos do Tratamento:** Compreender os propósitos específicos para os quais os dados pessoais estão sendo coletados e utilizados. Isso ajuda a garantir que o tratamento esteja alinhado com as finalidades legítimas declaradas.
5. **Requisitos Legais e de Política:** Identificar e documentar os requisitos legais, regulamentares e de políticas relacionados ao tratamento de dados pessoais. Isso inclui conformidade com leis de privacidade, regulamentações setoriais e políticas internas da organização.
6. **Riscos à Privacidade:** Avaliar os riscos potenciais à privacidade associados ao tratamento de dados pessoais, considerando fatores como a sensibilidade dos dados, o volume de dados processados e os métodos de processamento.

2.1.2. *Função Governar*

A função Governar no Framework de Gerenciamento de Risco de Privacidade do NIST refere-se à atividade de estabelecer, implementar e manter um programa de governança de privacidade eficaz dentro de uma organização. O objetivo dessa função é garantir que a privacidade seja tratada como parte integrante das operações e estratégias organizacionais, criando uma base sólida para a gestão eficaz de riscos de privacidade, garantindo a conformidade contínua com as regulamentações e promovendo uma cultura organizacional centrada na privacidade. As principais atividades associadas a essa função são:

1. **Desenvolver Políticas e Procedimentos de Privacidade:** Estabelecer políticas e procedimentos claros que orientem as práticas de privacidade em toda a organização. Isso pode incluir diretrizes específicas sobre coleta, uso, armazenamento e compartilhamento de dados pessoais.
2. **Designar Responsabilidades e Papéis:** Atribuir responsabilidades específicas e designar papéis relacionados à privacidade dentro da organização. Isso pode envolver a nomeação de um Encarregado de Dados (DPO - *Data Protection Officer*) ou outras funções relacionadas.

3. **Treinamento de Conscientização:** Fornecer treinamento regular para funcionários e outras partes envolvidas nas operações da organização, a fim de aumentar a conscientização sobre práticas adequadas de privacidade e conformidade com políticas internas.
4. **Avaliação Contínua de Conformidade:** Monitorar continuamente o ambiente operacional para garantir que as práticas de privacidade estejam em conformidade com as políticas estabelecidas, leis e regulamentos aplicáveis.
5. **Implementar Mecanismos de Avaliação de Risco:** Desenvolver e utilizar mecanismos para avaliação contínua dos riscos à privacidade associados às operações da organização. Isso pode incluir Avaliações de Impacto à Privacidade (PIA) e avaliações de risco periódicas.
6. **Garantir Conformidade Legal:** Monitorar e assegurar a conformidade contínua com leis e regulamentações de privacidade aplicáveis à organização.
7. **Estabelecer Processos para Atendimento a Solicitações dos Titulares dos Dados:** Desenvolver processos eficientes para lidar com solicitações de titulares dos dados, como pedidos de acesso, correção ou exclusão de informações pessoais.
8. **Implementar Medidas de Segurança e Controles Técnicos:** Implementar medidas de segurança e controles técnicos apropriados para proteger os dados pessoais contra acessos não autorizados, perda ou vazamento.

2.1.3. Função Controlar

A função Controlar no Framework de Gerenciamento de Risco de Privacidade do NIST refere-se às atividades destinadas a desenvolver e implementar controles eficazes para mitigar os riscos identificados durante a avaliação de privacidade. Essa função permite que as organizações desenvolvam uma postura proativa para gerenciar os riscos de privacidade, implementando medidas eficazes que protegem os dados pessoais contra ameaças e riscos identificados, garantindo que as práticas de privacidade estejam alinhadas com as políticas organizacionais e as expectativas dos titulares dos dados. As principais atividades associadas à função são:

1. **Implementar Controle de Privacidade:** Desenvolver e aplicar controles específicos de privacidade destinados a mitigar os riscos identificados durante a

avaliação. Isso pode incluir controles técnicos, procedimentais e organizacionais.

2. **Utilizar Técnicas de Minimização de Dados:** Adotar práticas de minimização de dados para garantir que apenas os dados necessários e relevantes sejam coletados e processados.
3. **Utilizar Técnicas de Segurança:** Implementar medidas de segurança técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados, perda, destruição ou alteração.
4. **Monitorar e Auditar o Tratamento de Dados:** Estabelecer processos para monitorar continuamente o tratamento de dados pessoais, bem como conduzir auditorias regulares para avaliar a conformidade com as políticas e os controles de privacidade.
5. **Implementar Controles de Acesso:** Adotar controles de acesso robustos para garantir que apenas pessoas autorizadas tenham acesso aos dados pessoais.
6. **Criptografia e Pseudonimização:** Aplicar técnicas de criptografia e pseudonimização para proteger dados pessoais durante o processamento e armazenamento.
7. **Gerenciar Incidentes de Privacidade:** Estabelecer procedimentos para lidar com incidentes de privacidade, incluindo vazamentos de dados, de modo a minimizar os impactos e atender às obrigações de notificação, quando aplicável.
8. **Atualizar Controles de Privacidade:** Manter os controles de privacidade atualizados em resposta a mudanças no ambiente operacional, ameaças ou requisitos regulatórios.
9. **Avaliar os Controles de Privacidade:** Conduzir avaliações regulares para garantir a efetividade dos controles implementados, ajustando-os conforme necessário.

2.1.4. Função Comunicar

A função Comunicar no Framework de Gerenciamento de Risco de Privacidade do NIST refere-se à necessidade de estabelecer comunicações claras e transparentes sobre as práticas de privacidade da organização, tanto interna quanto externa. Essa função é

essencial para promover a confiança dos titulares de dados e manter um ambiente de transparência em relação ao tratamento de dados pessoais. As principais atividades associadas à função incluem:

1. **Desenvolver Comunicações de Privacidade Claras e Acessíveis:** Criar comunicações, como políticas de privacidade, avisos de privacidade e declarações claras, acessíveis e compreensíveis para os titulares dos dados.
2. **Disponibilizar Informações sobre Práticas de Privacidade:** Fornecer informações sobre como os dados pessoais são coletados, usados, compartilhados e protegidos, conforme especificado nas políticas de privacidade.
3. **Estabelecer Canais para Perguntas e Solicitações:** Criar canais eficazes para que os titulares dos dados possam fazer perguntas, apresentar solicitações ou expressar preocupações sobre o tratamento de seus dados pessoais.
4. **Informar sobre Direitos dos Titulares dos Dados:** Comunicar claramente os direitos dos titulares dos dados, incluindo o direito de acesso, correção, exclusão e portabilidade de seus dados pessoais.
5. **Notificar sobre Mudanças nas Práticas de Privacidade:** Informar os titulares dos dados sobre quaisquer mudanças significativas nas práticas de privacidade, políticas ou procedimentos.
6. **Comunicar Incidentes de Privacidade:** Em caso de incidentes de privacidade, comunicar prontamente aos titulares dos dados sobre a natureza do incidente, os dados afetados e as medidas tomadas para mitigar os riscos.
7. **Treinar Funcionários sobre Comunicação de Privacidade:** Educar os funcionários sobre como comunicar efetivamente as práticas de privacidade e responder a perguntas de titulares dos dados.
8. **Colaborar com Partes Interessadas Externas:** Colaborar com reguladores, autoridades de proteção de dados e outras partes interessadas externas para fornecer informações necessárias e atender a obrigações regulatórias.

2.1.5. *Função Proteger*

A função Proteger no Framework de Gerenciamento de Risco de Privacidade do NIST está centrada nas atividades que visam garantir a segurança dos dados pessoais, protegendo-os contra ameaças, acessos não autorizados, perdas ou vazamentos. Essa função é essencial para a integridade e confidencialidade dos dados pessoais e envolve uma série de práticas e controles de segurança. As principais atividades associadas à função incluem:

1. **Implementar Mecanismos de Segurança:** Implementar controles e mecanismos de segurança, tanto técnicos quanto organizacionais, para proteger os dados pessoais contra ameaças cibernéticas e físicas.
2. **Adotar Criptografia e Pseudonimização:** Utilizar técnicas de criptografia para proteger a confidencialidade dos dados pessoais durante o armazenamento e a transmissão, além de empregar práticas de pseudonimização para reduzir a identificabilidade dos dados.
3. **Gestão de Identidades e Acesso:** Estabelecer controles rigorosos de autenticação e autorização para garantir que apenas usuários autorizados tenham acesso aos dados pessoais e que esse acesso seja concedido com base em princípios de necessidade.
4. **Monitorar Atividades de Acesso aos Dados:** Implementar sistemas de monitoramento para rastrear e registrar atividades de acesso aos dados pessoais, identificando e respondendo a qualquer atividade suspeita.
5. **Estabelecer Medidas contra Ameaças Internas e Externas:** Adotar medidas para proteger contra ameaças tanto internas quanto externas, incluindo políticas de segurança da informação e procedimentos para responder a incidentes de segurança.
6. **Implementar Controles de Segurança em Sistemas e Redes:** Aplicar controles de segurança em sistemas de tecnologia da informação, redes e aplicativos para proteger os dados pessoais contra exploração ou comprometimento.

7. **Garantir a Integridade dos Dados:** Garantir a integridade dos dados pessoais, implementando controles para evitar alterações não autorizadas e detectar qualquer manipulação indevida.
8. **Gerenciar Dispositivos e Mídias de Forma Segura:** Estabelecer controles para proteger dispositivos e mídias de armazenamento que contenham dados pessoais, garantindo que eles sejam usados e descartados de maneira segura.
9. **Realizar Testes de Segurança Regularmente:** Conduzir testes regulares de segurança, como testes de intrusão e avaliações de vulnerabilidade, para identificar e corrigir possíveis fraquezas no ambiente de segurança.
10. **Manter Atualizações e Patches de Segurança:** Manter sistemas e software atualizados com as últimas atualizações de segurança para proteger contra vulnerabilidades conhecidas.

Ao adotar as orientações e boas práticas definidas no Framework de Privacidade do NIST as organizações mitigarão os riscos de privacidade. Entretanto, é essencial que existam leis que definam os direitos e responsabilidades em relação a privacidade.

2.2.Aspectos Legais de Privacidade

O direito de proteção de dados pessoais, tornou-se mais evidente, com a edição de legislações específicas e decisões judiciais de diversos países, ratificando o reconhecimento global da necessidade de preservar a privacidade dos indivíduos em meio ao avanço tecnológico. Atualmente, vários países do mundo possuem leis de proteção de dados. Esses instrumentos compartilham o mesmo ideal, no qual os dados pessoais merecem uma tutela jurídica especial.

Sob uma perspectiva jurídica, os debates acerca do direito à privacidade foram iniciados devido ao surgimento de novas técnicas e instrumentos tecnológicos, que passaram a possibilitar o acesso e a divulgação de fatos relacionados à esfera privada da pessoa. Com isso, o direito de proteger os dados pessoais trouxeram novos desafios ao ordenamento jurídico. (SCHERTEL, 2014)

Para a legislação, a privacidade de dados pessoais é uma possibilidade de tutelar a personalidade do indivíduo, contra os riscos que podem ser causados pelo tratamento desses dados. A principal função é proteger o titular desses dados e não os dados em si.

Por isso, quando as informações pessoais de um indivíduo são violadas, comprometerá sua segurança e integridade. Dessa maneira, a privacidade de dados consiste em respeitar as normas preexistentes sobre a coleta, a divulgação e o uso de informações, como nome, idade, orientação sexual, raça, crenças religiosas, filosóficas, dados financeiros, entre outros (FONTES, 2010). Sendo assim, a privacidade será violada quando a manipulação das informações não está alinhada com as normas que são esperadas pela sociedade (NISSENBAUM, 2010).

Atualmente, muitos países buscam proteger os direitos de privacidade em um ambiente digital, por isso, as regulamentações acerca do tema estão sempre em evolução. Como exemplo, podemos citar algumas das leis que existem ao redor do mundo: Austrália: Princípios Australianos de Privacidade (APP) Brasil: Lei Geral de Proteção de dados (LGPD) Canadá: Lei de Privacidade da Informação Pessoal e Eletrônica (PIPEDA), Califórnia: Lei da Califórnia de Privacidade do Consumidor (CCPA), Japão: Emenda APPI de 2017 (APPI), União Europeia: Regulamento Geral de Proteção de dados.

A escolha da COPPA, da GDPR e da LGPD como foco da etapa de avaliação da legislação foi fundamentada em critérios de relevância jurídica, abrangência territorial e influência normativa no contexto da privacidade de crianças em ambientes digitais.

A COPPA (Children's Online Privacy Protection Act) foi selecionada por ser uma das primeiras legislações específicas voltadas à proteção da privacidade online de crianças. Criada nos Estados Unidos em 1998, ela estabelece diretrizes claras sobre o consentimento parental e a coleta de dados de menores de 13 anos, influenciando diretamente políticas de plataformas como YouTube, TikTok e Facebook.

A GDPR (General Data Protection Regulation) foi escolhida por representar o marco regulatório da União Europeia em proteção de dados pessoais, sendo reconhecida internacionalmente pela sua abordagem robusta e rigorosa. A GDPR inclui dispositivos específicos sobre o tratamento de dados de menores, sendo amplamente adotada como referência para legislações ao redor do mundo.

Por fim, a LGPD (Lei Geral de Proteção de Dados Pessoais) foi incluída por ser a legislação brasileira vigente sobre proteção de dados. Além de estabelecer princípios semelhantes aos da GDPR, ela traz dispositivos específicos sobre o tratamento de dados de crianças e adolescentes, considerando a realidade brasileira e a importância da análise no contexto nacional.

A seguir serão exploradas leis relacionadas à Privacidade, pertinentes ao trabalho, que são a GDPR, LGPD, COPPA.

2.2.1. GDPR

O Regulamento Geral de Proteção de dados (GDPR) é uma legislação da União Europeia, que entrou em vigor no ano de 2018, com a finalidade de estabelecer regras aos processamentos de dados pessoais (BRASIL, 2018). De maneira geral, o GDPR busca proporcionar aos indivíduos mais controles sobre os seus dados pessoais, de forma mais responsável e transparente. O GDPR irá estabelecer um padrão, que influenciou a abordagem de muitos países.

No que se refere ao tratamento de dados o GDPR irá trazer no seu Considerando 38 a necessidade de disposições regulamentares específicas para as crianças.

38. As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança.

O GDPR trará no seu artigo 8º as condições que são aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação. Alguns pontos importantes relacionado ao tratamento de dados:

1. Idade mínima para o consentimento

O GDPR irá estabelecer a idade mínima de 16 anos para o consentimento, ou seja, o processamento de dados em menores que 16 anos requer o consentimento dos pais ou de um responsável. Lembrando que, os Estados-Membros poderão dispor no seu direito uma idade inferior, desde que essa idade não seja superior a 13 anos.

2. Consentimento Parental

O processamento de dados só será legal apenas se o consentimento parental for obtido pelos pais ou responsáveis. O responsável pelo tratamento deverá realizar todos os esforços adequados para verificar que o consentimento foi dado, considerando a tecnologia disponível.

3. Informações Claras para as crianças

Os controladores dos dados são obrigados a fornecer informações claras e acessíveis para crianças, sobre como seus dados serão processados.

O GDPR não irá trazer uma seção específica acerca da proteção de dados de crianças, ele irá abordar de forma abrangente, incluindo as disposições que são mais relevantes, como idade mínima, consentimento parental. Vale ressaltar, que alguns estados da União Europeia poderão ter leis específicas de privacidade dados.

2.2.2. LGPD

A Lei Geral de Proteção de dados é uma legislação brasileira -Lei n. 13.709, de 14 de agosto de 2018. Ela busca garantir a privacidade de dados dos cidadãos, estabelecendo regras para coletar, armazenar, processar e compartilhar as informações pessoais. A legislação irá trazer disposições específicas para proteger a privacidade das crianças.

No que se refere ao tratamento de dados de crianças e adolescentes a LGPD trouxe somente o seu artigo 14, que determinará que o tratamento de dados deverá ser realizado com o “melhor interesse do menor”. O melhor interesse, trata-se de um princípio que integra o sistema protetivo das crianças e adolescentes no ordenamento jurídico, consistindo em atender prioritariamente aos interesses deles levando em consideração a vulnerabilidade e a necessidade de cuidado, por parte da família, sociedade e Estado. (FGV,2020)

Ressalva-se, acerca de uma discussão que anteriormente ocorria sobre a possibilidade de os tratamentos de dados ocorrerem somente com base no consentimento dos pais ou de um responsável, que o determinado pelo §1º do artigo 14º da LGPD. Essa discussão foi superada após o enunciado publicado pela ANPD, no dia 24 de maio, CD/ANPS N° 1 de 22 de maio de 2023, que reconheceu a possibilidade de que os tratamentos de dados pessoais de crianças e adolescentes sejam realizados em quaisquer hipóteses legais previstas na LGPD, desde que o interesse da criança seja respeitado.

O artigo 14º da LGPD veio para reforçar a importância de medidas especiais, que visam garantir a privacidade e segurança de dados das crianças, ratificando a vulnerabilidade desse grupo. Entretanto, ao reconhecer que não é mais necessário o consentimento dos pais e dos responsáveis para o tratamento de dados é um retrocesso, já que essa medida é para facilitar os controladores de dados.

A seção III da LGPD, trará todos os requisitos que devem ser cumpridos a respeito do tratamento de dados pessoais das crianças. O parágrafo 6º do artigo 14º, determinará que as informações sobre o tratamento de dados pessoais de crianças e adolescentes deverá ser fornecida de maneira simples, clara e acessível, considerando as do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança. (Art. 14, § 6º, LGPD) Sendo assim, deverá ser evitada linguagem complexa e a utilização de termos técnicos para quem não é da área. É válida e recomendável a utilização de desenhos, esquemas e fluxogramas, vídeos e outros recursos com a finalidade de tornar o conteúdo mais acessível para a criança e o responsável.

2.2.3. COPPA

A COPPA, Children's Online Privacy Protection (Lei de Proteção à Privacidade Online de Crianças), é uma legislação dos Estados Unidos, gerenciada pela Comissão Federal de Comércio, criada com a finalidade de proteger a privacidade online de crianças menores de 13 anos (UNITED STATES, 1998). Ela foi promulgada em 1998, como resposta às crescentes preocupações sobre a coleta de informações pessoais de crianças em plataformas online.

A Lei irá se aplicar a sites e serviços online direcionados às crianças, estipulando que tanto os sites quanto os serviços deverão exigir o consentimento dos pais para coletar e utilizar qualquer informação pessoal pertencente as crianças. As sessões da Lei são divididas em: Definições, Requisitos Gerais para proteção da privacidade das crianças, proibições, administração e aplicação, sanções civis, regulamentação e procedimentos e estudos e relatórios.

O capítulo definições irá estabelecer as definições chaves que são utilizadas na legislação. Na sessão de requisitos irá ter a disposições centrais da COPPA, estabelecendo as regras fundamentais que os operadores dos sites devem seguir. Entre

algumas delas, a Lei irá exigir que os sites notifiquem os pais e obtenham o consentimento verificável dos pais antes de coletar, usar e divulgar informações de crianças menores de 13 anos. A Lei também irá exigir que os sites mantenham seguras as informações que coletam das crianças, bem como o direito de revisar as informações pessoais fornecidas por uma criança.

Outros capítulos, irão tratar as proibições de algumas práticas, como a coleta de informações que não sejam estritamente necessárias para participar de uma atividade online. O capítulo de administração e aplicação que irá detalhar o papel da Comissão Federal de Comércio na administração e aplicação da COPPA. Consequentemente, a Comissão Federal de Comércio poderá criar regras específicas para implementar a Lei. Já no capítulo de sanções civis irá especificar as penalidades que podem ser aplicadas em caso de violação da lei. O capítulo de Regulamentação e Procedimentos irá abordar questões relacionada à criação de regras pela FTC, procedimentos para impor a COPPA. Por último, a seção de estudos e relatórios irá conduzir estudos e apresentar relatórios que demonstrem a eficácia da COPPA.

2.3. Desafios de Privacidade para Crianças

À medida que a adoção de tecnologias online e dispositivos móveis por parte de menores de idade apresenta um crescimento nos últimos anos, torna-se inevitável os desafios relacionados a privacidade. Isso porque, seus dados pessoais vêm sendo coletados e tratados nos mais diferentes contextos, expondo esse grupo etário a consideráveis riscos no que tange a sua privacidade.

As crianças são consideradas um grupo vulnerável, isso porque elas estão em constante desenvolvimento físico e mental, o que torna essencial a orientação e a assistência de adultos para garantir a segurança e a privacidade. Além disso, essa vulnerabilidade é reforçada pela fragilidade inerente, tanto física quanto psicológica, associada à sua capacidade limitada de tomar decisões de forma autônoma. (LIVINGSTONE; STOILOVA; NANDAGIRI, 2019)

Por meio da internet, elas podem realizar inúmeras atividades, como estudar, interagir com familiares e desconhecidos, assistir vídeos, realizar compras e entre outros. É indubitável o papel da internet para promover entretenimento, educação, e outras oportunidades. Entretanto, as crianças e os adolescentes ficam mais expostos a riscos digitais.

A coleta e o uso de dados pessoais de menores em redes sociais geram preocupações, pois podem violar o direito fundamental à privacidade e representar riscos para as crianças. Esses dados se tornaram um dos principais ativos econômicos das empresas, permitindo que elas conheçam detalhes íntimos sobre os usuários. No entanto, muitos adultos não sabem como esses dados são tratados, nem os riscos e prejuízos que isso pode causar, o que reflete diretamente nas práticas e orientações oferecidas às crianças. A falta de conscientização dos pais sobre a privacidade digital compromete a proteção dos dados dos filhos e aumenta a necessidade de uma maior conscientização e regulamentação.

O objetivo de avaliar o nível de conscientização dos pais em relação à privacidade digital é identificar lacunas no entendimento e nas práticas de proteção de dados. A pesquisa sobre esse tema visa destacar a importância de políticas públicas e regulamentações mais claras, que orientem não apenas as redes sociais, mas também forneçam aos pais as ferramentas e informações necessárias para proteger seus filhos online.

Essa utilização dos dados pessoais das crianças e dos adolescentes é preocupante, já que permite conhecer preferências, perfil de consumo, estado de saúde e tantas outras informações prejudiciais para eles, isso pois os dados podem ser utilizados para prejudicar, influenciar e manipular os seus comportamentos e condutas.

A coleta de dados pessoais de crianças e adolescentes, sem o devido cuidado e monitoramento, pode resultar em abusos, como a manipulação de comportamentos e a exposição a conteúdos impróprios. Além disso, observa-se que os legisladores não levam em consideração adequadamente os riscos para as crianças associados ao perfil, isso porque os legisladores não estão totalmente cientes dos riscos específicos para as crianças, conseqüentemente a legislação poderá não está atualizada para abordar adequadamente as preocupações emergentes.

As leis de proteção geral de dados concentram-se mais em salvaguardar os direitos gerais, desconsiderando as implicações específicas para as crianças, por exemplo muita

das vezes os requisitos de consentimentos, as políticas de privacidade e as medidas de segurança não são adaptadas para o público infantil.

Outro obstáculo significativo reside na aplicação consistente das leis em âmbito internacional. Diferenças nas interpretações e implementações das regulamentações de proteção de dados entre países podem criar lacunas e inconsistências, especialmente em um mundo onde as fronteiras digitais muitas vezes se sobrepõem às fronteiras geográficas tradicionais. A harmonização global nessas questões é fundamental para garantir uma proteção de dados eficaz e uniforme.

O nível de conscientização dos pais no entendimento da proteção de dados e privacidade online é crucial para a segurança das crianças no ambiente digital. Muitos pais enfrentam dificuldades em compreender as complexidades associadas à coleta e uso de dados pessoais, frequentemente devido à falta de familiaridade com as tecnologias envolvidas. Isso compromete a capacidade dos pais de orientar seus filhos sobre práticas seguras na internet, como a importância de proteger informações pessoais e identificar sinais de possíveis ameaças. (LIVINGSTONE; STOILOVA; NANDAGIRI, 2019)

Outro aspecto relevante é que muitos pais, apesar de reconhecerem a importância da privacidade, não sabem como aplicar de maneira prática os princípios de proteção de dados em suas rotinas digitais. A falta de ferramentas intuitivas e diretrizes claras pode dificultar a implementação de práticas seguras, como a configuração de controles de privacidade em aplicativos e redes sociais.

2.4. Privacidade de Crianças

Muitas crianças estão crescendo em um mundo “digital-por-padrão”, nas quais as tecnologias intermediam interações interpessoais, institucionais e comerciais. Essas interações online permitem que as crianças se conectem, comuniquem, interajam e joguem de maneira confortável (Priya et al., 2023). A privacidade estimula a autonomia das crianças, apoiando seu desenvolvimento psicossocial, responsabilidade, resiliência, confiança e habilidades de pensamento crítico (Nolan et al., 2011). As sociedades ao redor do mundo estão dando cada vez mais importância em relação a privacidade e segurança das crianças, pois as violações de privacidade no mundo digital podem ocorrer de diferentes maneiras. As tecnologias podem monitorar a localização física das crianças, armazenar suas informações pessoais e preferências e até influenciar suas tomadas de decisões (Carly et al., 2018).

Daniel Solove (2010) desenvolveu uma taxonomia de problemas de privacidade, contendo 16 problemas de privacidade organizado em quatro categorias: coleta de informações, processamento de informações, divulgação de informações e invasões. A coleta de informações envolve a vigilância e monitoramento, obtendo informações das crianças de maneira problemática. O processamento de informações está relacionado ao armazenamento, manipulação e utilização das informações, incluindo a agregação de informações com finalidades diferentes das acordadas previamente. A divulgação de informações tem relação com a violação de confidencialidade, divulgando as informações de maneira inadequada, podendo prejudicar a reputação de uma pessoa. Por fim, a invasão ocorre quando alguém invade o espaço físico, psicológico ou digital de outra pessoa ou quando interfere a tomada de decisão de outra pessoa.

O trabalho de Eva e Anders (2019) investigou a percepção das crianças em relação a privacidade. O estudo envolveu 25 crianças entre 10 e 11 anos, que passaram por um workshop com testes para avaliar: (1) o que as crianças fazem de maneira online; (2) qual o entendimento das crianças em relação as informações pessoais; (3) quais informações pessoais são solicitadas pelos aplicativos e jogos; (4) quais comportamentos online são considerados aceitáveis; (5) quais os riscos e preocupações elas tem no meio online. De maneira geral, esses testes demonstraram que o entendimento de privacidade que as crianças têm resume em não deixar uma pessoa estranha chegar perto delas, inclusive elas consideram o endereço da sua residência como a informação mais confidencial que elas possuem. Ou seja, é evidente que precisa

ser realizado um trabalho de conscientização com as crianças em relação a privacidade. Nesse sentido, várias organizações desenvolveram materiais de como dialogar com as crianças em relação a privacidade (Comissão Federal, 2014), inclusive incluindo em materiais escolares para serem ensinados nas Escolas (Google, 2017).

Em relação ao desenvolvimento desses materiais educativos, não há um consenso em relação a participação ou não das crianças na confecção desses materiais, mas é nítido que abordagens baseadas em jogos ou histórias são mais eficazes (Priya et al., 2018). Por exemplo, Rayers (2014) desenvolveu um jogo chamado “Os Vigilantes” que ajudou as crianças a aprenderem sobre a coleta de informações e suas utilizações, já o livro de historinha “Super-heróis” conta a história de um super-herói que ensina lições sobre informações pessoais, conversas online, compartilhamento de localização e cyberbullying.

Além da conscientização das crianças, é importante que as aplicações, jogos, sites e redes sociais estejam em conformidade com as leis (COPPA, GDPR, LGPD etc.), porém o cenário atual indica que muitos não cumprem as disposições legais. De acordo com a Comissão Federal de Comércio (Federal Trade Commission, FTC) Americana, a transparência em relação à privacidade dos aplicativos de celulares é decepcionante, apresentando pouca ou nenhuma informação de privacidade para os pais. A FTC realizou um estudo que demonstrou que os pais geralmente não conseguem determinar, antes de baixar um aplicativo, se o aplicativo apresenta riscos relacionados à coleta, uso e compartilhamento das informações pessoais de seus filhos. Os pais deveriam ser capazes de saber, antes de baixar um aplicativo para seus filhos, quais dados serão coletados, como os dados serão usados e quem terá acesso aos dados. Com essas informações, os pais podem tomar decisões informadas sobre os aplicativos que escolhem para seus filhos e adotar essas tecnologias com mais confiança.

Existem inúmeros casos de grandes empresas que violaram a privacidade das crianças, por exemplo, em 2019, o YouTube foi multado em 170 milhões de dólares por coletar informações para repassar a empresas de publicidades, violando uma regra da COPPA, que determina que os serviços devem solicitar o consentimento dos pais para crianças menores de 13 anos (Lisa, 2019). Liu et al. (2016) identificou que 68 mil aplicativos para crianças, dentro de um conjunto de 1 milhão de aplicativos Android, possuem potencial violação a COPPA, o autor avaliou o *metadata* dos aplicativos, sem executá-los, não conseguindo avaliar comportamentos em tempo real ou vazamento de dados. Irwin et al. (2017) desenvolveu um método de execução dinâmica de aplicativos

Android para crianças, que analisa o tráfego de rede em tempo real com o objetivo de identificar potenciais violações de privacidade da COPPA. Nesse sentido, o método teve quatro etapas: (i) identificar aplicativos de crianças que acessam informações sensíveis, (ii) identificar quaisquer terceiros com quem compartilham essas informações, (iii) verificar se os aplicativos solicitam o consentimento dos pais durante a execução e (iv) auxiliar advogados na avaliação do quanto essas políticas de privacidade são adequadas. Como resultado, o trabalho apresentou que diversos aplicativos famosos, com mais de 100 milhões de instalações potencialmente violam regras da COPPA.

O Trabalho de Ilaria et al. (2014) demonstra que apesar de aplicativos de celulares serem para um público infantil, vários aplicativos solicitam permissões sensíveis que não são apropriadas e/ou esperadas. Esse é um ponto crítico para entender potenciais violações de conformidade legal, pois não é fácil ter clareza de quais informações são coletadas e/ou utilizadas. Além disso, mesmo que um aplicativo esteja inativo, não há garantia que o aplicativo não está coletando informações pessoais. Empresas desenvolvedoras disponibilizam aplicativos gratuitos ou pagos nas lojas, sendo que os gratuitos obtêm receita por meio de publicidades, enquanto a versão paga não possui. Muitas vezes é mais lucrativo para a empresa desenvolvedora ter um aplicativo gratuito com propaganda, do que um pago devido a publicidade direcionada utilizando os dados coletados (Manoogian, 2012).

2.5. 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 (Burn, 1994, King e Teo, 1997). Neste trabalho, será utilizado o *Security Awareness Maturity Model* (SANS), de forma análoga, para se estabelecer os níveis de conscientização 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. O Modelo de maturidade SANS, serão divididos em 5 níveis de programas de conscientização sobre segurança, conforme descrito abaixo

- Inexistente (Non-Existent):

Neste estágio, não há programa formal de conscientização em segurança. Os indivíduos desconhecem os riscos digitais, não recebem orientação específica e não seguem diretrizes de segurança. A exposição a ameaças é elevada devido à ausência total de iniciativas educativas ou políticas de proteção.

- Focado em Conformidade (Compliance-Focused):

O programa é estruturado principalmente para atender requisitos legais ou normativos, como auditorias ou regulamentações. O foco está na entrega de informações básicas, muitas vezes de forma genérica. Embora existam ações pontuais, elas não promovem compreensão ou mudança real de comportamento.

- Conscientização e Mudança de Comportamento (Promoting Awareness & Behavioral Change):

Neste nível, o programa busca não apenas informar, mas transformar o comportamento dos usuários. As ações são direcionadas para que as pessoas compreendam sua responsabilidade na proteção da informação e passem a adotar práticas seguras de forma voluntária e consistente.

- Sustentação de Longo Prazo e Mudança Cultural (Long-Term Sustainment & Culture Change):

A segurança se torna parte da cultura organizacional. Os treinamentos são regulares, atualizados e personalizados. A conscientização é integrada ao dia a dia, e os valores de segurança são mantidos mesmo diante de mudanças de equipe ou tecnologias.

- Estágio Adaptativo (Adaptive Stage):

No nível mais avançado, o programa é dinâmico, estratégico e baseado em métricas. A organização consegue se antecipar a novas ameaças, adaptar suas abordagens e promover continuamente melhorias com base em dados e tendências. A segurança passa a ser uma prioridade coletiva e estratégica.

Ao aplicar este modelo de forma adaptada ao contexto familiar, este estudo visa identificar o nível de proteção de privacidade às crianças, com base na conscientização digital dos pais e compreender as práticas e desafios enfrentados na proteção da

privacidade infantil nas redes sociais. Essa abordagem permitirá não apenas diagnosticar lacunas, mas também orientar a criação de campanhas educativas, políticas públicas e ferramentas que incentivem uma cultura de segurança digital desde os primeiros anos de vida.

Capítulo 3

Trabalhos Relacionados

Este capítulo apresenta os trabalhos relacionados, dando ênfase na avaliação de privacidade em redes sociais na Seção 3.1. Já na Seção 3.2 é abordada a avaliação de privacidade de crianças. Na Seção 3.3 é apresentada a questão de avaliação de privacidade de crianças em redes sociais. Por fim, a Seção 3.4 apresenta uma discussão e comparação acerca dos trabalhos ao projeto proposto e quais problemas ele procura resolver que ainda são existentes na literatura.

3.1. Privacidade em Redes Sociais

As redes sociais estão presentes na vida cotidiana de milhões de pessoas em todo o mundo, proporcionando uma plataforma para se conectar, compartilhar informações e interagir. Tem-se que as redes sociais não são utilizadas somente para entretenimento, por exemplo empresas analisam tendências em redes sociais para comercializar produtos e serviços personalizados, empregadores consultam as redes sociais para verificar o perfil dos candidatos, o poder judiciário consulta as redes sociais para obter evidências para solucionar crimes e inclusive as redes sociais influenciaram resultados de eleições (Kayes e Iamnitich, 2017). Ou seja, é possível observar que as redes sociais possuem informações atualizadas de diferentes dimensões, por exemplo o Facebook possui informações sobre a vida pessoal, já o LinkedIn sobre as atividades profissionais, permitindo que seja possível agregar essas informações e ter um perfil completo de um indivíduo (Nissenbaum, 2011). No entanto, esse ambiente digital também levanta várias preocupações significativas em relação à privacidade. O principal desafio nas soluções de privacidade está na busca pelo equilíbrio entre preservar a privacidade do usuário e, ao mesmo tempo, não limitar o aproveitamento dos benefícios de socializar e compartilhar informações.

Um dos principais problemas da privacidade está relacionado ao vazamento de informações, sendo proveniente dos próprios usuários que se colocam em risco

interagindo ou divulgando suas informações pessoais, mas também podem ocorrer vazamentos por meio das aplicações terceiras / externas vinculadas as contas de redes sociais ou até mesmo pelas vulnerabilidades em serviços providos pela própria rede social. Essas exposições de informações são interessantes para diversos públicos, como: (a) Corretores de Dados (*data brokers*): vendem informações pessoais para outras partes, como bancos, seguradoras etc.; (b) Provedores de serviços: oferecerem serviços e anúncios direcionados; (c) Criminosos: realizam engenharia social, *spear phishing* ou recuperação de técnicas de autenticação;

Em relação às funcionalidades nativas de privacidade as redes sociais, normalmente, possuem a opção de um usuário limitar o acesso de suas informações, deixando-os visíveis apenas para os amigos, por exemplo. Inclusive, um usuário pode criar uma conta sem explicitamente revelar nenhuma informação. Isso provê autonomia ao usuário em deixar suas informações públicas e/ou privadas. Porém, existem ataques relacionados a privacidade que tem o objetivo de inferir atributos do usuário que estão incompletos ou ausentes (Neil e Bing, 2016). Existem diversos trabalhos na literatura que exploram a inferência de atributos em redes sociais, esses trabalhos podem ser classificados em duas principais categorias: inferência baseada em amigos e inferência baseada em comportamento (Ghazaleh e Huan, 2020).

As técnicas de inferência baseada em amigos usam a teoria de homofilia, que parte do princípio de que dois amigos são mais prováveis de compartilhar os mesmos atributos do que dois estranhos. Nesse contexto, caso a maioria dos amigos de um indivíduo em uma rede social esteja matriculada na PUCPR, é plausível inferir que esse próprio indivíduo também seja estudante da PUCPR. Assim, diversos trabalhos utilizaram técnicas de aprendizagem de máquina para comprovar essa teoria (Jianming et al., 2006, Jack et al., 2009, Kurt et al., 2010). Por outro lado, a técnica de inferência baseada em comportamento utiliza atributos públicos do usuário e de amigos similares a ele, Weinsberg et al. (2012) propôs um método de identificar atributos do usuário, inclusive o gênero, baseado na lista de filmes curtidas.

Nesse sentido, é essencial que existam configurações de privacidade de granularidade fina para que o usuário possa ter flexibilidade em relação à exposição de suas informações. Entretanto, essa granularidade fina pode exigir um esforço cognitivo grande por parte do usuário, no qual a tendência é que ele ignore e confie apenas nas configurações padrões de privacidade. Dessa forma, diversos autores propuseram técnicas de controles finos de privacidade. Kruk (2004) propôs um mecanismo de

controle de acesso baseado em ontologia que utiliza as relações entre usuários. A proposta utiliza uma definição genérica de relacionamentos ("conhece") como uma métrica de confiança e gera regras que controlam o acesso de um amigo a recursos com base no grau de interação na rede social. Choi et al. (2006) evoluiu o trabalho de Kruk (2004) com uma abordagem mais refinada, que considera relacionamentos mais granulares (por exemplo, "trabalhaCom", "éAmigoDe", "conhece") para modelar a rede social e o controle de acesso.

Fong (2011) propõe um modelo ReBAC (*Role and Relationship-Based Access Control*) que considera que as relações são polirrelacionais (por exemplo, relacionamentos professor-aluno são distintos de relacionamentos pais-filhos) e direcionados (por exemplo, relacionamentos professor-aluno são distintos de relacionamentos aluno-professor) que mapeiam múltiplos contextos de acesso organizados em uma hierarquia em forma de árvore. Quando o acesso é solicitado em um contexto, os relacionamentos de todos os contextos ancestrais são combinados com os relacionamentos no contexto de acesso alvo para construir uma rede na qual as decisões de autorização são tomadas.

Os estudos têm mostrado que usuários em redes sociais frequentemente não utilizam os controles de privacidade disponíveis. Por exemplo, mais de 99% dos usuários do Twitter mantêm a configuração padrão de privacidade, na qual seu nome, lista de seguidores, localização, site e informações biográficas são visíveis. Da mesma forma, a maioria dos usuários do Facebook mantém as configurações padrão (Kayes e Iamnitchi, 2017). A subutilização das opções de privacidade ocorre principalmente devido a uma interface não intuitiva de configuração de privacidade, configurações de privacidade complicadas e confiança inerente nas redes sociais.

No sentido de aumentar o engajamento do usuário em realizar as configurações de privacidade, é importante que exista uma interface gráfica apropriada, para facilitar o entendimento e reduzir o tempo de configuração. Assim, diversos trabalhos foram desenvolvidos com o intuito de desenvolver uma interface apropriada para configurar a privacidade. Por exemplo, o trabalho de Paul (2012) propôs C4PS (*Colors for Privacy Settings*), no qual aplica cores para diferentes visibilidades de atributos, por exemplo: (vermelho): visível para ninguém; (azul): visível para amigos selecionados; (amarelo): visível para todos os amigos; (cinza): visível para qualquer pessoa. Dessa maneira, os usuários podem selecionar a cor de cada atributo.

O problema em não alterar as configurações padrão é que elas quase sempre tendem a ser mais abertas do que os usuários prefeririam (Kayes e Iamnitich, 2017). Para superar essa situação, foram propostas abordagens para gerar automaticamente configurações padrão de privacidade mais apropriadas. O trabalho de PriMA (2016) propôs um gerador de preferências de privacidade baseado em usuários com perfis similares ao proprietário da conta. Já a proposta de PolicyMgr (Shehab et al., 2010), usou aprendizagem de máquina supervisionada com exemplos de políticas de privacidade para construir classificadores que automaticamente geram as políticas de privacidade.

Os desafios de privacidade se intensificam com a integração das redes sociais na vida cotidiana. Embora as redes sociais ofereçam inúmeras vantagens, como conexões pessoais e profissionais, também apresentam riscos significativos devido à grande coleta de dados pessoais. Nesse cenário, é fundamental que os usuários estejam conscientes sobre quais informações estão sendo compartilhadas. Soluções como a criação de configurações de privacidade de granularidade fina e a utilização de ferramentas intuitivas para simplificar essas configurações são passos importantes para garantir a segurança dos dados.

Além disso, a responsabilidade pela proteção da privacidade deve ser compartilhada entre usuários, plataformas e legisladores. Inovações como o modelo ReBAC e técnicas de aprendizagem de máquina para personalizar configurações de privacidade são avanços significativos. No entanto, é crucial que a legislação acompanhe os avanços tecnológicos para abordar os riscos emergentes de maneira adequada. Somente através de uma abordagem integrada e atualizada poderemos criar um ambiente digital que respeite a privacidade dos usuários e permita que eles aproveitem plenamente os benefícios das redes sociais.

3.2. Privacidade de Crianças em Redes Sociais

A privacidade das crianças em redes sociais é um assunto controverso, uma vez que muitas redes sociais, como o Facebook, determinam em seus termos de serviços que proíbem o uso por crianças. Entretanto, Yet et al. (2011) reportou que milhões de crianças menores de 13 anos utilizam o Facebook e mentiram a respeito de sua idade no momento de registro. É evidente que as redes sociais muitas vezes não são projetadas considerando os melhores interesses das crianças. Por exemplo, Instagram e o Twitter

mantêm os perfis de novas contas como públicos por padrão. Além disso, as crianças não compreendem que consentir em acessar uma rede social significa consentir na divulgação de suas informações pessoais, como localização e horários de acesso sendo coletadas e compartilhadas.

Os sistemas de verificação de identidade presentes na maioria das redes sociais e demais serviços online apresentam problemas em sua eficácia, uma vez que dependem de verificação remota que podem ser facilmente contornados. Muitos pais consideram, erroneamente, a restrição de idade em redes sociais importante para filtrar conteúdos inapropriados para seus filhos, e não se atentam aos riscos de privacidade. A COPPA considera a idade de 13 anos como um ponto de referência na vida de uma criança, principalmente em relação a tomada de decisões. Vários estudos concluem que, antes dos 11 anos, os jovens são em grande parte pouco críticos ao determinar a confiabilidade do conteúdo online (Bennett et al, 2008). Por exemplo, em um estudo com 135 crianças de 8 a 10 anos, foi identificado que a presença de recursos dinâmicos (animações) em um site era considerada um reflexo da confiabilidade, pois as crianças classificaram um site com imagens animadas de cachorros como mais confiável do que um site com o mesmo texto, mas sem imagens (Yet et al., 2011). Harris et al. (2011) relatou que crianças a partir de 8 anos conseguem identificar a intenção de venda em publicidades que aparecem em anúncios. No entanto, nessa idade, as crianças não conseguem perceber intenções persuasivas nas publicidades. Em uma pesquisa com 300 crianças, Turow e Nir (2000) apresentaram um cenário que um presente / prêmio seria oferecido as crianças que compartilhassem seus dados pessoais, 70% delas aceitaram a compartilhar detalhes relacionados a seus perfis (nome, idade, gênero, hobbies e lojas favoritas), em comparação com uma média de 22% dispostos a compartilhar seus dados de contato (endereço residencial, número de telefone residencial). Isso corrobora com o estudo de Eva e Anders (2019), no qual indicava que o receio das crianças ser apenas relacionado a sua localização física.

O trabalho de Alkhalifah e Alghafis (2022) realizou um estudo empírico sobre a privacidade das crianças sob a perspectiva dos pais, nesse estudo foi aplicado um formulário para 500 pais e mães com perguntas sobre o perfil das crianças e sobre o comportamento das crianças na Internet. A escala Likert foi usada para classificar as respostas em uma escala de 1 a 5 da seguinte forma: 1. 'Discordo totalmente;' 2. 'Discordo;' 3. 'Não concordo nem discordo;' 4. 'Concordo;' e 5. 'Concordo totalmente'. As perguntas foram relacionadas a 7 categorias, por exemplo:

- 1) **Comportamento da criança na Internet:** “Minha criança pode usar a Internet quando quiser”
- 2) **Privacidade:** “Estou ciente que pessoas não autorizadas podem estar acessando informações pessoais dos meus filhos”
- 3) **Vazamento de Informações:** “Eu não me importo com a identidade online da minha criança”
- 4) **Riscos de Privacidade:** “Informações pessoais da minha criança podem estar sendo utilizadas de maneira inapropriada”
- 5) **Controle Parental:** “Eu tenho total controle e responsabilidade do acesso da minha criança na Internet”
- 6) **Aspectos subjetivos:** “Minha criança consome conteúdos na Internet influenciado por seus amigos”
- 7) **Conteúdo:** “Estou utilizando mecanismos para filtrar de maneira apropriada o que minha criança pode assistir”

Esses foram alguns exemplos de perguntas realizadas no questionário, note que são perguntas provocativas. O estudo utilizou Modelagem por Equações Estruturais (*Structural Equation Modeling*, SEM) que é um método estatístico para testar e estimar relações causais, que permitiu encontrar correlações entre as categorias baseado em hipóteses. Por exemplo, comprovou a teoria que Pais que tem maior preocupação em relação ao vazamento de informações de seu filho, aplicam mecanismos de controles parentais (Alkhalifah e Alghafis, 2022). O público-alvo que participou desse estudo foi majoritariamente feminino (88%), e não aplicou nenhuma pergunta relacionado a aspectos legais de privacidade.

O trabalho de Rochelau e Sonia (2019) analisou a privacidade de adolescentes autistas em redes sociais, na qual há uma hipótese que autistas são mais vulneráveis a ameaças de privacidade em redes sociais. Os resultados do trabalho demonstraram o contrário, que crianças autistas são mais precavidas em relação ao uso de redes sociais. Além disso, o trabalho de Rochelau e Sonia (2019) identificou que existem fatores que afetam o comportamento e atitudes das crianças e adolescentes em redes sociais:

- 1) **Idade:** Pesquisas mostram que as preocupações com a privacidade e os comportamentos de proteção dos adolescentes diminuem de acordo com a idade [Bryce e James, 2014, Dhir et al., 2016]. As crianças ou adolescentes mais jovens geralmente obedecem às diretrizes de privacidade e segurança de seus pais, enquanto os adolescentes mais velhos seguem sua própria intuição sobre o que fazer nas redes sociais [Gool et al. 2015, Walrave e Heirman, 2013]. Como consequência, os adolescentes mais velhos têm mais probabilidade de sofrer violações de privacidade em redes sociais do que os usuários mais jovens.
- 2) **Gênero:** Estudos indicam que adolescentes do sexo feminino tem maiores preocupações em relação à privacidade do que os meninos (Chai et al., 2009), principalmente por existir uma prevalência de assédios sexuais nas adolescentes.
- 3) **Personalidade:** Adolescentes que são altamente extrovertidos e abertos a novas experiências tendem a usar redes sociais mais ativamente, e consequentemente estão mais sujeitos aos problemas de privacidade (Blackwell et al., 2017). Além disso, a saúde mental dos jovens pode influenciar, Radovic et al. (2017) examinou o uso positivo e negativo de redes sociais por adolescentes clinicamente deprimidos. Eles descobriram que adolescentes deprimidos tendem a compartilhar em excesso detalhes pessoais e publicar conteúdo arrependido em redes sociais quando estão estressados para lidar com suas emoções e receber apoio social.
- 4) **Frequência de uso:** Vários estudos demonstram a associação entre a frequência de uso de redes sociais e a susceptibilidade a violações de privacidade (Leung e Lee, 2012) ou seja, adolescentes que usam frequentemente redes sociais para se comunicar com outras pessoas são mais vulneráveis do que usuários menos ativos (Leung, 2014).
- 5) **Experiência com violação de privacidade:** Christofides et al. (2012) identificaram que adolescentes que tiveram uma experiência negativa no Facebook foram motivados a aprender e usar configurações de privacidade para proteger suas informações pessoais.
- 6) **Mediação dos Pais:** A mediação dos pais no uso de redes sociais é fundamental para mitigar os riscos de privacidade, normalmente os pais adotam duas abordagens: (i) Ações educadoras: Pais discutem os riscos e benefícios do uso

das redes sociais, ensinando-os como se proteger das ameaças; (ii) Ações restritivas: Pais utilizam ferramentas restritivas para limitar o uso da Internet pelas crianças. A ação educadora é mais eficaz do que as ações restritivas (Liu et al., 2013). Na verdade, ações altamente restritivas podem incentivar os adolescentes a se envolverem de forma rebelde em comportamentos arriscados em redes sociais (Shin e Ismail, 2014).

- 7) **Incentivo dos professores nas escolas:** Lofgren-Martenson et al. (2015) descobriram que os professores estavam mais cientes das atividades sociais e sexuais online de seus alunos do que os pais dos alunos. Em muitos casos, os professores eram responsáveis por ajudar os alunos a distinguir entre a divulgação segura ou perigosa de informações pessoais durante as aulas.
- 8) **Influência dos amigos:** A pesquisa mostra que os adolescentes têm mais probabilidade de se envolver em comportamentos online perigosos quando buscam conselhos de seus colegas sobre questões de privacidade, em vez de consultar seus pais ou professores (Shin e Ismail, 2014). No entanto, os colegas também podem ter uma influência positiva na privacidade e segurança dos adolescentes em redes sociais, como evidenciado no trabalho de Gool et al. (2015).

Os estudos sobre a conscientização dos pais quanto à privacidade infantil e a conformidade com legislações de proteção de dados têm abordado diversas perspectivas, evidenciando também algumas limitações importantes. O estudo de Porfirio e Almeida (2021) investiga como os pais no Brasil compreendem a LGPD e as implicações dessa legislação para o compartilhamento de dados de seus filhos nas redes sociais. O objetivo dos autores é avaliar o nível de conhecimento dos pais e como aplicam as diretrizes de privacidade ao expor informações das crianças. Embora a pesquisa indique uma conscientização inicial, muitos pais ainda desconhecem aspectos críticos da LGPD. Uma limitação significativa desse trabalho é seu enfoque restrito a uma amostra regional, o que dificulta a generalização dos resultados para outras áreas do Brasil. Além disso, o estudo se baseia em questionários autorrelatados, que podem não refletir fielmente o entendimento dos pais.

Complementando essa análise, Mendes, Silva e Rocha (2022) examinam a responsabilidade dos pais brasileiros na proteção de dados das crianças conforme a

LGPD. A pesquisa investiga as percepções dos pais sobre suas obrigações ao expor os filhos em plataformas online e aponta para a necessidade de campanhas educativas para aprimorar a compreensão da LGPD entre os pais. Entretanto, este estudo também possui limitações, principalmente pela falta de uma análise prática das ações dos pais, focando-se mais nos conhecimentos teóricos. Ademais, a ausência de uma comparação com legislações internacionais limita o entendimento das diferenças e similaridades entre a LGPD e outras regulamentações de privacidade infantil.

A perspectiva europeia é explorada por Livingstone, Stoilova e Nandagiri (2020), que examinam as experiências das crianças ao crescer em uma era digital sob a proteção da GDPR. Esse trabalho busca entender como as políticas de privacidade infantil influenciam o comportamento online das crianças e as práticas de supervisão dos pais, recomendando mais apoio e orientações às famílias. No entanto, uma limitação importante é seu foco exclusivo na União Europeia, o que restringe a aplicabilidade dos achados a regiões com regulamentações semelhantes. Além disso, o estudo se baseia amplamente em entrevistas qualitativas, o que limita a representatividade dos dados obtidos.

No contexto dos Estados Unidos, Kumar e O'Hara (2019) investigam a conformidade das plataformas online com a COPPA e o nível de conscientização dos pais sobre riscos à privacidade infantil. O estudo visa identificar as dificuldades que os pais enfrentam ao tentar monitorar a atividade online de seus filhos dentro dos requisitos da COPPA. Contudo, essa pesquisa é limitada pela dependência de dados secundários e análises de conformidade sem observação direta das práticas familiares, o que reduz a profundidade da análise. Além disso, os autores não comparam os desafios enfrentados nos EUA com aqueles em outros países que possuem regulamentações distintas.

Outro estudo focado na COPPA, de Manohar e Murthy (2021), examina como essa legislação afeta o comportamento dos pais ao permitir que seus filhos acessem plataformas online, enfatizando que, embora muitos pais tenham um conhecimento básico da COPPA, eles carecem de orientações claras para sua aplicação prática. Esse trabalho é limitado pelo enfoque exclusivo nos EUA, sem considerar a relevância de legislações semelhantes em outros contextos, como a GDPR ou a LGPD. Também se baseia em autorrelatos, sem explorar adequadamente as práticas das plataformas na aplicação de mecanismos de conformidade com a COPPA.

Por fim, Zaman e Nouwen (2020) analisam as práticas de orientação parental e proteção da privacidade infantil em diferentes contextos culturais, buscando entender as variações nas preocupações dos pais em diferentes regiões. A pesquisa propõe diretrizes adaptáveis que considerem as especificidades culturais para proteger a privacidade infantil. Contudo, o estudo enfrenta dificuldades em estabelecer diretrizes universais devido à diversidade cultural e falta de dados longitudinais, que permitiriam entender melhor a evolução das práticas de proteção ao longo do tempo.

Esses estudos contribuem para o entendimento das práticas de privacidade infantil e da conscientização dos pais em relação a diferentes regulamentações, mas cada um apresenta limitações específicas que evidenciam a necessidade de mais pesquisas comparativas e de observações práticas em diferentes contextos legislativos e culturais.

3.3. Discussão

Após os trabalhos apresentados no presente capítulo nota-se que foram relacionados a privacidade em redes sociais, privacidade de crianças, aspectos legais, avaliação de conformidade legal e novas soluções relacionadas a privacidade. A Tabela 1 lista todos os trabalhos relacionados em comparação com a proposta.

Tabela 1. Trabalhos relacionados comparados ao trabalho proposto.

Trabalho	Privacidade de crianças	Privacidade em Redes Sociais	Aspectos Legais	Avalia a Conformidade	Avalia a Conscientização dos	Propõe novas soluções
Ghazaleh e Huan (2020)	Não	Sim	Não	Sim	Não	Sim
Kruk (2004)	Não	Sim	Não	Sim	Não	Sim
Choi et al. (2006)	Não	Sim	Não	Sim	Não	Sim
Fong (2011)	Não	Sim	Não	Sim	Não	Sim
Kayes e Iamnitich (2017)	Não	Sim	Não	Sim	Não	Sim
Paul (2012)	Não	Sim	Não	Sim	Não	Sim

PriMA (2016)	Não	Sim	Não	Sim	Não	Sim
Shehab et al. (2010)	Não	Sim	Não	Sim	Não	Sim
Daniel Solove (2010)	Sim	Não	Não	Não	Não	Sim
Eva e Anders (2019)	Sim	Sim	Sim	Sim	Não	Não
Rayers (2014)	Sim	Sim	Sim	Não	Não	Sim
FTC (2012)	Sim	Sim	Sim	Sim	Não	Não
Liu et al. (2016)	Sim	Não	Sim	Sim	Não	Sim
Irwin et al. (2017)	Sim	Não	Sim	Sim	Não	Sim
Alkhalifah e Alghafis (2022)	Sim	Sim	Não	Não	Não	Sim
Rochelau e Sonia (2019)	Sim	Sim	Não	Não	Não	Sim
Porfirio e Almeida (2021)	Sim	Sim	Não	Não	Sim	Não
Mendes, Silva e Rocha (2022)	Sim	Não	Não	Não	Sim	Não
Livingstone, Stoilova e Nandagiri (2020)	Sim	Não	Não	Não	Sim	Não
Kumar e O'Hara (2019)	Sim	Sim	Não	Não	Sim	Não
Manohar e Murthy (2021)	Sim	Não	Não	Não	Sim	Não
Zaman e Nouwen (2020)	Sim	Não	Não	Não	Sim	Não

Fonte: Autoria Própria.

A análise comparativa evidencia que, embora existam diversos estudos que abordam soluções tecnológicas para melhorar as configurações de privacidade ou que tratam do comportamento infantil em ambientes digitais, há uma lacuna clara na abordagem integrada desses elementos, especialmente quando se considera a perspectiva dos pais enquanto agentes mediadores da proteção digital de seus filhos.

Observa-se que a maioria dos trabalhos abordam aspectos mais técnicos, como inferência de atributos (Ghazaleh e Huan, 2020), controle de acesso (Kruk, 2004; Choi et al., 2006) ou personalização automática de políticas de privacidade (PriMA, 2016; Shehab et al., 2010). Esses estudos oferecem contribuições relevantes para o aprimoramento das ferramentas de privacidade nas redes sociais, mas geralmente desconsideram a aplicação dessas soluções ao contexto infantil ou a percepção dos pais em relação a tais mecanismos.

Por outro lado, os estudos voltados para a privacidade infantil (como Alkhalifah e Alghafis, 2022; Rochelau e Sonia, 2019; Eva e Anders, 2019) focam mais nos comportamentos, riscos e percepções das crianças e adolescentes, ou na perspectiva dos

pais, mas ainda assim carecem de uma análise mais robusta quanto à conformidade legal e à conscientização dos pais em lidar com os direitos digitais das crianças. No entanto, esses trabalhos ainda carecem de uma análise mais aprofundada sobre a conformidade legal e sobre o nível de conscientização dos pais no enfrentamento dos desafios relacionados aos direitos digitais das crianças.

Diante disso, é possível concluir que o trabalho proposto apresenta uma contribuição relevante e necessária ao abordar de forma integrada a privacidade em redes sociais, a privacidade infantil, os aspectos legais e, sobretudo, ao incluir a avaliação da conscientização dos pais como um fator determinante para a efetividade das ações de proteção.

Capítulo 4

Metodologia

O trabalho tem como objetivo principal desenvolver um modelo de nível de conscientização parental que permita avaliar o nível de proteção à privacidade das crianças nas redes sociais, baseado no grau de conscientização dos pais ou responsáveis. Com base nisso, será possível propor estratégias e ações que contribuam para o aumento do nível de conscientização e adoção de boas práticas, promovendo uma evolução progressiva na conscientização dos pais em relação à segurança e privacidade digital dos filhos.

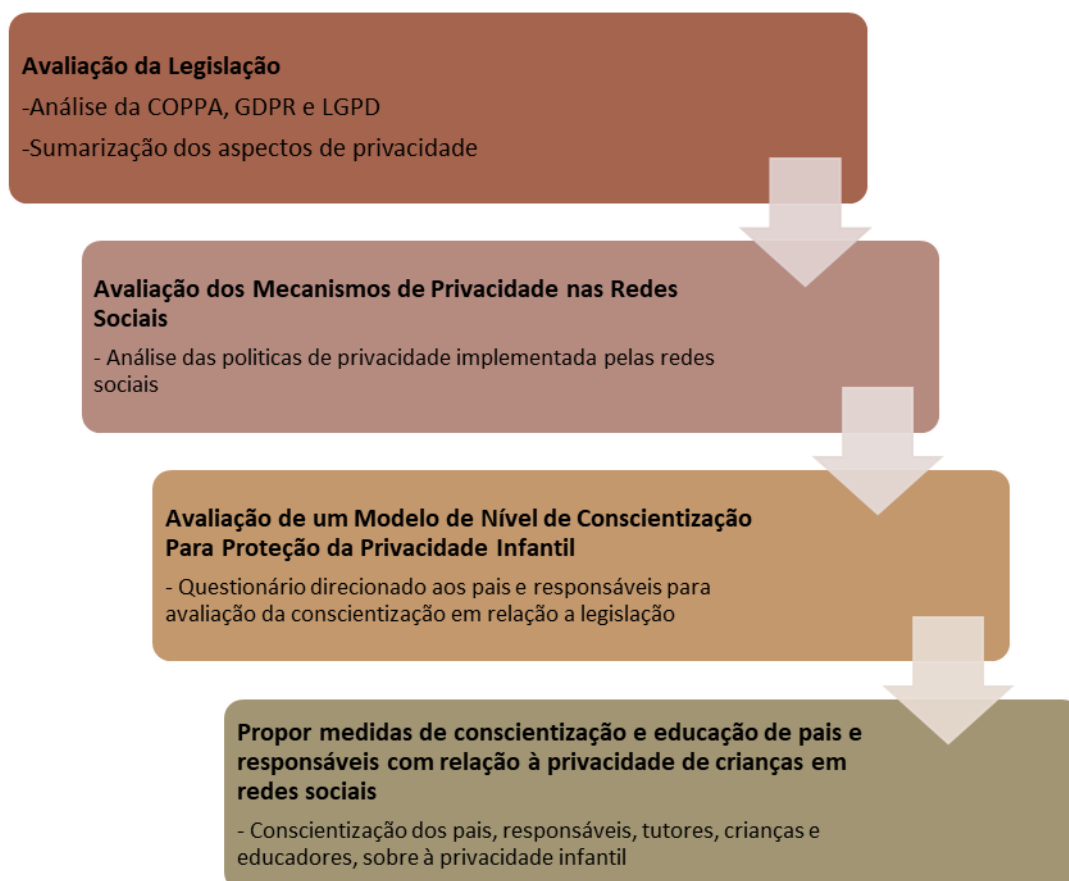


Figura 1. Método Proposto

Para tanto, a metodologia do trabalho é dividida em três partes, conforme exibido na Figura 1, sendo: (i) avaliar a legislação em relação a privacidade de redes sociais para menores de idade, (ii) avaliação dos mecanismos que são implementados nas redes sociais, (iii) desenvolvimento de um modelo de nível de conscientização para

mensurar o nível de conhecimento e as práticas adotadas por pais e responsáveis na proteção da privacidade digital de seus filhos, conformes os princípios de conformidade com a legislação (iv) proposição de medidas de conscientização para pais e responsáveis.

De maneira detalhada, a etapa de avaliação da legislação consiste em realizar uma análise abrangente das legislações nacionais e internacionais relacionada à privacidade de crianças nas redes sociais. Para isso foram analisados os aspectos de privacidades de algumas legislações, como a COPPA, a GDPR e a LGPD. A segunda etapa da proposta, apresenta os mecanismos que são implementados nas redes sociais para proteger a privacidade das crianças. Para isso serão analisadas as políticas de privacidade, configurações de privacidade disponíveis e os controles parentais.

Por fim, a terceira etapa consiste no desenvolvimento de um modelo de conscientização que possibilite a identificação e categorização do nível de proteção da privacidade das crianças nas redes sociais. Esse modelo será fundamentado na avaliação do nível de conhecimento e da conscientização digital dos pais e responsáveis, especialmente no que se refere às práticas de proteção de dados pessoais e privacidade infantil em ambientes digitais.

Nesse contexto, este capítulo está organizado da seguinte forma: a Seção 4.1 detalha a análise da legislação em relação a privacidade de redes sociais para menores de idade; a Seção 4.2 apresenta os mecanismos que são implementados nas redes sociais e, por fim, a Seção 4.3 descreve a criação de um modelo de nível de conscientização.

4.1. Aspectos de Privacidade

Conforme observado na fundamentação do presente documento, em relação a privacidade de dados das crianças, tem-se que existem três principais legislações que tratam a respeito de privacidade (COPPA, a GDPR e a LGPD). Para o propósito desse trabalho, é importante ter uma visão consolidada dessas leis, para isso denominamos como Aspectos de Privacidade. As subseções a seguir detalham cada aspecto de privacidade, considerando a ótica das leis vigentes.

Para todas as Leis, a COPPA, a GDPR e a LGPD os dados pessoais são quaisquer informações relacionadas a pessoa natural identificada ou identificável e

já o dado pessoal sensível é aquele vinculado a identificação da pessoa. É importante analisar esse atributo juntamente com o atributo de consentimento dos pais ou responsáveis, já que eles estão interligados entre si.

No que se refere a idade, observa-se que não há um consenso relacionado à idade da criança, já que cada Lei irá determinar de uma forma. De acordo com o GDPR da União Europeia, uma criança é definida como uma pessoa com idade inferior a 16 anos. A COPPA, legislação dos Estados Unidos, define crianças como indivíduos menores de 13 anos. Essa distinção é imprescindível, já que implica em diferentes obrigações e responsabilidades para empresas e provedores de serviços que trabalham com dados pessoais de crianças, incluindo a obrigação de obter o consentimento dos pais ou responsáveis antes de coletar, usar ou divulgar informações pessoais de crianças. No Brasil, alinhando-se com a definição de uma Lei complementar, o Estatuto da Criança e do Adolescente, define criança sendo até 12 anos.

Portanto, essas diferenças em relação a esse atributo irão implicar alguns desafios para as empresas, sites, já que eles atuam de forma global e devem estar adaptados a legislação de cada país, já que não existe uma lei que unifique esse tema. É essencial que empresas e organizações estejam cientes das exigências específicas de cada lei e estejam em conformidade para garantir o tratamento adequado dos dados pessoais de crianças.

A GDPR irá estipular que o consentimento dos pais ou responsáveis legais é necessário para processar os dados de uma criança, caso ela tenha menos de 16 anos. Ressalta-se que essa idade pode variar de 13 a 16 anos, dependendo das leis nacionais de cada país membro da UE.

A COPPA exige que os operadores de sites e serviços online direcionados a crianças menores de 13 anos obtenham o consentimento verificável dos pais antes de coletar, usar ou divulgar informações pessoais de crianças. Esse consentimento deve ser obtido de maneira apropriada e comprovável, garantindo que os pais estejam cientes das práticas de coleta e uso de dados pessoais de seus filhos.

Com a publicação do Enunciado Interpretativo nº 1/2023 pela Autoridade Nacional de Proteção de Dados (ANPD), em maio de 2023, foi esclarecido que, embora o consentimento dos pais ou responsáveis continue sendo a regra geral para o tratamento de dados pessoais de crianças, a LGPD admite exceções específicas,

desde que fundamentadas no melhor interesse da criança. Isso significa que, em determinadas situações, o tratamento poderá ocorrer sem o consentimento direto, desde que sejam observados princípios como a necessidade, a adequação, a transparência e a segurança dos dados.

É importante ressaltar a dificuldade para se comprovar que realmente existiu o consentimento dos pais para o tratamento dos dados, já que na maior parte dos casos, a obtenção do consentimento é feita de forma eletrônica, por meio de um simples botão de confirmação. Essa questão trará à tona mais um problema, que é a autenticidade do consentimento, ainda mais se a criança já tiver a capacidade de mentir sobre essa autorização. Por isso, a proteção eficaz da privacidade das crianças requer uma combinação de regulamentação sólida e de tecnologia adequada.

A transparência no uso das informações refere-se a como as informações deverão estar, isto é, de modo público e contendo o tipo de dado que foi coletado, para que ele será utilizado. Mas esse atributo vai além disso, ele exige que as empresas e sites forneçam explicações claras e compreensíveis sobre como os dados foram coletados, armazenados e compartilhados, além de ter o dever de informar aos usuários sobre seus direitos em relação aos dados pessoais, como podem acessar, corrigir ou excluir. A COPPA, a GDPR e a LGPD, todas essas leis irão destacar a importância da transparência no uso das informações, embora seja desafiador verificar se essas diretrizes estão sendo cumpridas. Isso porque envolve uma combinação de vigilância regulatória e conscientização por parte dos usuários, que no caso são os pais ou responsáveis e as crianças, que uma boa parte das vezes não estão cientes dos seus direitos. Algumas organizações podem não ser transparentes sobre as suas práticas de coleta, uso e compartilhamento, acarretando o não cumprimento da Lei.

O direito de revisar dados consiste na possibilidade de acessar, analisar e, se necessário, corrigir ou excluir informações pessoais que foram coletadas por uma organização. A COPPA, LGPD e GDPR reconhecem o direito dos indivíduos de revisar os dados pessoais que são coletados e processados por organizações, garantindo assim maior transparência, controle e proteção da privacidade online.

O princípio da minimização de dados estabelece que apenas os dados pessoais estritamente necessários para atingir os fins específicos e legítimos devem ser coletados e processados, evitando a coleta excessiva ou irrelevante de informações.

A COPPA, a GDPR e a LGPD aderem a esse princípio para garantir que a privacidade dos indivíduos seja respeitada e protegida.

No que se refere a finalidade limitada, observa-se que as leis estabelecem requisitos claros que deverão ser cumpridos, para que seja garantido a proteção da privacidade. Isto é, irão estabelecer que os dados pessoais devem ser coletados para finalidade específicas, legítimas e explícitas e, posteriormente, não podem ser processados de maneira diferente das finalidades originais.

Outro atributo relevante é o de aviso de tratamento de dados, que deverá estar de formas simples, clara e acessível, sendo importante que a criança e o responsável compreendam facilmente. No entanto, embora o consentimento muitas vezes seja claramente solicitado, os pais e responsáveis podem não entender completamente as implicações do compartilhamento de dados. Isso ocorre por vários motivos, como a falta de conhecimento sobre os direitos que possuem e os riscos envolvidos. Consequentemente, muitos acabam aceitando os termos sem a devida reflexão, muitas vezes confiando na empresa ou por conveniência, sem perceber o impacto real do compartilhamento de informações pessoais. A COPPA, a GDPR e a LGPD, tratam de maneira clara a respeito desse atributo.

O princípio da confidencialidade das informações coletadas, garantem que as empresas deverão proteger os dados pessoais que foram compartilhados, além do que caso divulgue para terceiros, deve estar ciente que ele faça a mesma proteção de dados.

O atributo de design orientado à privacidade refere-se à incorporação de medidas de privacidade desde o início do desenvolvimento do sistema, com o objetivo de garantir a conformidade com as regulações. As Leis de proteção de dados incentivam o design orientado a privacidade como uma forma proativa de garantir a conformidade com as leis.

4.1.1 Sumarização

A seguir, é apresentada uma síntese dos principais atributos relacionados à privacidade de dados pessoais infantis, com base nos marcos regulatórios da LGPD, GDPR e COPPA. A Tabela 2 oferece uma visão comparativa desses referenciais

legais, facilitando a compreensão dos elementos centrais que orientam a proteção da privacidade de crianças em ambientes digitais.

A partir dessa análise normativa, foram identificados nove aspectos essenciais que devem nortear a conscientização de pais e responsáveis. Esses aspectos abrangem desde a definição de dados pessoais, passando por critérios etários para consentimento, até princípios como transparência, minimização de dados e garantia de linguagem acessível. Tais elementos constituem uma base sólida para avaliar o grau de salvaguarda conferido à privacidade infantil, a partir do nível de compreensão e das práticas adotadas pelos responsáveis diante dos riscos associados à exposição de crianças nas redes sociais.

A comparação entre as três legislações mostra que, embora todas abordem pontos importantes — como a exigência de consentimento dos pais, o uso adequado dos dados e a limitação de finalidades —, existem diferenças importantes entre elas. Um dos principais pontos é a variação na idade que define quem é considerado criança, além dos tipos de medidas exigidas para proteger esses dados. Essa falta de padronização pode dificultar a atuação das redes sociais, especialmente as que operam em vários países, e confundir pais e responsáveis, que precisam entender regras diferentes para proteger a privacidade de seus filhos.

Tabela 2 . Sumarização dos atributos de privacidade de dados

Aspectos de Privacidade	Definição	LGPD	GDPR	COPPA
Definição de 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	Artigo 5º, Inciso I	Artigo 4º	Artigo 3º
Definição de Criança	Idades definidas para a necessidade do consentimento dos responsáveis sobre a proteção de dados	Até 12 anos	Até 16 anos	Até 13 anos
Consentimento dos pais ou responsáveis	Como regra, o tratamento de dados pessoais, deverá ser realizado pelos pais ou responsáveis	Artigo 14º, Parágrafo 1º e 5º	Artigo 8º, 1º e 2º	§312.3 §312.5
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, como correção, eliminação etc.	Artigo 6º, Inciso VI Artigo 14º,	Artigo 25º	§312.3 §312.8

		Parágrafo 2º		
Finalidade Limitada	Os dados das crianças só podem ser coletados para finalidades determinadas, específicas e legítimas	Artigo 6º, Inciso I	Artigo 5º, I	§312.10 §312.14, III
Minimização de Dados	A coleta de dados deve ser limitada ao mínimo necessário para atingir a finalidade específica.	Artigo 6º, Inciso III	Artigo.5º, C	§312.3
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	Artigo 14º, Parágrafo 3º	Artigo 38º	§312.5.C (1,2,3,4,5,6)
Aviso de tratamento de dados	O aviso de tratamento de dados deve estar de forma simples, clara e acessível	Artigo 14º, Parágrafo 6º	Artigo 39º	Artigo 12º 1 §312.4. A
Direito de Revisar os dados fornecidos	A qualquer momento os dados poderão ser revisados e ou apagados	Artigo 18º	Artigo 16º Artigo 17º	§312.6. A.1

Design Orientado à Privacidade	Organizações devem considerar e incorporar medidas de privacidade desde o início do desenvolvimento de produtos e serviços	Artigo 50º Artigo 50º, Parágrafo 1º	Artigo 25º (1,2,3)	
Confidencialidade das Informações Coletadas	As empresas devem proteger os dados pessoais que foram compartilhados, além do que caso divulgue para terceiros, deve estar ciente que esse terceiro faça a mesma proteção destes dados.	Artigo 6º, Inciso VII	Artigo 5º, F	§312.8

Fonte: Autoria Própria

4.2 Mecanismos que são implementados nas redes sociais

As redes sociais implementam diversos mecanismos que buscam garantir a privacidade dos usuários, em especial, as crianças. Esses mecanismos mudam de acordo com cada rede social, isso pode ser visto de forma negativa do ponto de vista do usuário, pois além de causar confusão para os usuários, pode acarretar uma desigualdade na proteção de privacidade, já que os mecanismos oferecidos variam em funcionalidade, facilidade de uso e abrangência, o que impacta diretamente a capacidade dos usuários e responsáveis de protegerem adequadamente os dados pessoais e a privacidade das crianças.

Entre esses mecanismos estão as configurações personalizáveis de privacidade, que permitem controlar quem pode acessar o perfil e as informações pessoais. Além disso, muitas plataformas limitam a coleta e o compartilhamento de dados para contas infantis, adotam políticas claras e linguagem acessível para obtenção de consentimento informado, e oferecem ferramentas de bloqueio e denúncia para evitar abusos. Também são comuns controles parentais que possibilitam aos responsáveis monitorar e limitar o uso das redes sociais pelas crianças. A autenticação forte e a limitação da publicidade direcionada completam as medidas adotadas para proteger a privacidade e a segurança dos menores nessas plataformas.

Para este tópico do trabalho foi realizado um estudo dos termos de uso do Youtube Kids e do TikTok, que atualmente são amplamente utilizadas pelas crianças, com a finalidade de avaliar os mecanismos que são implementados nesses serviços para que as Leis de privacidade de dados possa ser cumprida.

O YouTube Kids oferece duas opções de autenticação para os pais ou responsáveis. A primeira é vincular uma conta do Google já existente, permitindo que os responsáveis utilizem suas próprias credenciais para acessar a plataforma, o que facilita o processo de criação da conta para seus filhos. A segunda opção consiste na criação de uma nova conta específica para a plataforma, o que pode ser útil para separar as contas de adultos e crianças. Dependendo da escolha na criação da conta, diferentes recursos de proteção de dados podem ser disponibilizados, garantindo um controle adequado sobre a privacidade das informações.

Por outro lado, ao criar uma conta no TikTok, o usuário deve escolher entre dois métodos de autenticação: número de telefone ou endereço de e-mail. Cada uma dessas opções tem implicações para a segurança e a privacidade, influenciando o tratamento e a proteção dos dados pessoais dos usuários. As subseções a seguir explorarão em detalhes os aspectos de privacidade e as práticas adotadas por essas duas redes sociais, destacando como elas lidam com a proteção de dados e o controle oferecido aos pais e responsáveis.

4.2.3 Dados Pessoais

Ao acessar o YouTube Kids por meio de uma conta Google, é possível ativar o controle parental e configurar preferências de personalização para a criança. Caso o login não seja efetuado, o aplicativo é utilizado de forma desconectada. Quando vinculado a uma conta Google, são coletadas informações fornecidas pelo responsável, como nome, idade e mês de nascimento da criança. Já no modo desconectado, os dados coletados se limitam à idade, ano de nascimento e informações de acesso.

Por outro lado, o TikTok coleta diversos dados pessoais durante a criação da conta, tais como número de telefone, e-mail, data de nascimento, dados de pagamento, curtidas, compartilhamentos, histórico de buscas, histórico de navegação no aplicativo, características do dispositivo e informações sobre a localização aproximada do usuário.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece que o tratamento de dados pessoais deve ser realizado com o devido cuidado, incluindo, sempre que possível, a anonimização ou pseudonimização dos dados. A anonimização consiste na remoção ou alteração de informações que possam identificar diretamente o indivíduo, tornando os dados irreconhecíveis. No entanto, o TikTok não realiza a anonimização completa dos dados pessoais, uma vez que esses são utilizados para fornecer serviços personalizados, conforme descrito em sua política de privacidade. A anonimização total seria incompatível com a proposta da plataforma, que visa oferecer uma experiência adaptada ao perfil do usuário.

Durante o processo de criação de conta no TikTok, os termos de uso são apresentados na tela inicial, redirecionando o usuário para uma página onde são especificados os dados que serão coletados. O consentimento ocorre por meio da aceitação desses termos e da política de privacidade. O mesmo processo se aplica ao YouTube Kids. Ao aceitar essas condições, o usuário (ou seu responsável legal) autoriza

a coleta e o uso dos dados pessoais conforme estabelecido pela plataforma. Após a criação da conta, o próprio usuário pode ajustar suas preferências de privacidade por meio das configurações disponíveis.

4.2.4 Idade, Consentimento dos pais ou dos responsáveis

As redes sociais geralmente impõem restrições etárias para acesso às suas plataformas. No caso do YouTube Kids, o aplicativo pode ser utilizado por crianças de todas as idades; no entanto, se a criança tiver menos de 13 anos, o acesso deve ser autorizado e configurado por pais ou responsáveis legais.

Quando os usuários optam por acessar o YouTube Kids por meio de uma conta Google, é possível ativar controles parentais adicionais e configurar preferências de personalização. Contudo, essa opção também implica a coleta de um número maior de informações da criança. Por outro lado, ao utilizar o aplicativo de forma desconectada, são coletados menos dados, mas não há acesso às funções de controle parental nem à personalização da experiência de uso.

No TikTok, é exigido que o usuário informe sua data de nascimento no momento da criação da conta, sendo necessário ter, no mínimo, 12 anos. Em alguns países, esse limite é superior — como na Coreia do Sul e na Indonésia, onde a idade mínima permitida é 14 anos. Caso a plataforma identifique que o requisito etário não foi cumprido, a conta poderá ser suspensa ou excluída. Para reverter essa situação, o desbloqueio da conta pode exigir a submissão de recursos específicos, que variam conforme o país. Entre os métodos utilizados estão: envio de uma selfie com documento de identidade, foto com o pai/mãe ou responsável, autorização via cartão de crédito ou ainda estimativas baseadas em análise facial.

O atributo “idade” envolve múltiplos aspectos — culturais, sociais, legais e técnicos — que dificultam sua verificação precisa. Tanto o YouTube Kids quanto o TikTok baseiam-se, principalmente, na autoafirmação do usuário, o que torna o processo suscetível a manipulações. Essa fragilidade impacta diretamente na efetividade das restrições de idade e, conseqüentemente, na proteção da privacidade de dados de crianças.

Apesar de ambas as redes sociais oferecerem mecanismos de controle e consentimento, a dependência de informações autorrelatadas limita a eficácia da verificação de idade. Usuários ainda podem inserir dados falsos ou utilizar contas de terceiros para contornar as restrições, evidenciando os desafios persistentes na implementação de medidas eficazes de proteção infantil no ambiente digital.

4.2.5 Transparência do uso das informações e Direito de revisar os dados

O YouTube Kids e o TikTok possuem políticas voltadas à transparência no uso das informações dos usuários, por meio da adoção de termos de uso e políticas de privacidade. Esses documentos detalham como os dados são coletados, utilizados e compartilhados, configurando-se como mecanismos formais de transparência no tratamento das informações pessoais.

No entanto, embora essas redes sociais apresentem diretrizes sobre o uso dos dados, a efetividade da transparência é limitada por diversos fatores. Em primeiro lugar, o conteúdo das políticas muitas vezes é extenso, técnico e de difícil compreensão, especialmente para o público-alvo das redes (pais, responsáveis e crianças). Além disso, a linguagem jurídica e generalista dificulta o entendimento completo sobre o que, de fato, está sendo coletado e com quem os dados são compartilhados.

Outro ponto crítico está na forma como o consentimento é obtido. Frequentemente, ele ocorre de maneira passiva ou implícita, mediante a simples aceitação dos termos durante a criação da conta, sem garantir que o usuário (ou o responsável legal) tenha compreendido plenamente as implicações da decisão. Isso compromete a transparência e a autodeterminação informativa dos usuários — especialmente no caso de crianças, que são mais vulneráveis e dependem da mediação dos adultos. Assim, embora exista uma estrutura formal de transparência, a prática revela lacunas significativas que afetam o exercício consciente da privacidade digital.

4.2.6 *Minimização de dados e Finalidade Limitada*

O YouTube Kids e o TikTok especificam, em suas políticas de privacidade, as finalidades e os usos dos dados pessoais coletados. No caso do TikTok, a plataforma disponibiliza alguns mecanismos de controle para os usuários, permitindo que configurem aspectos relacionados à privacidade e à segurança — o autocontrole do usuário.

Apesar disso, observa-se um excesso na quantidade e na sensibilidade dos dados coletados pelo TikTok. A plataforma pode acessar informações como localização precisa, histórico de navegação, interações com outros usuários e até mesmo dados biométricos, como reconhecimento facial. Além disso, o aplicativo pode acessar conteúdos armazenados na área de transferência do dispositivo (texto, imagens, vídeos copiados), desde que o usuário conceda essa permissão.

Todavia, a maioria dos usuários não compreende plenamente as implicações do compartilhamento desses dados. A linguagem técnica dos termos de uso e a forma como as permissões são solicitadas dificultam o entendimento sobre os riscos associados, especialmente no contexto infantil.

4.2.7 *Aviso de Tratamento de dados*

O YouTube Kids e o TikTok apresentam avisos de tratamento de dados que informam os usuários sobre como suas informações são coletadas, utilizadas e compartilhadas. Esses avisos integram as políticas de privacidade de cada plataforma e visam garantir maior transparência no tratamento dos dados pessoais.

No caso do TikTok, o principal mecanismo utilizado para obtenção do consentimento é a aceitação dos termos de uso no momento do registro da conta. Além disso, a plataforma pode enviar notificações aos usuários sempre que houver atualizações em sua política de privacidade, termos de serviço ou em outras informações relevantes relacionadas à proteção de dados.

Já no YouTube Kids, o aviso de tratamento de dados ocorre durante a configuração da conta supervisionada, quando o responsável realiza o login por meio de

uma Conta Google. Nesse processo, o responsável deve consentir com a coleta de determinadas informações da criança, como nome, idade e preferências de conteúdo.

4.2.8 *Design Orientado à privacidade*

O atributo de design orientado à privacidade é pouco evidenciado nas plataformas TikTok e YouTube Kids, especialmente pela falta de ênfase prática nas suas políticas de privacidade. No TikTok, por exemplo, durante o processo de criação de conta, muitos usuários não são claramente direcionados aos termos de uso e à política de privacidade, o que contribui para uma aceitação automática e pouco crítica das condições impostas pela plataforma.

Como consequência, grande parte dos usuários aceitam o compartilhamento de dados pessoais sem compreender integralmente as implicações envolvidas. Além disso, ao acessar os documentos de política de privacidade, observa-se um formato textual extenso, técnico e pouco amigável, o que pode desestimular a leitura e dificultar o entendimento por parte do público geral — especialmente pais e responsáveis, no caso do uso por crianças.

4.2.9 Sumarização dos Mecanismos de Privacidade utilizados pelas Redes Sociais e seus problemas

O YouTube Kids e o TikTok possuem mecanismos e práticas voltados à proteção da privacidade e à segurança dos dados pessoais dos usuários, especialmente das crianças. No entanto, esses recursos nem sempre são fáceis de identificar ou acessar de forma imediata. Muitas vezes, pais, responsáveis ou tutores encontram dificuldades para compreender como esses mecanismos funcionam ou como podem ser utilizados de forma eficaz.

Além disso, as crianças ainda não possuem maturidade suficiente para entender a importância das configurações de privacidade ou as consequências de suas interações nas redes sociais. Isso pode levar ao uso inadequado das configurações ou à coleta de dados sem a devida consciência dos riscos envolvidos.

Portanto, apesar de existirem ferramentas de controle e mecanismos de segurança, esses recursos precisam ser mais acessíveis e intuitivos para garantir que os pais e as crianças possam entender facilmente as implicações das configurações e possam ajustá-las de forma eficaz para proteger a privacidade dos usuários.

Tabela 3. Sumarização dos Mecanismos de Privacidade das Redes Sociais

Aspectos de Privacidade	Redes Sociais	Mecanismos utilizados nas redes sociais	Problemas dos Mecanismos
Definição de dados pessoais	TikTok	Consentimento do usuário	Falta de clareza sobre como os dados serão utilizados.
	YouTube Kids	Consentimento do usuário	
Definição idade	TikTok	Autoafirmação do usuário	Crianças podem fornecer dados incorretos; idade nem sempre reflete maturidade digital.
	YouTube Kids	Autoafirmação do usuário	
Consentimento dos pais ou responsáveis	TikTok	Autoafirmação do usuário	Pais podem não estar cientes da extensão da coleta de dados. Falta de verificação eficaz da idade pelos pais ou responsáveis
	Youtube Kids	Autoafirmação do usuário	
Transparência do uso das informações	TikTok	Políticas de Privacidade e Termo de uso	Linguagem técnica difícil de entender para as crianças e pais. Pouco detalhamento sobre como os dados serão usados para personalização.
	Youtube Kids	Políticas de Privacidade e Termo de uso	
Finalidade Limitada	TikTok	Políticas de Privacidade e Termo de uso	Risco de dados serem utilizados para fins não especificados.
	Youtube Kids	Políticas de Privacidade e Termo de uso	

Minimização de Dados	TikTok	Autocontrole do usuário	Falta de opções para os usuários limitarem a quantidade de dados coletados
	Youtube Kids	Autocontrole do usuário	
Coleta de dados sem o consentimento dos pais	TikTok	Autoafirmação do usuário	Risco de menores fornecerem dados sem o conhecimento dos pais
	Youtube Kids	Autoafirmação do usuário	
Aviso de tratamento de dados	TikTok	Aceitação do Termo de Uso	Falta de compreensão do que implica aceitar os termos de uso
	Youtube Kids	Aceitação do Termo de Uso	
Direito de Revisar os dados fornecidos	TikTok	Ferramentas de Controle de Privacidade	Dificuldade em acessar e revisar os dados pessoais armazenados
	Youtube Kids	Ferramentas de Controle de Privacidade	
Design Orientado à Privacidade	TikTok	Inexistente	Ausência de práticas claras de privacy by design
	Youtube Kids	Interface mais amigável	
Confidencialidade das Informações Coletadas	TikTok	Criptografia de dados	Risco de violações de dados e acesso não autorizado.
	Youtube Kids	Criptografia de dados	

Fonte: Autoria Própria

4.3 Modelo de Conscientização Para Proteção de Privacidade das crianças

Este estudo propõe avaliar o nível de proteção à privacidade das crianças nas redes sociais, com base no grau de conscientização digital dos pais ou responsáveis. Para isso, será aplicado um questionário estruturado, que visa medir o conhecimento dos responsáveis e as ações por eles adotadas para resguardar os dados pessoais dos filhos no ambiente digital. O principal objetivo é identificar em que nível de conscientização digital

eles se encontram, a fim de compreender suas atitudes, dificuldades e desafios relacionados à privacidade online.

Inspirado no modelo de maturidade da SANS, descrito na fundamentação teórica, este estudo propõe uma adaptação voltada à privacidade infantil no contexto digital. A conscientização dos pais será avaliada em cinco níveis: (Security Awareness Maturity Model, 2025)

- **Nível 1 – Ausência de conscientização:** os pais desconhecem completamente os riscos digitais e a coleta de dados pessoais dos filhos, não adotando qualquer medida de proteção.
- **Nível 2 – Conscientização limitada:** há um entendimento superficial sobre a importância da privacidade, porém as ações práticas ainda são limitadas ou inexistentes.
- **Nível 3 – Compreensão moderada:** os pais demonstram algum conhecimento e adotam medidas pontuais, como ajustes básicos nas configurações de privacidade ou orientações esporádicas às crianças.
- **Nível 4 – Conscientização consistente:** os responsáveis têm uma compreensão mais sólida, aplicam práticas regulares e proativas de proteção, e educam os filhos de forma contínua sobre os riscos digitais.
- **Nível 5 – Conscientização avançada:** os pais não apenas protegem efetivamente os dados dos filhos, mas também atuam como defensores da privacidade digital, promovendo o tema em suas redes de convivência.

O nível de conscientização em relação à privacidade e segurança digital das crianças será determinado com base nas respostas fornecidas pelos pais ou responsáveis em um questionário estruturado. Cada pergunta está associada a comportamentos e atitudes que refletem diferentes níveis de conscientização na proteção da privacidade infantil no ambiente digital.

Neste modelo, a criança é o foco de avaliação quanto à proteção de seus dados pessoais, enquanto os pais ou responsáveis funcionam como mediadores — suas ações, conhecimentos e percepções serão analisados como indicadores do nível de proteção efetiva que a criança recebe. Assim, ao avaliar o grau de conscientização, conhecimento e as práticas adotadas pelos pais, será possível inferir o grau de proteção à privacidade da criança nas redes sociais. Esse modelo permite não apenas mapear a situação atual, mas

também identificar lacunas e oportunidades para fortalecer a privacidade infantil por meio de ações educativas, políticas públicas e desenvolvimento de ferramentas mais acessíveis.

Para isso, foram criadas perguntas que possam avaliar diferentes aspectos do conhecimento e da percepção dos pais sobre a privacidade e a proteção de dados dos seus filhos. Estas perguntas buscam identificar o grau de instrução dos pais, a idade e o sexo das crianças, bem como as redes sociais que elas utilizam e como os pais se envolvem na criação e gestão dos perfis dos seus filhos.

Além disso, as perguntas irão explorar o nível de conhecimento dos pais sobre a coleta de dados realizada pelas redes sociais, o grau de consciência de como esses dados são utilizados, e se os pais e ou responsáveis estão cientes das implicações legais e das práticas recomendadas pela LGPD. Através dessa análise, pretende-se identificar as lacunas de conhecimento e conscientização, possibilitando a criação de estratégias eficazes para aumentar o entendimento dos pais sobre a proteção da privacidade digital das crianças.

Este modelo de conscientização também abordará dimensões centrais, como o conhecimento dos pais sobre a coleta e o uso de dados pessoais das crianças, o envolvimento dos responsáveis na criação de perfis digitais e as ações tomadas para proteger esses dados.

Essa abordagem permite identificar possíveis lacunas entre o conhecimento percebido e o real, proporcionando uma visão mais precisa da conscientização dos pais em relação à privacidade digital de seus filhos.

Para compreender o nível de conhecimento e a percepção dos participantes em relação às práticas de privacidade adotadas pelas redes sociais no tratamento de dados de crianças, foi utilizada a Tabela 4. Para cada atributo de privacidade mencionado na Tabela 4, são apresentadas duas dimensões de análise:

- Conhecimento Autodeclarado, no qual os participantes avaliam seu próprio entendimento sobre o tema em uma escala Likert de 1 a 5 (sendo 1 "nenhum conhecimento" e 5 "pleno conhecimento");
- Métrica do Conhecimento, que propõe uma análise baseada na interpretação de trechos reais extraídos dos termos de uso de redes sociais populares. Os participantes devem posicionar-se novamente em escala, indicando o quanto compreendem ou concordam com as práticas descritas.

Essa abordagem permite identificar possíveis lacunas entre o conhecimento percebido e o real, proporcionando uma visão mais precisa do nível de conscientização dos pais em relação à privacidade digital de seus filhos.

O experimento foi realizado da seguinte forma:

Primeiramente, foi realizado um questionário para os pais ou responsáveis responderem de forma online, e a partir das respostas, é atribuído um nível de conscientização destes em relação ao conhecimento e envolvimento sobre a coleta e uso de dados pessoais. A tabela 4 exibe as perguntas que foram realizadas neste questionário:

Tabela 4. Perguntas do Formulário

#	Categoria	Pergunta	Objetivo
1	Perfil	Qual seu gênero?	Coletar dados demográficos para segmentar os resultados e observar se existem padrões relacionados ao gênero.
2	Perfil	Qual sua faixa etária?	Verificar a relação entre a idade dos pais e o nível de conhecimento sobre privacidade digital.
3	Perfil	Qual seu grau de instrução?	Avaliar a influência do nível educacional dos pais no grau de compreensão sobre as leis de proteção de dados e práticas de segurança digital.
4	Perfil	Qual a faixa etária da criança, sobre a qual você irá responder o questionário? Caso você tenha mais de 1 criança, menor de 12 anos, escolha a criança de menor idade.	Informação
5	Perfil	Qual o sexo da criança, sobre a qual você irá responder o questionário?	Coletar informações sobre o sexo das crianças para verificar se existem diferenças nas práticas de proteção de dados por sexo.

6	Perfil	Qual (ais) rede sociais que a criança, sobre a qual você irá responder o questionário, utiliza?	Identificar as plataformas mais utilizadas pelas crianças
7	Perfil	Essa criança possui perfil próprio em uma rede social ou acessa por meio de perfis terceiros (responsáveis e/ou amigos)?	Analisar o tipo de acesso das crianças às redes sociais, o que pode indicar o nível de controle exercido pelos pais.
8	Conhecimento (Definição de Idade)	Você considera que seu conhecimento sobre a definição de 'criança' segundo a LGPD é adequado? Marque sua opinião em uma escala de 1 a 5.	Verificar se os pais sabem que a LGPD, algumas redes sociais impõem restrições relacionadas à idade mínima.
9	Comprovação (Definição de Idade)	Considerando o trecho retirado do termo de uso de uma rede social: "...Você precisa ter no mínimo 13 anos de idade para usar o Serviço..." Em uma escala de 1 a 5, você considera que esta afirmação está de acordo com a LGPD?	
10	Conhecimento (Consentimento)	Qual é o seu nível de conhecimento em relação as exigências legais de idade e autorização parental, especialmente, considerando a criação de contas por crianças sem permissão dos pais? Marque sua opinião em uma escala de 1 a 5.	Verificar se os pais estão cientes das exigências legais relacionadas à autorização parental para o uso de redes sociais por menores, bem como aos termos de uso das plataformas.
11	Comprovação (Consentimento)	Considerando o trecho retirado do termo de uso de uma rede social: "...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...". Em uma escala de 1 a 5, qual o seu nível de conhecimento em relação aos termos de uso da rede social utilizada pela criança?	
12	Comprovação (Consentimento)	Algumas redes sociais proíbem o uso por menores de 13 anos, enquanto outras exigem autorização dos pais para a coleta e processamento de dados se o usuário for menor de 13 anos. Em uma escala de 1 a 5, qual é o seu nível de concordância com a necessidade de garantir que as redes sociais cumpram exigências de idade e autorização parental, especialmente considerando a possibilidade de crianças criarem contas sem permissão?	
13	Conhecimento (Transparência dos dados pessoais)	Você concorda com a afirmação: "Sinto que estou adequadamente informado sobre como os dados do meu filho são coletados e utilizados pelas redes sociais" Marque sua opinião em uma escala de 1 a 5.	Avaliar o grau de conhecimento dos pais, em relação como os dados de seus filhos são tratados pelas redes sociais, se

14	Comprovação (Transparência dos dados pessoais)	Em uma escala de 1 a 5, quanto você concorda que é apropriado que as redes sociais utilizem os dados das crianças para avaliar a eficácia dos anúncios e fornecer publicidade personalizada com base nos interesses e atividades deles na plataforma?	eles têm ciência dos usos desses dados para fins publicitários, por exemplo.
15	Conhecimento (Minimização de dados)	Você concorda com a quantidade de dados coletados pelas redes sociais das crianças? Marque sua opinião em uma escala de 1 a 5.	Validar o conhecimento sobre a quantidade de dados que as redes sociais coletam das crianças, como por exemplo a coleta de dados de localização.
16	Comprovação (Minimização de dados)	Considerando esse trecho retirado de uma rede social: “Ao criar uma conta em uma rede social e aceitar os Termos de Uso, você concorda com a coleta de informações sobre a localização aproximada, incluindo dados baseados em cartão SIM e/ou endereço IP”. Ou seja, isso implica que você está autorizando a disponibilização de informações, como a localização atual da criança. Em uma escala de 1 a 5, com base nisso, qual é o seu nível de concordância com a coleta dessas informações de localização ao aceitar os Termos de Uso?	
17	Conhecimento (Direito de Revisar)	Você está ciente de que a rede social permite a revisão (atualização) dos dados da criança na plataforma a qualquer momento, conforme previsto pela legislação? Marque sua opinião, em uma escala de 1 a 5.	Avaliar o conhecimento dos pais sobre o que as redes sociais oferecem de mecanismos para revisar os dados das crianças e se eles sabem como realizar essa revisão.
18	Comprovação (Direito de Revisar)	Esse trecho, retirado de uma rede social, menciona: “incluir o direito de acessar, excluir, atualizar ou retificar seus dados, ser informado sobre o tratamento de seus dados, apresentar reclamações às autoridades e, potencialmente, outros direitos”. Isso garante que você possa, por exemplo modificar os dados da criança como idade, e interesses a qualquer momento. Em uma escala de 1 a 5, se você precisasse revisar os dados da criança para interromper os anúncios direcionados, qual seria seu nível de conhecimento sobre como realizar essa alteração?	
19	Conhecimento (Finalidade limitada)	Você considera que a rede social utilizada pela criança é transparente sobre como as informações pessoais dela são coletadas, utilizadas e compartilhadas? Marque sua opinião, em uma escala de 1 a 5.	Avaliar se os pais compreendem que os dados devem ser coletados de forma limitada, como por exemplo se eles entendem que existem a possibilidade de as redes sociais compartilharem dados para terceiros.
20	Comprovação (Finalidade limitada)	Esse trecho, retirado dos termos de uso de uma rede social, menciona: “Também podemos divulgar suas informações a terceiros: caso vendamos ou compremos qualquer negócio ou ativo”. Isso quer dizer que as informações da criança podem ser compartilhadas com outras empresas, sem seu prévio conhecimento e aprovação. Em uma escala de 1 a 5, qual é seu nível de concordância com a prática de divulgar suas informações para terceiros?	
21	Conhecimento (Confidencialidade das informações)	Você concorda sobre como as redes sociais utilizam os dados para veicular anúncios direcionados às	Avaliar a concordância dos pais com a coleta

22		crianças? Marque sua opinião, em uma escala de 1 a 5.	de dados para fins publicitários direcionados às crianças.
	Comprovação (Confidencialidade das informações)	Ao aceitar os Termos de Uso em uma rede social, você concorda com a coleta de informações sobre os vídeos que a criança assiste, os termos de pesquisa e outras interações com conteúdo e anúncios no aplicativo. Isso significa que a rede social pode exibir anúncios baseados no histórico de vídeos da criança, mas não se responsabiliza pela coleta destes dados por outros sites visitados após clicar nesses anúncios. Em uma escala de 1 a 5, qual é seu nível de concordância com essa prática?	
23	Conhecimento (Aviso de tratamento de dados)	Você concorda com a clareza e a transparência do aviso de tratamento de dados das redes sociais sobre as informações da criança? Marque sua opinião, em uma escala de 1 a 5	Avaliar se os pais realmente compreendem sobre os termos de uso, que eles aceitam após a criação da rede social e todas as implicações dessa aceitação.
	24	Comprovação (Aviso tratamento de dados)	

Este estudo tem como objetivo avaliar se as crianças estão, de fato, sendo adequadamente protegidas em relação à sua privacidade no ambiente digital. Ao mapear as práticas e o conhecimento dos pais sobre privacidade digital, especialmente no que se refere à proteção dos dados das crianças, buscamos identificar se as ações dos responsáveis são eficazes na garantia da segurança das informações pessoais dos filhos. Além disso, ao abordar questões relacionadas à legislação de proteção de dados, como a LGPD, o estudo permitirá identificar lacunas no entendimento dos pais e como essas lacunas podem ser preenchidas, promovendo um ambiente digital mais seguro e confiável para as crianças.

Espera-se que os dados obtidos a partir do questionário ofereçam uma visão detalhada dos pontos de melhoria nas políticas de privacidade para menores, bem como indicar como os pais podem ser mais eficazes na gestão da privacidade digital de seus filhos.

CAPÍTULO 5

Coleta e Análise de Dados

Este capítulo tem como objetivo descrever o processo de coleta de dados voltado à investigação do nível de conscientização e das práticas adotadas por pais e responsáveis no que diz respeito à privacidade e à segurança digital de seus filhos.

A organização do capítulo está de forma que a Seção 5.1 irá descrever como foi aplicado a pesquisa. A seção 5.2 irá analisar o perfil dos participantes. Na seção 5.3 será avaliado o nível de proteção à privacidade. Na seção 5.4 será descrito a avaliação da conscientização parental na gestão da privacidade infantil, baseado na avaliação da pesquisa.

5.1 Aplicação da Pesquisa

De acordo com a resolução nº 466/12 “toda pesquisa envolvendo seres humanos deve ser submetida à apreciação de um Comitê de Ética em Pesquisa (CEP)”, e somente após a aprovação pode ser iniciado a coleta de dados. O projeto deste trabalho foi submetido ao comitê de ética e aprovado sob o número de CAAE 82341424.7.0000.0020 (em anexo).

A pesquisa realizada neste trabalho tem como objetivo principal avaliar a privacidade digital de crianças e adolescentes a partir do papel exercido pelos pais no seu gerenciamento. A investigação enfoca a percepção, o conhecimento prático e a capacidade de atuação dos pais em relação às redes sociais, buscando compreender o quanto estão preparados para proteger a exposição digital de seus filhos. Para orientar essa investigação, foram definidas três perguntas de pesquisa (RQs), que estruturam a coleta e análise dos dados, bem como a construção do modelo de conscientização proposto.

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 redes 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 são capazes de gerenciar a privacidade dos filhos nas redes sociais?

A primeira pergunta de pesquisa (RQ1) visa explorar a percepção que os próprios pais têm sobre sua competência e compreensão no que se refere às práticas de proteção da privacidade digital de seus filhos menores. A segunda pergunta de pesquisa (RQ2) tem como objetivo identificar possíveis lacunas entre o conhecimento declarado pelos pais e o conhecimento demonstrado por eles ao serem confrontados com situações práticas ou questões objetivas relacionadas à proteção da privacidade nas redes sociais. A terceira pergunta de pesquisa (RQ3) busca investigar se os pais são, de fato, capazes de gerenciar a privacidade digital de seus filhos nas redes sociais. Para isso, a análise será baseada em dados empíricos, considerando a relação entre o conhecimento autodeclarado e os resultados obtidos por meio de métricas específicas aplicadas para avaliar esse conhecimento. Essa abordagem permitirá verificar se há alinhamento entre a percepção que os pais têm de sua própria capacidade e suas ações concretas no ambiente digital. Dessa forma, será possível compreender, de maneira mais precisa, a presença — ou ausência — de competências e atitudes necessárias para assegurar a proteção da privacidade digital dos filhos nas redes sociais.

A coleta de dados foi realizada entre os meses de novembro de 2024 e abril de 2025. O questionário foi disponibilizado por meio de um link público e amplamente divulgado em redes sociais e plataformas de mensagens, com o objetivo de alcançar um público diversificado.

Ao todo, 77 pessoas responderam ao questionário, informando seu nível de conscientização, envolvimento e as medidas adotadas para proteger os dados de seus filhos em redes sociais. As respostas coletadas foram analisadas para identificar o nível de conscientização digital parental de cada participante, com base em seus conhecimentos e comportamentos alinhados aos principais princípios de proteção à privacidade.

Essa abordagem permite não apenas identificar lacunas entre o conhecimento percebido e o conhecimento prático, mas também avaliar o grau de criticidade com que

os responsáveis compreendem os mecanismos de coleta, uso e compartilhamento de dados pessoais das crianças.

5.2 Análise do Perfil dos Participantes

O perfil dos participantes está sumarizado na Figura 2. A análise dos dados revelou que a maioria dos participantes se encontra nas faixas etárias entre 26 e 45 anos, correspondendo a 85% do total — sendo 42% com idades entre 26 e 35 anos, e 43% entre 36 e 45 anos. A faixa de 18 a 25 anos representou 1% da amostra, enquanto os maiores de 45 anos corresponderam a 14%.

Quanto à escolaridade, observou-se um predomínio de indivíduos com ensino superior, sendo 83% com graduação completa e 12% com ensino superior incompleto. Apenas 5% dos respondentes tinham o ensino médio como maior nível de escolaridade.

No que diz respeito ao sexo das crianças mencionadas pelos responsáveis, observou-se uma distribuição relativamente equilibrada, com leve predominância do sexo masculino. Crianças do sexo masculino corresponderam a 57% da amostra, enquanto o sexo feminino representou 43%. Essa proporcionalidade permite afirmar que as conclusões extraídas dos dados possuem aplicabilidade relativamente equitativa entre meninos e meninas, no que se refere ao uso de privacidade em redes sociais.

A análise dos dados revela que a faixa etária de 2 a 5 anos é a mais representativa (49%) entre as crianças cujos responsáveis participaram da pesquisa. Na sequência, observam-se percentuais menores nas faixas de 6 a 9 anos e 10 a 12 anos, que tradicionalmente são associadas ao início do uso mais autônomo de dispositivos digitais, especialmente em contextos escolares e sociais. Ainda que essas faixas também representem uma parcela relevante da amostra, o destaque para a predominância da faixa de 2 a 5 anos evidencia que a presença infantil no ambiente digital está ocorrendo cada vez mais cedo.

Figura 2. Visão geral do perfil dos entrevistados da pesquisa

Gênero	Masculino 69%		Feminino 31%			
Faixa Etária	26 a 35 42%		18 a 25 1%	36 a 45 43%		45+ 14%
Escolaridade	EM 5%	Sup. Inc. 12%	Superior Completo 83%			
Idade do filho	2 a 5 49%		6 a 8 25%		9 a 11 26%	
Gênero do filho	Masculino 57%			Feminino 43%		
Rede Social	IG 10%	YouTube 9%	YouTube Kids 56%		lilok 17%	Outros 9%
Acesso	Perfil de terceiros 77%				Próprio perfil 23%	

Em relação à posse de perfis próprios em redes sociais, os resultados chamam atenção. Aproximadamente 23% das crianças mencionadas possuem perfis próprios em alguma plataforma digital, ainda que a maioria delas esteja abaixo da idade mínima exigida pelos termos de uso dessas redes sociais. A presença de perfis próprios entre crianças, especialmente na faixa etária inferior a 12 anos, representa um fator de risco potencial no que se refere à exposição a conteúdos inadequados, coleta indevida de dados pessoais e vulnerabilidade a práticas de publicidade direcionada. Esses dados reforçam a necessidade de medidas de conscientização voltadas aos pais e responsáveis, assim como o fortalecimento de mecanismos de verificação etária e proteção infantil nas redes sociais.

O perfil dos participantes irá contribuir de forma relevante para a compreensão dos desafios relacionados à privacidade infantil e ao uso de dados em ambientes digitais neste trabalho. Isso porque, conforme a figura 2 mostra, o nível de escolaridade dos respondentes é elevado, sugerindo um público com maior acesso à informação. Isso irá contribuir para uma compreensão crítica sobre os riscos e implicações do uso precoce da

internet por crianças. Além disso, o alto nível de escolaridade pode colaborar com a formulação de estratégias de conscientização mais eficazes, já que os responsáveis demonstram capacidade de compreender e aplicar orientações sobre segurança digital.

A predominância de adultos entre 26 e 45 anos também é significativa, pois corresponde a uma faixa etária geralmente mais familiarizada com tecnologias digitais e que, ao mesmo tempo, está diretamente envolvida com a criação de filhos pequenos. Esse contexto torna ainda mais pertinente a discussão sobre o papel da mediação parental no uso de dispositivos digitais por crianças.

Outro dado importante é a concentração de crianças na faixa etária de 2 a 5 anos, que representa 49% da amostra. Esse dado é relevante, uma vez que indica um contato precoce com tecnologias digitais. Essa faixa etária concentra crianças em fase pré-escolar, em processo de desenvolvimento cognitivo e afetivo intenso, o que levanta preocupações quanto à exposição a conteúdos e ambientes digitais sem mediação adequada. A presença tão cedo no ambiente digital levanta questões sobre a adequação dos conteúdos acessados, a ausência de filtros protetivos e a possível coleta indevida de dados.

Além disso, o fato de aproximadamente 23% das crianças mencionadas já possuírem perfis próprios em redes sociais, mesmo estando abaixo da idade mínima exigida pelas plataformas, reforça a urgência de medidas de proteção. A existência desses perfis representa um risco potencial quanto à exposição a conteúdos inadequados, à vulnerabilidade a práticas de publicidade direcionada e à coleta de dados pessoais sem consentimento apropriado.

Diante disso, o perfil da amostra não apenas confirma a atualidade e relevância dos temas abordados na pesquisa, como também evidencia a necessidade de políticas públicas, ações educativas voltadas aos pais e responsáveis, e o fortalecimento de mecanismos de verificação etária e segurança nas redes sociais. A participação de indivíduos com maior acesso à informação é estratégica para fomentar o debate público, validar diretrizes e promover boas práticas relacionadas ao uso consciente da tecnologia por crianças.

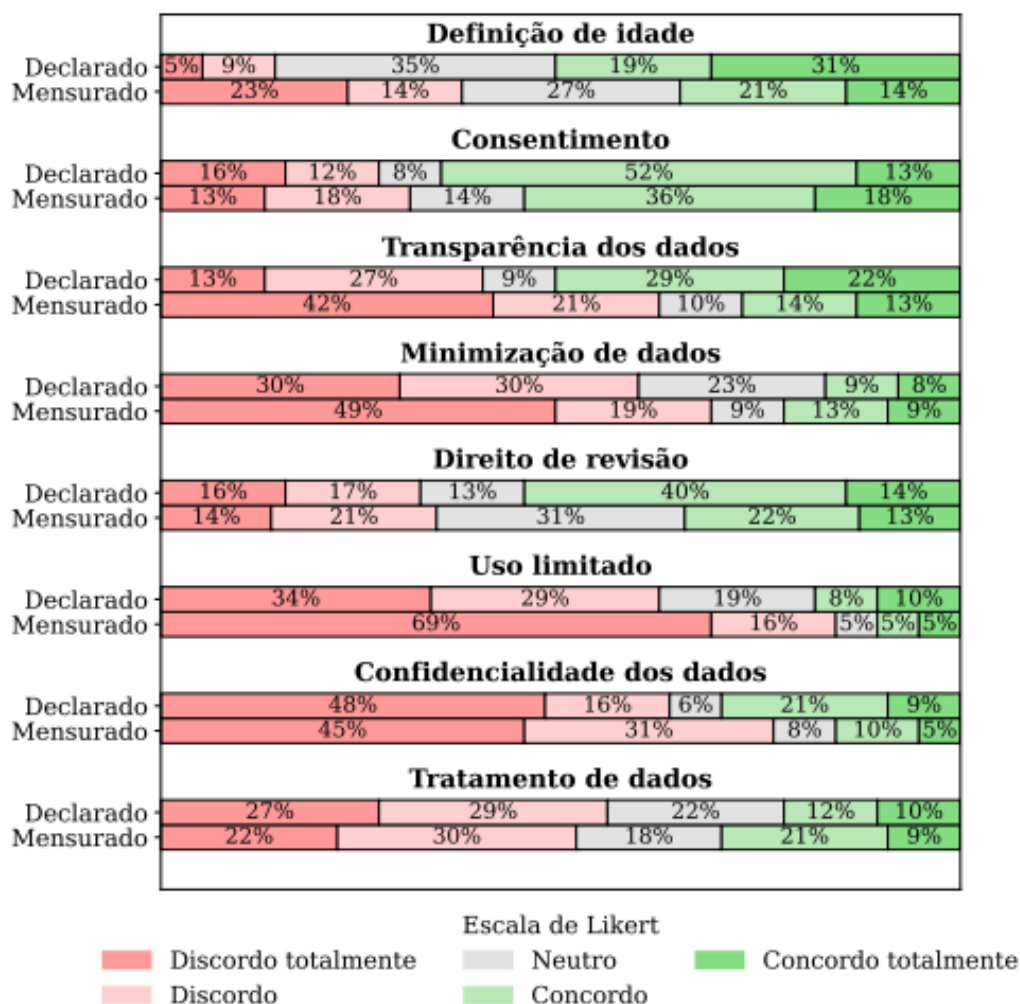
5.3 Avaliação do nível de proteção à privacidade, com base na conscientização dos responsáveis

Nesta seção serão analisadas as respostas do questionário obtidas por meio da Escala Likert, com o objetivo de avaliar o nível de proteção à privacidade das crianças,

considerando a conscientização dos responsáveis. A análise busca compreender o grau de conscientização, o entendimento e as práticas dos pais em relação à proteção dos dados pessoais dos filhos nas redes sociais.

Serão abordados aspectos essenciais, como a definição da idade mínima para uso, o consentimento dos pais, a transparência na coleta e uso dos dados, a minimização das informações coletadas, os direitos de revisão, a limitação da finalidade do tratamento, a confidencialidade e a clareza dos avisos. A Figura 3, a seguir apresenta o conhecimento declarado e a métrica de conhecimento dos responsáveis, seguida por uma análise detalhada de cada item.

Figura 3. Distribuição das respostas da pesquisa de acordo com cada atributo de privacidade avaliado (Tabela 2)



5.3.1 Definição de idade

Em relação a idade, 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.

5.3.2 Consentimento dos Pais

No item Consentimento, 65% dos respondentes declararam concordar ou concordar totalmente com as exigências legais de idade e autorização parental (52% e 13%, respectivamente). No entanto 54% efetivamente afirmaram saber que os pais ou responsáveis são legalmente responsáveis pelas atividades online de seus filhos (36% concordam e 18% concordam totalmente), enquanto 31% demonstraram discordância (13% discordam totalmente e 18% discordam).

Esses dados revelam que, embora a maioria reconheça a importância do consentimento, há uma lacuna significativa no conhecimento ou na aceitação da responsabilidade legal dos pais, o que pode comprometer a efetividade das medidas protetivas destinadas às crianças nas redes sociais.

5.3.3 Transparência dos dados

No item Transparência dos dados, em que 51% dos pais declararam estar informados sobre como os dados de seus filhos são coletados e utilizados pelas redes sociais — sendo 29% em concordância parcial e 22% em concordância total com essa afirmação. Todavia, na prática, essa percepção não se confirma, pois apenas 27% dos pais concordaram com as práticas das redes sociais — sendo 14% que concordaram e 13% que concordaram totalmente com as situações apresentadas na mensuração. Além do número de rejeição da prática, que foi de 63%.

Essa discrepância evidencia uma clara desconfiança dos pais e uma percepção de falta de transparência, sugerindo que as informações fornecidas pelas redes sociais não são suficientes ou claras o bastante para garantir a confiança dos responsáveis.

5.3.4 Minimização dos dados

No critério da Minimização de dados, no qual apenas 17% dos respondentes demonstraram concordância com a quantidade de informações coletadas pelas redes sociais — sendo 9% em concordância parcial e 8% em concordância total. Por outro lado, 68% dos participantes declararam discordar do volume de dados coletados, especialmente em relação a informações consideradas sensíveis ou excessivas, como a coleta da localização aproximada da criança.

Esses dados mostram que muitos pais não concordam com a quantidade de informações que as redes sociais coletam sobre seus filhos. A maioria considera que são coletados dados além do necessário, como a localização aproximada da criança, o que gera uma percepção negativa sobre esse processo.

5.3.5 Revisão dos Dados

No item Revisão de dados, que busca avaliar o conhecimento dos responsáveis sobre a possibilidade de atualização das informações pessoais, 54% dos respondentes afirmaram saber sobre a existência desse direito – o que demonstra um nível razoável de consciência teórica -. No entanto, quando questionados sobre como essa revisão poderia ser realizada, apenas 35% declararam saber como efetuar essa alteração na prática, evidenciando uma lacuna entre o conhecimento teórico e a aplicação efetiva desse direito.

Essa discrepância sugere que, embora os pais estejam cientes da existência do direito à correção dos dados, a falta de informações claras e acessíveis dificulta o exercício desse direito na prática.

5.3.6 Finalidade Limitada

No aspecto da finalidade limitada, que estabelece que os dados devem ser coletados para propósitos específicos e claramente definidos, apenas 18% dos pais afirmaram se sentir informados sobre como as redes sociais utilizam os dados de seus filhos — o que

indica uma percepção de falta de transparência por parte das redes sociais. Além disso, 85% dos respondentes declararam discordar das práticas adotadas pelas redes sociais, especialmente quanto à possibilidade de compartilhamento ou venda desses dados a terceiros, como ocorre em situações de compra, venda ou fusão de empresas.

Esses números apontam para uma forte percepção de falta de transparência e controle sobre a finalidade do tratamento dos dados, o que contribui para a insegurança dos pais. Além disso essa ausência compromete não apenas a percepção dos pais, mas também a possibilidade de exercício pleno dos direitos legais relacionados à privacidade de seus filhos, como a revogação do consentimento ou a limitação do uso dos dados para finalidades específicas.

5.3.7 Confidencialidade das Informações

No que se refere à confidencialidade das informações, princípio que garante a proteção dos dados pessoais coletados contra acessos não autorizados ou usos indevidos, observa-se que 30% dos pais demonstraram concordância com o uso de dados pelas redes sociais para veiculação de anúncios direcionados — sendo 21% em concordância parcial e 9% em concordância total. No entanto, 76% dos respondentes discordaram da afirmação de que a rede social não seria responsável pela coleta de dados em sites de terceiros acessados após o clique em um anúncio. Isso evidencia uma preocupação com a falta de controle e rastreabilidade do uso dos dados, especialmente no contexto da publicidade personalizada, que muitas vezes ocorre sem o conhecimento pleno do usuário.

5.3.8 Aviso de Tratamento de Dados

No que diz respeito ao aviso de tratamento de dados, os respondentes foram convidados a avaliar o nível de clareza e transparência das informações fornecidas pela rede social. Apenas 22% demonstraram concordância com a clareza do aviso — sendo 10% totalmente de acordo e 12% de acordo. Confirmando a falta de clareza, 52% indicaram que não consideram claras as informações relacionadas à forma de coleta, ao local de armazenamento e aos demais aspectos do tratamento dos dados pessoais.

Esse resultado evidencia uma falha significativa de comunicação entre as redes sociais e os usuários responsáveis por crianças. A linguagem técnica, extensa ou ambígua

dos termos de uso e políticas de privacidade, frequentemente redigida de forma a proteger juridicamente a empresa e não a informar o cidadão comum, dificulta a compreensão por parte dos pais, o que os impede de tomar decisões informadas sobre a exposição dos dados de seus filhos.

A ausência de avisos claros, completos e adequados compromete não apenas o direito à informação, mas também inviabiliza o exercício de outros direitos fundamentais previstos na legislação de proteção de dados, como o direito de acesso, de retificação, de eliminação e de oposição ao tratamento. Na prática, muitos pais desconhecem o que exatamente está sendo feito com os dados de seus filhos, quem são os destinatários dessas informações e quais são os canais disponíveis para questionar ou limitar esse uso.

5.3.9 Perguntas de Pesquisa

Para responder à primeira pergunta de pesquisa — qual é o conhecimento autodeclarado dos pais sobre como gerenciar a privacidade dos filhos em redes sociais —, foram analisadas as informações fornecidas diretamente pelos responsáveis. Os dados indicam que os pais se autodeclararam como relativamente bem-informados sobre os aspectos legais e práticos da proteção da privacidade digital de seus filhos. No entanto, essa percepção não necessariamente reflete um conhecimento efetivo ou aprofundado das políticas de privacidade das plataformas e da legislação vigente, como a LGPD.

Sobre a segunda pergunta de pesquisa — existe uma discrepância significativa entre o conhecimento mensurado e o autodeclarado pelos pais em relação ao gerenciamento da privacidade digital dos filhos? —, foram comparados os dados de percepção dos pais com os resultados obtidos a partir de questões práticas e objetivas. Os resultados indicam uma diferença expressiva entre o que os pais afirmam saber e o que demonstram conhecer ou aplicar efetivamente.

Em diversos aspectos avaliados, como transparência, revisão de dados e finalidade do uso das informações, observa-se que os pais tendem a superestimar seu nível de conhecimento. Por exemplo, 51% disseram compreender como os dados dos filhos são utilizados pelas redes sociais, mas apenas 27% concordaram com as práticas descritas, e 63% rejeitaram essas práticas — sinalizando desconfiança ou desconhecimento prático.

Para responder à terceira pergunta de pesquisa — os pais são capazes de gerenciar a privacidade dos filhos nas redes sociais? — foram analisados dados que avaliam tanto o conhecimento declarado quanto o comportamento prático dos responsáveis.

Os resultados indicam que, apesar de apresentarem um perfil educacional elevado, muitos pais enfrentam limitações importantes na prática do gerenciamento da privacidade digital de seus filhos. Aproximadamente 23% das crianças citadas possuem perfis próprios em redes sociais, frequentemente em desacordo com os termos de uso das plataformas, o que já revela falhas na mediação parental.

Embora a maioria dos pais demonstre insatisfação com a forma como as redes sociais coletam e utilizam os dados de seus filhos, essa preocupação não se reflete, na prática, em ações concretas de proteção à privacidade infantil. Os dados revelam que apenas 22% dos pais consideram claros os avisos sobre o tratamento de dados, apenas 17% concordam com a quantidade de informações coletadas pelas plataformas, e somente 18% se sentem informados sobre a finalidade para a qual os dados são usados. Esses baixos índices indicam que muitos pais não compreendem de forma adequada conceitos centrais da legislação de proteção de dados, como transparência, minimização da coleta e finalidade específica. Isso mostra que muitos pais não estão preparados para exercer um controle eficaz sobre a exposição digital dos filhos, seja por desconhecimento técnico ou por barreiras práticas no uso das ferramentas de privacidade disponíveis.

5.4 A Conscientização Parental na Privacidade Infantil

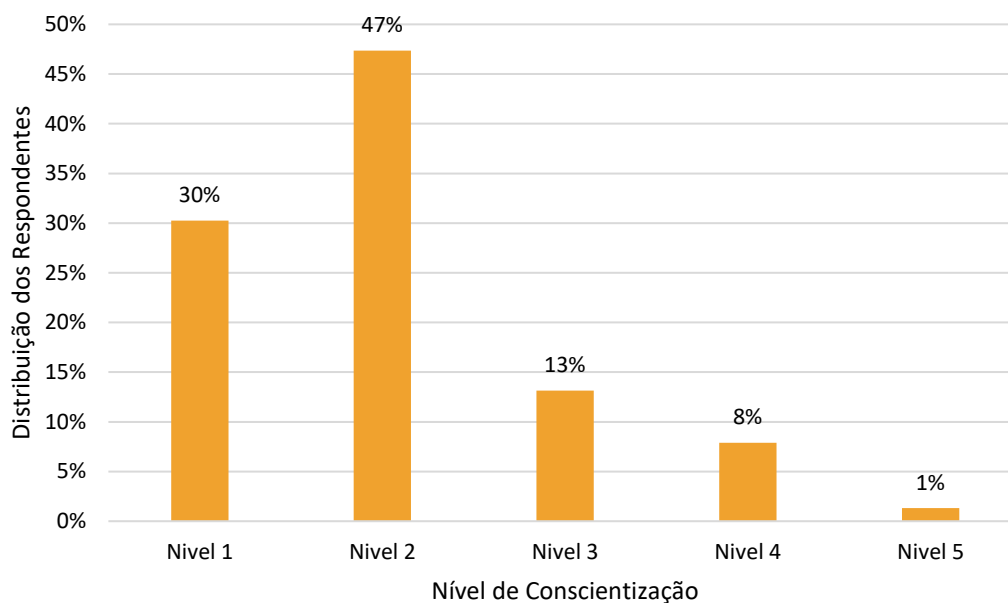
O nível de proteção à privacidade infantil foi avaliado com base na conscientização digital e legal dos responsáveis, por meio da análise de sua compreensão e posicionamento diante de trechos reais de termos de uso de redes sociais, bem como dos princípios estabelecidos pela LGPD.

A análise considerou nove questões destinadas a aferir o conhecimento dos respondentes. As respostas foram pontuadas conforme o grau de concordância: “discordo totalmente”, “discordo parcialmente” e “neutro” receberam zero pontos, por indicarem ausência de compreensão ou familiaridade com o tema. Já “concordo parcialmente” e “concordo totalmente” receberam, respectivamente, 1 e 2 pontos, refletindo níveis crescentes de alinhamento com os conceitos avaliados.

A atribuição de peso zero às respostas negativas ou neutras baseia-se no propósito da avaliação: mensurar o conhecimento efetivo sobre os direitos de proteção de dados pessoais das crianças. Respostas discordantes sugerem desalinhamento com os princípios da LGPD, enquanto a neutralidade aponta para incerteza ou desconhecimento. Por isso, apenas as respostas que indicam concordância foram pontuadas, pois revelam maior compreensão e familiaridade com o tema.

A figura 4 apresenta o gráfico com a porcentagem de responsáveis por nível de conscientização, identificando em que estágio se encontram quanto à sua capacidade de compreender e aplicar conceitos fundamentais relacionados à privacidade infantil no ambiente digital.

Figura 4. Distribuição dos respondentes por nível de conscientização



Fonte: Autoria Própria

A análise dos dados revelou que a maioria dos responsáveis estão em estágios iniciais de conscientização digital no que diz respeito à proteção de dados pessoais das crianças nas redes sociais. Cerca de 30% dos participantes foram classificados no Nível 1 – Ausência de conscientização, indicando que esses pais ou responsáveis desconhecem completamente os riscos digitais e não adotam qualquer medida de proteção em relação à coleta de dados dos filhos.

A maior parte da amostra, 47%, está no Nível 2 – Conscientização limitada, apresentando um entendimento superficial sobre o tema, com pouca ou nenhuma ação prática de proteção. Um grupo menor, correspondente a 13%, alcançou o Nível 3 – Compreensão moderada, demonstrando algum conhecimento e aplicando medidas pontuais, como ajustes básicos em configurações de privacidade ou orientações esporádicas às crianças. Apenas 8% atingiram o Nível 4 – conscientização consistente, caracterizado por uma compreensão sólida e práticas regulares de orientação e proteção digital. Por fim, apenas 1% dos participantes foram classificados no Nível 5 – Conscientização avançada, mostrando não apenas pela proteção efetiva dos dados dos filhos, mas também uma postura ativa de promoção da privacidade digital em seu ambiente social.

Esses resultados demonstram que devem ser promovidas estratégias educativas voltadas ao fortalecimento da conscientização digital e legal dos pais e responsáveis. A predominância de níveis baixos de conscientização indica uma lacuna significativa na compreensão dos direitos digitais das crianças e na capacidade de aplicar práticas efetivas de proteção à privacidade. Além disso, isso sugere que as regulamentações atuais, assumem a capacidade dos pais de desempenhar de forma eficaz esse papel de proteção.

5.5 Medidas de conscientização e educação de pais e responsáveis

A análise dos dados revelou que aproximadamente 77% dos responsáveis encontram-se em níveis iniciais de conscientização digital sobre a proteção dos dados pessoais das crianças nas redes sociais, o que é preocupante. Esse grupo inclui 30% sem qualquer noção dos riscos digitais e 47% com compreensão limitada e poucas ações práticas de proteção. Apenas uma pequena parcela apresenta níveis moderado a avançado de conscientização, indicando a necessidade urgente de medidas educativas para fortalecer a proteção da privacidade infantil.

Diante desse cenário, esta seção apresenta um conjunto de medidas recomendadas para a conscientização e educação dos responsáveis, visando aprimorar sua capacidade de proteger a privacidade infantil no ambiente digital. Essas propostas abrangem desde o entendimento dos fundamentos legais e técnicos da privacidade até estratégias práticas de supervisão e diálogo com as crianças, de modo a promover um ambiente virtual mais seguro e responsável.

i) **Compreender os Fundamentos da Privacidade Digital**
Pais e responsáveis devem adquirir conhecimentos básicos sobre o que constitui privacidade de dados no ambiente digital, incluindo o reconhecimento de informações pessoais e sensíveis, especialmente as relativas às crianças. Conhecer as legislações específicas, como a LGPD no Brasil, o GDPR na Europa e a COPPA nos EUA, é fundamental para garantir uma proteção eficaz.

ii) **Desmistificando Termos de Uso e Políticas de Privacidade**
As plataformas digitais costumam apresentar termos de uso extensos e complexos, dificultando a compreensão pelos usuários. É essencial que os pais se sintam motivados a ler e entender esses documentos. Recomenda-se que as redes sociais disponibilizem versões simplificadas ou guias que destaquem os pontos críticos sobre coleta, uso e compartilhamento de dados infantis, pois atualmente há pouca clareza e transparência nesses conteúdos.

iii) **Atenção à Idade Mínima e Criação de Contas**
Muitas crianças criam perfis nas redes sociais antes da idade mínima permitida, o que representa um risco à sua segurança e privacidade. Pais e responsáveis precisam estar atentos a essas restrições etárias e supervisionar a criação das contas, garantindo que as configurações de privacidade sejam rigorosas desde o início e que o consentimento parental, quando exigido, seja informado e genuíno.

iv) **Engajamento Ativo com Configurações de Privacidade**
É comum que os pais desconheçam ou não utilizem as configurações de privacidade disponíveis nas redes sociais. Para aumentar essa competência, tutoriais visuais e orientações práticas podem ser muito eficazes, ajudando-os a controlar quem pode acessar as informações e publicações das crianças, além de gerenciar contatos e o uso dos dados para publicidade.

vi) **Diálogo Aberto e Contínuo com as Crianças**
Além das ferramentas tecnológicas, a segurança digital depende de uma comunicação aberta entre pais e filhos. Estimular conversas frequentes sobre os riscos online, o cuidado com informações pessoais e as ações a serem tomadas em situações desconfortáveis fortalece a confiança e capacita as crianças a navegar com mais segurança.

As medidas apresentadas evidenciam a importância de fortalecer a conscientização dos pais e responsáveis sobre a proteção da privacidade das crianças nas redes sociais. Para que essas ações sejam efetivas, é fundamental que envolvam não só as famílias, mas

também escolas, instituições e a sociedade como um todo. Com a ampliação da educação digital dos responsáveis, será possível criar um ambiente online mais seguro, em que as crianças possam usufruir dos benefícios da tecnologia sem expor seus dados pessoais a riscos. Assim, espera-se que as propostas apresentadas inspirem futuras iniciativas que promovam mudanças reais no comportamento dos pais e garantam a proteção adequada das crianças no mundo digital.

Para trabalhos futuros, é fundamental buscar maneiras eficazes de levar as medidas de conscientização e educação até os pais e responsáveis. Uma estratégia importante é identificar quais canais de comunicação são mais acessados e confiáveis para esse público, como grupos de WhatsApp, redes sociais e reuniões escolares, adaptando as campanhas para esses meios.

Outra possibilidade é promover campanhas educativas em escolas e ambientes de trabalho, acompanhadas por pesquisas que avaliem o impacto dessas ações no aumento do conhecimento e na mudança de comportamento dos responsáveis. Além disso, estabelecer parcerias com instituições educacionais e empresas pode fortalecer essas iniciativas, integrando a conscientização digital aos programas dessas organizações.

6 Conclusão

A análise realizada ao longo deste trabalho evidencia que a privacidade de crianças em redes sociais é uma questão de alta complexidade e relevância. A crescente presença de menores em redes sociais, conforme apontado pela pesquisa TIC Kids Online (2024), destaca a exposição precoce ao ambiente online e, conseqüentemente, a vulnerabilidade desse grupo à coleta e uso inadequados de dados pessoais. Este cenário é agravado por práticas muitas vezes negligentes das plataformas digitais, como destacado por trabalhos relacionados, que mostram a falta de conformidade com regulamentações legais e a ineficácia de mecanismos, como a verificação de idade e consentimento parental (Liu et al., 2016; Irwin et al., 2017).

Os aspectos legais, tratados neste estudo por meio da análise da LGPD, GDPR e COPPA, revelam a disparidade entre as regulamentações nacionais e internacionais. Embora essas leis tragam avanços significativos na proteção de dados, a falta de padronização e a ausência de definições claras para crianças em muitos contextos dificultam sua aplicação uniforme. Por exemplo, a COPPA foca em crianças menores de 13 anos, enquanto a GDPR permite que as entidades definam idades mínimas entre 13 e 16 anos. Essa incoerência cria lacunas que deixam as crianças mais expostas, como apontado por Solove (2010) em sua taxonomia de problemas de privacidade.

A fundamentação teórica também ressaltou que a privacidade não é apenas um direito fundamental, mas um elemento essencial para o desenvolvimento psicossocial das crianças (Nolan et al., 2011). No entanto, como mostrado no trabalho de Eva e Anders (2019), as crianças têm uma compreensão limitada sobre o que constitui privacidade e segurança online, o que reforça a necessidade de uma mediação parental efetiva.

A pesquisa, realizada por Alkhalifah e Alghafis, revelou que muitos pais não possuem nível de maturidade para lidar com questões de privacidade digital (2022). A falta de conscientização e entendimento sobre as configurações de privacidade das plataformas prejudica a capacidade dos pais de proteger os dados de seus filhos. Além disso, as próprias plataformas frequentemente apresentam interfaces complexas e configuram padrões de privacidade abertos, dificultando a adoção de práticas seguras pelos usuários (Kayes e Iamnitchi, 2017).

Para abordar essas lacunas, o modelo de conscientização proposto neste trabalho busca identificar o nível de proteção à privacidade das crianças nas redes sociais, com base no grau de conscientização digital dos pais ou responsáveis. Essa abordagem visa não apenas identificar os pontos críticos, mas também orientar a criação de estratégias educacionais e tecnológicas para promover maior segurança online. Por exemplo, o trabalho de Paul (2012) propôs interfaces intuitivas para configurar privacidade, uma estratégia que pode ser aplicada no desenvolvimento de soluções orientadas ao público infantil.

Com o objetivo de abordar essa questão de maneira estruturada, foi proposta uma abordagem em três etapas. Na primeira, identificamos os principais atributos de privacidade relevantes para a proteção de dados de crianças, com base em três marcos regulatórios importantes: o Regulamento Geral sobre a Proteção de Dados (GDPR), a Lei de Proteção à Privacidade Online das Crianças (COPPA) e a Lei Geral de Proteção de Dados (LGPD). Essa análise permitiu estabelecer uma base normativa sólida que orienta a avaliação da conscientização dos responsáveis quanto ao tema.

Na segunda etapa, foi realizado um estudo comparativo dos termos de uso de duas redes sociais amplamente utilizadas por crianças: YouTube Kids e TikTok. O objetivo foi avaliar os mecanismos implementados por essas redes sociais para garantir a privacidade dos usuários infantis e verificar em que medida esses mecanismos atendem às exigências estabelecidas pelas legislações de proteção de dados. Observou-se que, embora existam mecanismos por parte dessas redes para cumprir as normas legais, eles podem variar significativamente entre os serviços. Essa falta de padronização pode gerar confusão entre os usuários e criar desigualdades na proteção da privacidade, especialmente no caso das crianças, que são mais vulneráveis.

Na terceira fase, foram realizadas entrevistas com 77 pais e responsáveis, com o objetivo de avaliar o grau de conscientização em relação à privacidade infantil. Isso foi analisado a partir de três dimensões principais: conscientização, compreensão e capacidade de aplicar medidas práticas de proteção de dados. O resultado da avaliação de conscientização dos pais e responsáveis, demonstrou que apenas 1% da amostra está em um nível de conscientização considerado avançado, e mais de 75% dos entrevistados se encontram em um nível de conscientização ausente ou limitado.

As descobertas obtidas a partir desse estudo revelam uma lacuna significativa entre o conhecimento autodeclarado pelos responsáveis e sua real competência prática. Muitos

deles demonstraram não estar plenamente preparados para atender às exigências legais relativas à privacidade infantil, o que levanta preocupações importantes quanto à eficácia da atual distribuição de responsabilidades prevista na legislação.

Diante do exposto, fica claro que a proteção da privacidade das crianças nas redes sociais é um desafio complexo, que exige a integração de esforços entre legislação, tecnologia e educação. A disparidade nas regulamentações, aliada à baixa conscientização dos pais e à complexidade das plataformas digitais, contribui para a vulnerabilidade dos menores no ambiente online. Portanto, é fundamental promover não apenas o aprimoramento das políticas públicas e o desenvolvimento de interfaces mais intuitivas, mas também investir em programas educativos que capacitem pais e responsáveis a compreenderem e aplicarem práticas eficazes de proteção.

Este trabalho evidencia que a conscientização digital dos pais é aspecto fundamental para garantir um ambiente seguro para as crianças nas redes sociais. Somente por meio de uma abordagem integrada, que envolva a atuação conjunta de famílias, instituições e desenvolvedores de tecnologia, será possível minimizar os riscos e assegurar que os direitos à privacidade e ao desenvolvimento saudável das crianças sejam respeitados e protegidos na era digital.

6.1 Trabalhos futuros

Com base na análise realizada e nos dados coletados por meio do formulário aplicado aos pais, as próximas etapas devem focar em ações práticas que promovam o aumento da conscientização e reforcem a proteção da privacidade das crianças no ambiente digital. Para isso, planeja-se desenvolver um Programa de Conscientização em Privacidade Digital voltado para crianças, pais e educadores, com o propósito de fortalecer o entendimento sobre a importância da proteção dos dados pessoais e incentivar práticas seguras, em conformidade com as legislações vigentes, como LGPD, GDPR e COPPA.

O objetivo é promover um ambiente online mais seguro e responsável para as crianças, por meio do desenvolvimento de materiais educativos, campanhas de sensibilização e atividades que envolvam toda a comunidade escolar e familiar.

6.2 Publicações Científicas

No desenvolvimento desse trabalho de pesquisa, foi publicado o seguinte artigo:

1. SOUSA, M. F.; VIEGAS, EDUARDO KUGLER; SANTIN, A. O. . **A Review of Social Network Regulations and Mechanisms for Safeguarding Children's Privacy**. In: International Conference on Advanced Information Networking and Applications (AINA), 2024. International Conference on Advanced Information Networking and Applications (AINA), 2024. p. 1-14. Qualis A3;

Os artigos a seguir foram aceitos para publicação:

2. SOUSA, M. F.; VIEGAS, EDUARDO KUGLER; SANTIN, A. O; GEREMIAS J.. **Toward an Assessment of Parental Maturity in Managing Child Privacy on Social Networks**. In: IEEE International Conference on Systems, Man, and Cybernetic (SMC), 2025. Qualis A2.
3. SOUSA, M. F.; VIEGAS, EDUARDO KUGLER; SANTIN, A. O. **Avaliação da Competência Parental na Gestão da Privacidade dos Filhos em Ambientes Digitais**. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), 2025. Qualis A4.

Referências

1. Fundação Getúlio Vargas (FGV). *Guia de Proteção de Dados Pessoais – Crianças e Adolescentes*. Versão 1.0, 2020
2. UNICEF. “Os direitos das crianças e dos adolescentes por que eles são importantes” <https://www.unicef.org/brazil/os-direitos-das-criancas-e-dos-adolescentes-e-por-que-eles-sao-importantes>
3. UNICEF. (2020). *Children's rights in the digital age: A download from the digital world*. UNICEF. Disponível em: <https://www.unicef.org/documents/childrens-rights-digital-age>
4. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L13709.htm. Acesso em: 16 nov. 2024.
5. UNIÃO EUROPEIA. Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial da União Europeia, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 16 nov. 2024
6. ESTADOS UNIDOS. Children's Online Privacy Protection Act (COPPA), Pub. L. No. 105-277, 112 Stat. 2681 (1998). Disponível em: <https://www.ftc.gov/legal-library/browse/statutes/children-s-online-privacy-protection-act>. Acesso em: 16 nov. 2024.

7. Convenção sobre os Direitos da Criança (1989). *Nações Unidas*. Disponível em: <https://www.ohchr.org/pt/professionalinterest/pages/crc.aspx>
8. Imrul Kayes, Adriana Iamnitchi, Privacy and security in online social networks: A survey, *Online Social Networks and Media*, Volumes 3–4, 2017, Pages 1-21, ISSN 2468-6964,
9. H. Nissenbaum , A contextual approach to privacy online, *Daedalus* 140 (4) (2011) 32–48 .
10. H. Jiang, J. Pei, D. Yu, J. Yu, B. Gong and X. Cheng, "Applications of Differential Privacy in Social Network Analysis: A Survey," in *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 1, pp. 108-127, 1 Jan. 2023, doi: 10.1109/TKDE.2021.3073062
11. Lingjing Yu, Sri Mounica Motipalli, Dongwon Lee, Peng Liu, Heng Xu, Qingyun Liu, Jianlong Tan, and Bo Luo. 2018. My Friend Leaks My Privacy: Modeling and Analyzing Privacy in Social Networks. In *Proceedings of the 23rd ACM on Symposium on Access Control Models and Technologies (SACMAT '18)*. Association for Computing Machinery, New York, NY, USA, 93–104. <https://doi.org/10.1145/3205977.3205981>
12. Neil Zhenqiang Gong and Bin Liu. 2016. You are who you know and how you behave: Attribute inference attacks via users' social friends and behaviors. In *Proceedings of the USENIX Security Symposium*. 979–995.
13. Ghazaleh Beigi and Huan Liu. 2020. A Survey on Privacy in Social Media: Identification, Mitigation, and Applications. *ACM/IMS Trans. Data Sci.* 1, 1, Article 7 (January 2020), 38 pages.
14. Jianming He, Wesley W. Chu, and Zhenyu Victor Liu. 2006. Inferring privacy information from social networks. In *Proceedings of the International Conference on Intelligence and Security Informatics*. Springer, 154–165.

15. Jack Lindamood, Raymond Heatherly, Murat Kantarcioglu, and Bhavani Thuraisingham. 2009. Inferring private information using social network data. In Proceedings of the Annual Conference of the World Wide Web (WWW'09). ACM, 1145–1146.
16. Kurt Thomas, Chris Grier, and David M Nicol. 2010. unfriendly: Multi-party privacy risks in social networks. In Proceedings of the International Symposium on Privacy Enhancing Technologies Symposium. Springer, 236–252.
17. UdiWeinsberg, Smriti Bhagat, Stratis Ioannidis, and Nina Taft. 2012. BlurMe: Inferring and obfuscating user gender based on ratings. In Proceedings of the 6th ACM Conference on Recommender Systems. ACM, 195–202.
18. S. Kruk , FOAM-Realm: control your friends access to the resource, in: Proceedings of the First Workshop on Friend of a Friend, 2004 .
19. H.C. Choi , S.R. Kruk , S. Grzonkowski , K. Stankiewicz , B. Davis , J. Breslin , Trust models for community aware identity management, in: Proceedings of the 2006 Identity, Reference and Web Workshop, in Conjunction with WWW, 2006, pp. 140–154 .
20. A.C. Squicciarini , F. Paci , S. Sundareswaran , Prima: a comprehensive approach to privacy protection in social network sites, Ann. Telecommun.-Ann. Télé- commun. 69 (1–2) (2014) 21–36 .
21. M. Shehab , G. Cheek , H. Touati , A. Squicciarini , P.-C. Cheng , User centric policy management in online social networks, in: Proceedings of the 2010 IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY), 2010, pp. 9–13 .
22. P.W. Fong , Relationship-based access control: protection model and policy language, in: Proceedings of the First ACM Conference on Data and Application Security and Privacy, 2011, pp. 191–202 .

23. T. Paul , M. Stopczynski , D. Puscher , M. Volkamer , T. Strufe , C4PS –helping facebookers manage their privacy settings, in: Proceedings of the 2012 Social Informatics, 2012, pp. 188–201 .
24. Jason Nolan, Kate Raynes-Goldie, and Melanie McBride. 2011. The Stranger Danger: Exploring Surveillance, Autonomy, and Privacy in Children’s Use of Social Media. *Journal of Childhood Studies* 36, 2: 24–32. <https://doi.org/10.18357/jcs.v36i2.15089>
25. Priya C. Kumar, Fiona O'Connell, Lucy Li, Virginia L. Byrne, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2023. Understanding Research Related to Designing for Children's Privacy and Security: A Document Analysis. In Proceedings of the 22nd Annual ACM Interaction Design and Children Conference (IDC '23). Association for Computing Machinery, New York, NY, USA, 335–354. <https://doi.org/10.1145/3585088.3589375>
26. Carly Nyst, Amaya Gorostiaga, and Patrick Geary. 2018. Industry Toolkit: Children’s Online Privacy and Freedom of Expression. UNICEF. Retrieved from [https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression\(1\).pdf](https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf)
27. Federal Trade Commission. 2014. Net Cetera: Chatting with Kids About Being Online. U.S. Federal Trade Commission. Washington, DC.
28. Google. 2017. Digital Citizenship & Safety Curriculum. Google.
29. Raynes-Goldie, K. and Allen, M. 2014. Gaming Privacy: a Canadian case study of a children’s co-created privacy literacy game. *Surveillance & Society*. 12, 3 (Jun. 2014), 414–426.
30. “YouTube pays big for tracking kids” By Lisa Weintraub Schifferle, Attorney, FTC, Division of Consumer & Business Education. Online: <https://consumer.ftc.gov/consumer-alerts/2019/09/youtube-pays-big-tracking-kids>

31. Irwin Reyes, Primal Wieseckera, Abbas Razaghpanah, Joel Reardon, Narseo Vallina-Rodriguez, Serge Egelman, and Christian Kreibich. 2017. "is our children's apps learning?" automatically detecting COPPA violations. In Workshop on Technology and Consumer Protection (ConPro 2017). Workshop on Technology and Consumer Protection (ConPro 2017), in conjunction with the 38th IEEE Symposium on Security and Privacy (IEEE S&P 2017). San Jose, CA, USA
32. Liccardi, Ilaria, Joseph Pato, and Daniel J. Weitzner. "Improving mobile app selection through transparency and better permission analysis." *Journal of Privacy and Confidentiality* 5.2 (2014): 1-55.
33. J. Manoogian. How free apps can make more money than paid apps. TechCrunch, August 26 2012.
34. d. boyd, E. Hargittai, J. Schultz, and J. Palfrey, "Why parents help their children lie to Facebook about age: Unintended consequences of the 'Childrens Online Privacy Protection Act'," *First Monday*, vol. 16, no. 11, 2011.
35. M. Liu, H. Wang, Y. Guo, and J. Hong, "Identifying and analyzing the privacy of apps for kids," in *ACM HotMobile*, 2016.
36. S. Bennett, K. Maton, and L. Kervin, "The 'digital natives' debate: A critical review of the evidence," *British Journal of Educational Technology*, vol. 5, pp. 775–786, 2008.
37. J. Harris, S. Speers, M. Schwartz, and K. Brownell, "US food company branded advergames on the Internet: Childrens exposure and effects on snack consumption," *Journal of Children and Media*, vol. 6, no. 1, pp. 51–68, 2011
38. J. Turow and L. Nir, "The Internet and the family 2000. The view from parents. The view from kids," Pennsylvania: The Annenberg Public Policy Center of the University of Pennsylvani, 2000.


39. 2024. Instagram Help Center. <https://help.instagram.com/116024195217477>.
40. Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences*, 25(1), 1-24.
41. Jessica N. Rocheleau and Sonia Chiasson. 2022. Privacy and Safety on Social Networking Sites: Autistic and Non-Autistic Teenagers' Attitudes and Behaviors. *ACM Trans. Comput.-Hum. Interact.* 29, 1, Article 1 (February 2022), 39 pages.
42. Jo Bryce and James Fraser. The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions. *Computers in Human Behavior*, 30:299{306, 2014.
43. Amandeep Dhir, Puneet Kaur, Kirsti Lonka, and Marko Nieminen. Why do adolescents untag photos on Facebook? *Computers in Human Behavior*, 55:1106{1115, 2016.
44. Ellen Van Gool, Joris Van Ouytsel, Koen Ponnet, and Michel Walrave. To share or not to share? Adolescents' self-disclosure about peer relationships on Facebook: An application of the Prototype Willingness Model. *Computers in Human Behavior*, 44:230{239, 2015.
45. Michel Walrave and Wannes Heirman. Adolescents, online marketing and privacy: Predicting adolescents willingness to disclose personal information for marketing purposes. *Children & Society*, 27(6):434{447, 2013.
46. Sangmi Chai, Sharmistha Bagchi-Sen, Claudia Morrell, H Raghav Rao, and Shambhu J Upadhyaya. Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication*, 52(2):167{182, 2009.

47. David Blackwell, Carrie Leaman, Rose Tramosch, Ciera Osborne, and Miriam Liss. Extraversion, neuroticism, attachment style and fear of missing out as predictors of social media use and addiction. *Personality and Individual Differences*, 116:69{72, 2017.
48. Ana Radovic, Theresa Gmelin, Bradley D Stein, and Elizabeth Miller. Depressed adolescents' positive and negative use of social media. *Journal of adolescence*, 55:5{15, 2017.
49. Louis Leung. Predicting Internet risks: A longitudinal panel study of gratifications-sought, Internet addiction symptoms, and social media use among children and adolescents. *Health Psychology and Behavioral Medicine: An Open Access Journal*, 2(1):424{439, 2014.
50. Louis Leung and Paul SN Lee. The influences of information literacy, Internet addiction and parenting styles on Internet risks. *New Media & Society*, 14(1):117{136, 2012.
51. Emily Christofides, Amy Muise, and Serge Desmarais. Risky disclosures on Facebook: The effect of having a bad experience on online behavior. *Journal of adolescent research*, 27(6):714{731, 2012.
52. Cong Liu, Rebecca P Ang, and May O Lwin. Cognitive, personality, and social factors associated with adolescents' online personal information disclosure. *Journal of adolescence*, 36(4):629{638, 2013.
53. Wonsun Shin and Nurzali Ismail. Exploring the role of parents and peers in young adolescents' risk taking on social networking sites. *Cyberpsychology, Behavior, and Social Networking*, 17(9):578{583, 2014.

56. Lotta Lofgren-Martenson, Emma Sorbring, and Martin Molin. T@ngled up in blue: Views of parents and professionals on internet use for sexual purposes among young people with intellectual disabilities. *Sexuality and disability*, 33(4):533-544, 2015.
57. Porfirio, G., & Almeida, R. (2021). *A compreensão dos pais sobre a LGPD e o compartilhamento de dados de crianças nas redes sociais*. *Revista Brasileira de Direito Digital*, 3(1), 45-62.
58. Mendes, J. T., Silva, L. M., & Rocha, T. A. (2022). *Responsabilidade dos pais na proteção de dados de crianças: uma análise sob a perspectiva da LGPD*. *Cadernos de Estudos em Direito*, 8(2), 112-130.
59. Livingstone, S., Stoilova, M., & Nandagiri, R. (2020). *Children's data and privacy online: Growing up in a digital age*. London School of Economics and Political Science.
60. Byrne, J., Kardefelt-Winther, D., Livingstone, S., & Stoilova, M. (2018). *Global Kids Online: Researching children's rights globally in the digital age*. Innocenti Research Briefs no. 2. UNICEF Office of Research.
61. Kumar, P., & O'Hara, K. (2019). *Privacy and safety risks for children on online platforms: A review of COPPA compliance and parental awareness*. *Journal of Internet Law*, 23(4), 15-32.
62. Manohar, M., & Murthy, V. (2021). *Compliance challenges of COPPA: Parental awareness and its implications on children's online activities*. *Journal of Policy and Internet Studies*, 14(3), 89-105.
63. Zaman, B., & Nouwen, M. (2020). *Parenting in the digital age: Understanding parental guidance and children's data privacy concerns globally*. *Media International Australia*, 177(1), 77-90.

7 ANEXOS

7.1 Parecer consubstanciado do CEP

<p>PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ - PUC/ PR</p> 																
PARECER CONSUBSTANCIADO DO CEP																
DADOS DO PROJETO DE PESQUISA																
Título da Pesquisa: Mecanismos de Privacidade para Crianças em Redes Sociais																
Pesquisador: ALTAIR OLIVO SANTIN																
Área Temática:																
Versão: 3																
CAAE: 82341424.7.0000.0020																
Instituição Proponente: Pontifícia Universidade Católica do Parana - PUCPR																
Patrocinador Principal: Financiamento Próprio																
DADOS DO PARECER																
Número do Parecer: 7.213.076																
Apresentação do Projeto:																
Texto copiado a partir do arquivo "PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_2374422.pdf"																
Desenho:																
A pesquisa a ser desenvolvida é de natureza exploratória, visando propor melhorias nos mecanismos de privacidades em redes sociais voltadas para o uso por crianças. A pesquisa em questão emprega o método Design Science Research Methodology (DSRM), visando criar um artefato que busca entender a percepção de privacidade das crianças em redes sociais, sob a ótica dos pais ou responsáveis																
Resumo:																
A ascensão da tecnologia digital e das redes sociais tem transformado a forma como as pessoas de todas as idades se comunicam, trazendo a luz preocupações significativas sobre a privacidade dos usuários, especialmente aqueles menores de idade. Essas interações online proporcionam às crianças conforto ao se conectar, comunicar, interagir e jogar. Em meio a esse cenário, as sociedades em todo o mundo estão cada vez mais preocupadas com a privacidade e a segurança das crianças, reconhecendo que as violações de																
<table border="0" style="width: 100%;"> <tr> <td colspan="4">Endereço: Rua Imaculada Conceição, n° 1155 - prédio administrativo, térreo</td> </tr> <tr> <td>Bairro: Prado Velho</td> <td colspan="2"></td> <td>CEP: 80.215-901</td> </tr> <tr> <td>UF: PR</td> <td>Município: CURITIBA</td> <td colspan="2"></td> </tr> <tr> <td>Telefone: (41)3271-2103</td> <td>Fax: (41)3271-2103</td> <td colspan="2">E-mail: nep@puopr.br</td> </tr> </table>	Endereço: Rua Imaculada Conceição, n° 1155 - prédio administrativo, térreo				Bairro: Prado Velho			CEP: 80.215-901	UF: PR	Município: CURITIBA			Telefone: (41)3271-2103	Fax: (41)3271-2103	E-mail: nep@puopr.br	
Endereço: Rua Imaculada Conceição, n° 1155 - prédio administrativo, térreo																
Bairro: Prado Velho			CEP: 80.215-901													
UF: PR	Município: CURITIBA															
Telefone: (41)3271-2103	Fax: (41)3271-2103	E-mail: nep@puopr.br														
Página 01 de 06																

Continuação do Parecer: 7.213.076

privacidade no ambiente digital podem ocorrer de várias formas. Isso é evidenciado pela promulgação de legislações específicas e por decisões judiciais em diversos países, refletindo o reconhecimento global da importância de preservar a privacidade em face do avanço tecnológico. No entanto, existe uma lacuna entre o que a legislação estabelece e a prática relacionada ao uso de redes sociais por crianças. Por exemplo, embora o Facebook proíba explicitamente o uso por crianças em seus termos de serviço, milhões delas utilizam a plataforma, com ou sem consentimento dos pais. Esta pesquisa visa avaliar a percepção dos pais ou responsáveis sobre a privacidade de seus filhos em redes sociais. Além disso, identificamos oportunidades de melhorias nos mecanismos de privacidade em plataformas amplamente utilizadas por crianças, como YouTube Kids e TikTok, e usaremos a pesquisa para avaliar sua aceitação pelos pais. O experimento será conduzido com voluntários que responderão a perguntas sobre os aspectos de privacidade das crianças em redes sociais. Posteriormente, com base nas respostas, avaliaremos se os mecanismos propostos contribuem para melhorar o controle de privacidade em redes sociais.

Hipótese:

Os pais não têm domínio/conhecimento do que a legislação impõe nas plataformas, em relação à privacidade de dados.

Critério de Inclusão:

Qualquer pessoa maior de 18 anos que seja pai, mãe, responsável ou tutor de crianças a partir de 2 anos de idade até 12 anos.

Critério de Exclusão:

Não serão aceitas pessoas que não sejam responsáveis, pais ou tutores de crianças.

Objetivo da Pesquisa:

Texto copiado a partir do arquivo "PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_2374422.pdf"

Endereço: Rua Imaculada Conceição, n° 1155 - prédio administrativo, térreo
Bairro: Prado Velho CEP: 80.215-901
UF: PR Município: CURITIBA
Telefone: (41)3271-2103 Fax: (41)3271-2103 E-mail: nep@puopr.br

Continuação do Parecer: 7.213.076

Objetivo Primário:

O objetivo primário deste trabalho é investigar o nível de maturidade dos pais e responsáveis em relação aos mecanismos de privacidade utilizados

em redes sociais, expondo os riscos associados à proteção dos dados das crianças e adolescentes.

Objetivo Secundário:

1. Conscientizar os pais e responsáveis a respeito dos riscos relacionado à privacidade das crianças em redes sociais; 2. Avaliar o nível de confiança dos pais nas plataformas de redes sociais, em relação à proteção da privacidade de dados de seus filhos; 3. Compreender os resultados obtidos até o momento por meio da análise dos estudos realizados; 4. Propor melhoria nos mecanismos de privacidade em redes sociais para crianças. 5. Avaliar as melhorias sugeridas.

Avaliação dos Riscos e Benefícios:

Texto copiado a partir do arquivo "PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_2374422.pdf"

Riscos:

Todos os esforços serão considerados para que os respondentes não tenham qualquer risco. No entanto, existe o risco de o participante sentir-se constrangido em participar. Neste caso, o participante poderá manifestar seu desconforto e abandonar a pesquisa a qualquer momento. Os dados pessoais dos participantes (demográficos) somente serão divulgados de forma agrupada nos resultados desta pesquisa, garantindo seu anonimato.

Benefícios:

Os resultados da pesquisa serão úteis para pais ou responsáveis por crianças de até 16 anos, uma vez que o estudo resultará em novos mecanismos de privacidade para crianças em redes sociais. Além disso, os participantes da entrevista serão conscientizados em relação aos riscos de privacidade relacionado as crianças.

Comentários e Considerações sobre a Pesquisa:

Ver Conclusões ou Pendências e Lista de Inadequações

Endereço: Rua Imaculada Conceição, n° 1155 - prédio administrativo, térreo
Bairro: Prado Velho CEP: 80.215-901
UF: PR Município: CURITIBA
Telefone: (41)3271-2103 Fax: (41)3271-2103 E-mail: nep@puopr.br

Continuação do Parecer: 7.213.076

Considerações sobre os Termos de apresentação obrigatória:

Ver Conclusões ou Pendências e Lista de Inadequações

Recomendações:

Para as próximas submissões de projeto ao CEP, ou mesmo, elaboração de projetos, é importante considerar:

Rever se todas os segmentos do projeto são consistentes. Por exemplo, na submissão do dia 25/10/2024 consta no formulário a ser respondido pelo pai/responsável

4) Qual a faixa etária da criança, sobre a qual você irá responder o questionário? Caso você tenha mais de 1 criança, menor de 12 anos, escolha a criança de menor idade.

*

2 a 5 anos

6 a 8 anos

9 a 11 anos

Acima de 12 anos

Porem no criterio de inclusao consta

Critério de Inclusão:

Qualquer pessoa maior de 18 anos que seja pai, mãe, responsável ou tutor de crianças a partir de 2 anos de idade até 12 anos.

Em principio crianças acima de 12 anos não atendem ao criterio de inclusao.

Consta do título do formulário apresentado ao participante

"Avaliação dos Mecanismos de Privacidade para crianças, maiores de 2 e menores de 12 anos de idade, em Redes Sociais."

Esta prática de revisão, em relação ao CEP, propicia que o projeto seja aprovado sem necessidade de tantas rodadas.

Endereço: Rua Imaculada Conceição, n° 1155 - prédio administrativo, térreo
 Bairro: Prado Velho CEP: 80.215-901
 UF: PR Município: CURITIBA
 Telefone: (41)3271-2103 Fax: (41)3271-2103 E-mail: nep@pucpr.br

Continuação do Parecer: 7.213.076

Conclusões ou Pendências e Lista de Inadequações:

Não foram observados óbices de ordem ética para a execução da proposta conforme apresentada. Projeto de pesquisa aprovado, pois em consonância com os ditames éticos e legais das Resoluções nºs 466/12 e 510/16, ambas do CNS.

Considerações Finais a critério do CEP:

Lembramos aos senhores pesquisadores que, no cumprimento da Resolução 466/12, o Comitê de Ética em Pesquisa (CEP) deverá receber relatórios semestrais sobre o andamento do estudo, bem como a qualquer tempo e a critério do pesquisador nos casos de relevância, além do envio dos relatos de eventos adversos, para conhecimento deste Comitê.

Salientamos ainda, a necessidade de relatório completo ao final do estudo. Eventuais modificações ou emendas ao protocolo devem ser apresentadas ao CEP-PUCPR de forma clara e sucinta, identificando a parte do protocolo a ser modificado e as suas justificativas.

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_2374422.pdf	25/10/2024 14:24:54		Aceito
Outros	perguntasformulariosubmeter3.docx	25/10/2024 14:23:42	MYKAELE FORTES SOUSA	Aceito
Outros	Cartaresposta.docx	25/10/2024 14:19:29	MYKAELE FORTES SOUSA	Aceito
Projeto Detalhado / Brochura Investigador	projetodetalhado3.docx	25/10/2024 14:19:17	MYKAELE FORTES SOUSA	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	TCLEPrivacidaderevisado3.docx	25/10/2024 14:18:59	MYKAELE FORTES SOUSA	Aceito
Outros	TermoDeConfidencialidadePrivacidade1.pdf	12/08/2024 15:52:24	MYKAELE FORTES SOUSA	Aceito
Outros	TCUD_Privacidade1.pdf	12/08/2024 15:49:47	MYKAELE FORTES SOUSA	Aceito
Folha de Rosto	ProjetoMykaela.pdf	05/07/2024 16:14:14	MYKAELE FORTES SOUSA	Aceito

Situação do Parecer:

Endereço: Rua Imaculada Conceição, n° 1155 - prédio administrativo, térreo
 Bairro: Prado Velho CEP: 80.215-901
 UF: PR Município: CURITIBA
 Telefone: (41)3271-2103 Fax: (41)3271-2103 E-mail: nep@pucpr.br

PONTIFÍCIA UNIVERSIDADE
CATÓLICA DO PARANÁ - PUC/
PR



Continuação do Parecer: 7.213.076

Aprovado

Necessita Apreciação da CONEP:

Não

CURITIBA, 07 de Novembro de 2024

Assinado por:
Rafaella Stradiotto Bernardelli
(Coordenador(a))

Endereço: Rua Imaculada Conceição, n° 1155 - prédio administrativo, térreo
Bairro: Prado Velho CEP: 80.215-901
UF: PR Município: CURITIBA
Telefone: (41)3271-2103 Fax: (41)3271-2103 E-mail: nep@puopr.br