Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Daiane Godoy Prudente

INFÂNCIA EM RISCO NA ERA DIGITAL:
Como a segurança da informação e a educação digital podem prevenir a pedofilia *online*

Americana, SP
2025

Daiane Godoy Prudente

INFÂNCIA EM RISCO NA ERA DIGITAL:
Como a segurança da informação e a educação digital podem prevenir a pedofilia *online*

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação na área de concentração em Segurança da Informação.

Orientadora: Prof.ª Drª. Maria Cristina Aranda

Este trabalho corresponde à versão final do Trabalho de Conclusão de Curso apresentado por Daiane Godoy Prudente e orientado pela Prof.ª Drª. Maria Cristina Aranda.

Americana, SP
2025

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS Dados Internacionais de Catalogação-na-fonte

PRUDENTE, Daiane Godoy

Infância em risco na era digital: como a segurança da informação e a educação digital podem prevenir a pedofilia online. / Daiane Godoy Prudente – Americana, 2025.

56f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientadora: Profa. Dra. Maria Cristina Aranda

1. Inclusão digital 2. Lei de tecnologia de informação 3. Risco. I. PRUDENTE, Daiane Godoy II. ARANDA, Maria Cristina III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681.3
34:381.3
330.7

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Daiane Godoy Prudente

Infância em risco na era digital: como a segurança da informação e a educação digital podem prevenir a pedofilia online

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.
Área de concentração: Segurança da Informação

Americana, 25 de junho de 2025.

Banca Examinadora:

Maria Cristina Aranda
Doutora
Fatec Americana "Ministro Ralph Biasi"

Diógenes de Oliveira
Mestre
Fatec Americana "Ministro Ralph Biasi"

Thais Godoy Vazquez Macetti
Doutora
Fatec Americana "Ministro Ralph Biasi"

DEDICATÓRIA

Dedico este trabalho a mim mesma, por não desistir, mesmo diante das dificuldades e por seguir acreditando nos meus sonhos. E ao meu filho Gui, minha maior inspiração e motivo de forças para seguir. Cada esforço valeu a pena, e tudo o que faço, faço por nós. Essa vitória é nossa. Mais uma vez, conseguimos!

AGRADECIMENTOS

Agradeço primeiramente a Deus, pela minha vida, saúde e por me conceder forças todos os dias para continuar trilhando este caminho, mesmo diante dos desafios.

Agradeço e parabenizo a mim mesma, por não desistir dos meus sonhos e por continuar lutando por uma vida melhor para mim e para meu filho. Este trabalho é fruto de perseverança e da certeza de que cada esforço vale a pena.

Ao meu esposo Valter (In Memoriam), minha eterna gratidão. Mesmo após sua partida, sua generosidade continua presente em nossas vidas, permitindo-me dedicar-me exclusivamente aos estudos e ao meu crescimento pessoal e profissional.

Ao Guilherme, meu filho amado, minha maior razão de viver. Obrigada por ser minha inspiração e por dar sentido à minha caminhada. Você me dá forças para seguir em frente, mesmo nas horas mais difíceis.

À minha mãe, agradeço por estar ao meu lado nos momentos em que mais precisei, oferecendo apoio e amor quando eram tão necessários.

Quero também expressar minha profunda gratidão a alguns professores que marcaram minha trajetória acadêmica com sua dedicação, carinho e competência.

Ao Prof. Rogério Freitas, por me ajudar a conquistar um estágio, essencial não apenas para a conclusão do curso, mas também para contribuir com minha vida financeira.

Às professoras Thaís Macetti, Maria Cristina Aranda e Luciene Garbuio, minha profunda admiração e agradecimento por serem mulheres inspiradoras, que, com suas trajetórias e ensinamentos, me motivaram — e ainda motivam — a continuar crescendo e superando desafios.

Ao professor Thiago, meu sincero agradecimento por tornar o aprendizado da língua inglesa mais leve e inspirador. Sua forma gentil e envolvente de ensinar despertou em mim um interesse ainda maior pela língua e me mostrou que aprender pode — e deve — ser algo prazeroso.

Ao professor Clerivaldo, que esteve presente em três semestres da minha caminhada, agradeço imensamente pela paciência, acolhimento e maneira cuidadosa de ensinar. Sua postura fez toda a diferença para que eu pudesse absorver os conteúdos com mais tranquilidade e confiança.

Ao professor Diógenes, que no último semestre me apresentou uma área da TI que até então eu desconhecia e que hoje enxergo como uma possível direção a seguir. Seu compromisso com o que ensina ampliou meu olhar e despertou novas possibilidades em minha trajetória.

A cada um de vocês, meu muito obrigada por terem sido mais do que professores — foram guias generosos nesse percurso de aprendizado.

Aos amigos de sala de aula, Edmar e Victor, deixo meu carinho e gratidão. Edmar, obrigada pela paciência em me ajudar nas matérias mais desafiadoras e por compartilhar tantos conhecimentos comigo. Victor, obrigada pelas risadas e pela parceria no dia a dia, que tornaram essa jornada mais leve e especial.

A todos estes, minha eterna gratidão. Este trabalho carrega um pedaço de cada um de vocês.

RESUMO

Este trabalho aborda a problemática da pedofilia no ambiente virtual e a importância da educação digital e da segurança da informação na prevenção desse crime. A pesquisa destaca como a Internet, apesar de suas inúmeras oportunidades, também apresenta riscos para crianças e adolescentes, que são expostos à pedofilia virtual. O estudo busca responder à questão de como a educação digital, aliada aos princípios de segurança da informação, pode contribuir para a proteção dos jovens nesse ambiente, considerando os desafios da confidencialidade, integridade e disponibilidade dos dados. A relevância do tema é ressaltada pela legislação brasileira, que caracteriza a pedofilia virtual como crime. O objetivo geral do trabalho é investigar o uso da educação digital e das práticas de segurança da informação como ferramentas de prevenção à pedofilia *online*. Os objetivos específicos incluem a análise das características e dinâmicas da pedofilia nos ambientes *online*, as diferenças entre os ambientes *online* e sua facilitação de práticas ilícitas, as consequências legais e sociais da pedofilia virtual, a proposição de estratégias de prevenção e combate, e a sensibilização da sociedade para a importância da segurança na navegação. A metodologia adotada é qualitativa e exploratória, com foco na revisão bibliográfica de artigos científicos, livros, legislações, relatórios e estudos de caso. A pesquisa identifica as dinâmicas do crime, as plataformas utilizadas e as estratégias de prevenção e combate. O referencial teórico aborda a definição e as características da pedofilia, seus aspectos psicológicos e criminais, e a importância da compreensão desse tema para a criação de estratégias de prevenção e combate. O estudo também explora o perfil do pedófilo, os tipos de perfis (abusadores e molestadores) e os ambientes *online* (Internet*, deep web e dark web*) e suas particularidades. A pesquisa ressalta a complexidade da pedofilia no ambiente virtual e a necessidade de uma abordagem multifacetada que envolva a sociedade, famílias, instituições de ensino, governos e órgãos de segurança. A aplicação prática do estudo reforça essa visão, destacando a relevância complementar de soluções tecnológicas como o Qustodio e o Projeto Arachnid. O Qustodio age na proteção doméstica, capacitando pais a gerenciar o uso digital e filtrar conteúdos, criando uma camada de defesa direta para as crianças. Em contraste, o Projeto Arachnid atua na escala global, dedicando-se à identificação e remoção proativa de material de abuso sexual infantil (CSAM) da Internet. Essa abordagem dupla é fundamental, pois combina a defesa individual e familiar com o combate sistêmico ao conteúdo ilícito, garantindo uma proteção mais robusta e eficaz para a criança e a sociedade.

Palavras Chave: Pedofilia *online*; Educação digital; Segurança da Informação.

ABSTRACT

This study addresses the issue of online pedophilia and emphasizes the role of digital education and information security in preventing such crimes. While the Internet provides numerous opportunities, it also poses significant risks to children and adolescents, who are increasingly exposed to virtual abuse. The research aims to understand how digital education, combined with the principles of information security—confidentiality, integrity, and availability—can contribute to the protection of young users in the digital space. The relevance of this topic is underscored by Brazilian legislation, which classifies online pedophilia as a criminal offense. The main objective of this study is to investigate how digital education and information security practices can be used as effective tools to prevent online child exploitation. Specific objectives include analyzing the dynamics and characteristics of pedophilia on virtual environments, understanding how these environments facilitate illicit activities, identifying the legal and social consequences, proposing prevention and response strategies, and raising public awareness on safe Internet practices. A qualitative and exploratory methodology was adopted, based on bibliographic research involving scientific articles, books, legislation, reports, and case studies. The findings highlight the operational dynamics of the crime, the platforms most commonly used by offenders, and the tools available for detection and prevention. The theoretical framework explores the definition and psychological and criminal aspects of pedophilia, offering critical insight into the development of countermeasures.
Furthermore, the study examines offender profiles, differentiating between abusers and molesters, and investigates the use of the Internet, deep web, and dark web in the commission of these crimes. The research concludes by emphasizing the complexity of online pedophilia and the urgent need for a multidisciplinary approach involving society, families, educational institutions, governments, and law enforcement agencies. The practical application of the study reinforces this perspective, highlighting the complementary relevance of technological solutions such as Qustodio and the Arachnid Project. Qustodio operates in the realm of domestic protection, empowering parents to manage digital usage and filter content, creating a direct layer of defense for children. In contrast, the Arachnid Project works on a global scale, focusing on the proactive identification and removal of child sexual abuse material (CSAM) from the Internet. This dual approach is essential, as it combines individual and family-level protection with a systemic fight against illicit content, ensuring more robust and effective safeguarding for both children and society.

Keywords: *Online Pedophilia; Digital Education; Information Security.*

SUMÁRIO

1 INTRODUÇÃO 11

2 REFERENCIAL TEÓRICO 13
2.1 Pedofilia no contexto da segurança digital 13
2.1.1 O perfil do pedófilo 16
2.1.2 Tipos de perfis: abusadores versus molestadores 18
2.2 Ambientes *online*: *Internet, deep web* e *dark web* 20
2.3 Dinâmica da pedofilia nos ambientes *online* 23
2.3.1 *Grooming* e manipulação virtual 24
2.3.2 Compartilhamento de material abusivo infantil 25
2.3.3 Símbolos da pedofilia 27
2.4 Consequências legais e sociais 29
2.5 Prevenção e combate 31
2.6 Segurança da informação como aliada na prevenção e combate à pedofilia *online* 33
2.7 Controle parental 35
2.7.1 Ferramentas de controle parental 36

3 APLICAÇÃO PRÁTICA 41
3.1 Qustodio 42
3.1.1 Segurança da informação no Qustodio 44
3.2 Project Arachnid 46

4 CONSIDERAÇÕES FINAIS 50

REFERÊNCIAS 52

1 INTRODUÇÃO

A expansão da Internet e o crescente uso de dispositivos digitais transformaram as interações sociais e o acesso à informação. Embora proporcionem inúmeras oportunidades de aprendizado e socialização, esse ambiente digital também expõe crianças e adolescentes a sérios riscos, especialmente no que concerne à pedofilia virtual. Esse crime se aproveita do anonimato e da facilidade de acesso oferecidos pelos ambientes *online*, incluindo a *web* visível e as camadas mais obscuras como a *deep web* e a *dark web*, para explorar a vulnerabilidade infantil, dificultando a identificação e o combate a essas práticas ilícitas.

Diante desse cenário, este estudo busca responder à seguinte questão: Como a educação digital, aliada a princípios de segurança da informação, pode contribuir para prevenir a pedofilia e proteger crianças e adolescentes no ambiente virtual, considerando os desafios da confidencialidade, integridade e disponibilidade dos dados?

A relevância deste tema é inegável e encontra respaldo na legislação brasileira. A pedofilia virtual é tipificada como crime, conforme a Lei nº 11.829, de 25 de novembro de 2008, que alterou o Estatuto da Criança e do Adolescente (Lei nº 8.069, de 13 de julho de 1990). Essa legislação aprimora o combate à produção, venda e distribuição de pornografia infantil, além de criminalizar a posse e o compartilhamento de materiais relacionados à pedofilia na Internet.

O objetivo geral deste trabalho, é investigar como a educação digital, integrada a práticas de segurança da informação, pode ser utilizada como ferramenta para prevenir a pedofilia e proteger crianças e adolescentes no ambiente virtual, destacando estratégias práticas, políticas públicas relevantes e a importância da proteção de dados.

Para alcançar o objetivo geral, definem-se objetivos específicos como compreender as características e a dinâmica da pedofilia nos ambientes *online*, analisar as diferenças entre os diversos ambientes *online* e como eles facilitam práticas ilícitas, discutir as consequências legais e sociais associadas à pedofilia virtual, propor estratégias de prevenção e combate ao crime, com enfoque na educação digital e sensibilizar a sociedade sobre a importância de práticas seguras de navegação para crianças e adolescentes.

Em termos de método científico, este estudo adota uma abordagem qualitativa e exploratória, com foco na revisão bibliográfica. A coleta de dados se baseou em artigos científicos, livros, legislações, relatórios de organizações e estudos de caso relacionados à pedofilia virtual. Essa metodologia permitiu identificar as dinâmicas do crime, as plataformas mais utilizadas e as estratégias existentes para prevenção e combate. As informações coletadas foram organizadas em categorias, analisadas criticamente e contextualizadas para fundamentar as propostas apresentadas.

A partir da exploração dos conhecimentos teóricos adquiridos, foi proposta uma análise crítica de ferramentas e iniciativas para resolução de um problema simulado do mundo real, contribuindo assim para a comodidade em geral quanto ao controle digital parental e a segurança *online* infantil.

Diante do cenário exposto, torna-se evidente que o combate à pedofilia virtual demanda uma abordagem múltipla, que integre medidas legais, tecnológicas e principalmente educacionais. Nos capítulos subsequentes, serão exploradas as dinâmicas desse crime, os principais ambientes digitais explorados pelos aliciadores, bem como estratégias preventivas e educativas que podem ser implementadas por famílias, instituições de ensino e governos. Espera-se com isso, estimular reflexões e ações que promovam uma navegação mais segura e consciente, fortalecendo uma cultura de proteção à infância no ambiente digital.

2 REFERENCIAL TEÓRICO

A proteção de crianças e adolescentes no ambiente digital exige uma abordagem que combine orientação e supervisão de um adulto. Diversos estudos ressaltam que a combinação entre a orientação familiar, por meio da educação digital, e o monitoramento ativo, através do uso de ferramentas de controle parental, constitui uma estratégia eficaz nesse sentido. A mediação ativa dos pais — que envolve diálogo, supervisão e uso conjunto das tecnologias — associada ao estabelecimento de regras claras e ao uso de *softwares* de controle, contribui significativamente para a redução da exposição a conteúdos inapropriados e para o desenvolvimento de uma compreensão crítica sobre os riscos e benefícios da Internet. Essa abordagem integrada fortalece o vínculo entre pais e filhos e promove um uso mais seguro e responsável das tecnologias digitais.

2.1 A PEDOFILIA NO CONTEXTO DA SEGURANÇA DIGITAL

A pedofilia configura-se como um dos temas mais sensíveis e alarmantes da sociedade contemporânea, ganhando contornos ainda mais complexos no ambiente digital, onde a ampla conectividade potencializa os riscos. Este segmento do estudo se dedica à análise da definição e das características multifacetadas da pedofilia, explorando seus aspectos psicológicos e criminais profundamente ligados à cultura digital. A compreensão detalhada dessa questão em suas diversas dimensões é fundamental para a formulação de estratégias focadas em segurança da informação que sejam eficazes na prevenção e combate.

A gravidade da pedofilia no mundo atual é frequentemente estampada em notícias de casos relacionados. A percepção pública se volta para a presença de conteúdos com características questionáveis em programas infantis e, de maneira intensa, para a Internet como um espaço onde indivíduos com atração por crianças encontram um terreno fértil para a disseminação de pornografia infantil, troca de informações e aliciamento de vítimas. Conforme a observação de Piscitelli (2004), a rede é vista por muitos como "um paraíso dos pedófilos, uma terra sem lei".

O Manual Diagnóstico e Estatístico de Transtornos Mentais (DSM-5) apresenta diversas definições para a pedofilia. Na perspectiva psiquiátrica, ela é compreendida

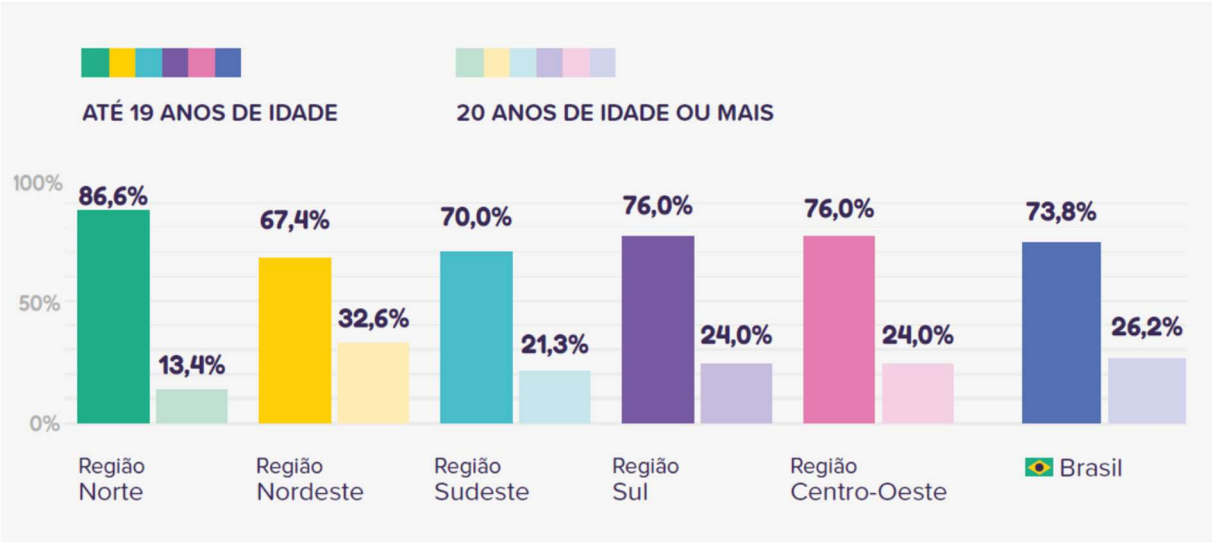
como um transtorno de personalidade, caracterizado pelo desenvolvimento de fantasias ou comportamentos sexuais intensos envolvendo crianças com idade inferior a 14 anos.

A Classificação Internacional de Doenças (CID), descreve a pedofilia como um distúrbio psicológico, um desvio sexual e uma condição patológica. É inserida como modalidade dos Transtornos de preferência sexual, sob o código F654. De acordo com a CID, ela se refere à "preferência sexual por crianças, quer sejam meninos, meninas ou ambos, geralmente pré-púberes". Trata-se da atração sexual de adultos com mais de 16 anos por crianças na fase pré-puberal ou no início da puberdade. A mera existência desse desejo sexual por crianças nessa faixa etária já configura a pedofilia, independentemente da ocorrência de qualquer contato sexual.

No Brasil, a problemática da pedofilia ganhou maior destaque somente a partir da década de 1990, conforme observado por Piscitelli (2004). Anteriormente, o tema era abordado de maneira superficial pela mídia, com poucas reportagens sobre abuso sexual infantil. Contudo, com a expansão da Internet, a discussão sobre o tema se intensificou.

Os números apresentados na Figura 1, retratam a violência sexual infantil no Brasil registradas em 2022.

Figura 1: Proporção de notificações de violência e exploração sexuais segundo grupo etário



Fonte: Fundação Abrinq – Disponível em https://www.fadc.org.br/noticias/cenario-violencia-sexual. Acesso em 11/06/2025

Outro ponto relevante é o conceito de idade de consentimento sexual, que apresenta variações significativas entre países e legislações. Na Holanda, por exemplo, a idade mínima é de 12 anos, enquanto nos Estados Unidos varia conforme o estado, sendo 13 anos em alguns deles. No Brasil, atos sexuais com menores de 14 anos são categoricamente considerados abuso, mesmo que haja alegação de consentimento, em conformidade com o artigo 217-A do Código Penal (Brasil, 2009).

A relevância do tema está respaldada pela legislação brasileira. De acordo com o Decreto do Congresso Nacional (Brasil, 2008), a pedofilia virtual é considerada crime, regida pela Lei nº 11.829, de 25 de novembro de 2008, que revogou a Lei nº 8.069, de 13 de julho de 1990 – Estatuto da Criança e do Adolescente. Essa lei aprimora o combate à produção, venda e distribuição de pornografia infantil, bem como criminaliza a posse e o compartilhamento de materiais relacionados à pedofilia na Internet.

Apesar dos esforços contínuos no combate à pedofilia, existem movimentos organizados que defendem a redução da idade mínima para o consentimento sexual, argumentando que relações sexuais consensuais deveriam ser permitidas independentemente da idade da criança.

Embora a Internet seja inegavelmente utilizada como um meio para a prática de atos pedófilos, é fundamental reconhecer que ela não pode ser responsabilizada isoladamente. Como bem pontua Sanderson (2005, p. 105), "a tecnologia não abusa das crianças; as pessoas sim". Essa afirmação sublinha a necessidade de abordar a questão de forma abrangente, direcionando o foco para o agressor que promove e mantém essas práticas criminosas.

No campo da saúde mental, a pedofilia é reconhecida como um transtorno parafílico, caracterizado pela atração sexual recorrente e intensa por crianças pré-púberes. O manual diagnóstico e estatístico de transtornos mentais (DSM-5) classifica essa condição como um distúrbio quando causa sofrimento significativo ao indivíduo ou quando resulta em atos sexuais com menores. No entanto, no âmbito jurídico brasileiro, o termo pedofilia está diretamente associado a atos criminosos, especialmente aqueles previstos no Estatuto da Criança e do Adolescente (ECA), como a produção, posse e distribuição de pornografia infantil (Brasil, 1990; Ribeiro, 2021). A Internet, nesse contexto, emergiu como um meio facilitador para a proliferação desses crimes, demandando o desenvolvimento de novas abordagens legais e investigativas para o seu efetivo combate.

2.1.1 O PERFIL DO PEDÓFILO

O pedófilo, em geral, apresenta um perfil psicossocial que pode envolver isolamento social, dificuldades nos relacionamentos interpessoais — especialmente com adultos — e comportamentos manipuladores. Conforme observa Ribeiro (2021), muitos atuam de forma premeditada, estabelecendo vínculos afetivos falsos com suas vítimas, utilizando a confiança como principal mecanismo de aproximação. É comum que esses indivíduos sejam bem inseridos em seu meio social, considerados cidadãos exemplares, o que dificulta sua identificação e responsabilização.

O indivíduo que comete esse tipo de crime, caracterizado por um transtorno de conduta sexual no qual um adulto manifesta desejos intensos por crianças ou pré-adolescentes, é denominado pedófilo. Trata-se de uma condição de altíssimo risco social. Estudos clínicos apontam que a pedofilia afeta predominantemente homens — cerca de 99% dos casos — com faixa etária média entre 30 e 45 anos (Sanderson, 2005; Serafim, 2009). Psicologicamente, esses indivíduos tendem a ser introvertidos, reservados, emocionalmente inseguros e, em muitos casos, apresentam histórico de abuso sexual na infância. Tal vivência pode influenciar significativamente sua trajetória psíquica e comportamental.

Além disso, os pedófilos enfrentam sérias dificuldades em estabelecer vínculos afetivos e sexuais duradouros com adultos. Quando estão em relacionamentos estáveis, é comum que estejam insatisfeitos com a vida sexual e apresentem distúrbios emocionais que afetam diretamente a relação conjugal. Há relatos de esposas que têm conhecimento das inclinações dos parceiros, mas preferem silenciar, temendo o julgamento social (Machado, 2013). A dissimulação do comportamento, aliada ao receio de denúncia, contribui para a perpetuação do ciclo de abuso.

Com o tempo, esses indivíduos podem desenvolver tolerância à pornografia convencional, migrando para o consumo de pornografia infantil em busca de maior excitação. O conceito clínico da pedofilia indica que o indivíduo só sente prazer sexual pleno ao se envolver, direta ou indiretamente, com crianças. Mesmo mantendo relações com adultos, seu objeto de desejo permanece centrado na infância. Esse comportamento é representado de forma sensível e crítica no filme O Lenhador (2004), dirigido por Nicole Kassell, que retrata os dilemas de um pedófilo em processo de reinserção social.

Segundo dados de estudos forenses, a diferença de idade média entre o molestador e sua vítima é geralmente de 15 anos, revelando uma assimetria de poder que favorece o domínio e o controle sobre a criança (Serafim, 2009). Nesse cenário, o pedófilo experimenta sensação de superioridade, uma vez que detém total controle sobre a vítima, em contraste com sua fragilidade emocional em relações com adultos.

Quando confrontados com a Justiça, muitos pedófilos alegam que não cometeram crime, uma vez que não utilizaram violência física. Alguns chegam a culpar a própria vítima, alegando que comportamentos infantis foram mal interpretados como sedução. Trata-se de uma estratégia de manipulação que reflete a dissociação da realidade e a negação da responsabilidade, características frequentemente associadas a transtornos de personalidade (APA, 2013).

Matos (2013) enfatiza que no ambiente virtual, muitos encontram terreno fértil para projetar suas fantasias, por meio de consumo de material abusivo, conversas *online*, jogos e simulações que, embora não envolvam contato físico direto, representam formas concretas de violência sexual. O anonimato da Internet permite que o pedófilo teste seus limites, legitime seus desejos e, em muitos casos, evolua para condutas presenciais de abuso.

Diante da complexidade, a análise do perfil do pedófilo deve considerar não apenas os aspectos clínicos e legais, mas também os impactos sociais, psicológicos e tecnológicos envolvidos em sua atuação.

É fundamental desmistificar a imagem estereotipada do pedófilo como um indivíduo marginalizado e de aparência suspeita. Abusadores podem ser pessoas aparentemente comuns, como vizinhos, familiares, professores ou líderes religiosos, o que aumenta a dificuldade de detecção e a vulnerabilidade das vítimas. Segundo o Ministério Público do Distrito Federal e Territórios (MPDFT, 2025), o pedófilo é, na maioria das vezes, alguém que aparenta normalidade em seu convívio social e ambiente profissional. Torna-se criminoso ao explorar sexualmente o corpo de uma criança, com ou sem o uso de violência física. Ato inaceitável, independentemente de qualquer aparente consentimento.

Além disso, um relatório da Câmara dos Deputados destaca que o pedófilo é um agente com tipologias física e comportamental desconhecidas. Ele é um criminoso sem ser enquadrado em um núcleo de crime predefinido com tal nome, afinal, o que comumente se entende como delito pedofílico é o estupro de vulnerável.

A pedofilia transcende barreiras socioeconômicas, culturais e de gênero, podendo ocorrer em qualquer contexto social e familiar.

Embora menos conhecida e representando um número menor de casos em comparação à masculina, a pedofilia feminina existe e precisa ser reconhecida e enfrentada com a mesma seriedade. Segundo Bandeira (2022), cerca de 10% dos casos de pedofilia investigados no Brasil envolvem mulheres, número que pode ser ainda maior devido à subnotificação. Essa estimativa destaca os tabus sociais e psicológicos que dificultam o reconhecimento e a denúncia desse tipo de abuso quando cometido por mulheres. Falar sobre pedofilia feminina ainda é um tabu, mas o silêncio contribui para a impunidade e a revitimização das crianças.

Essas informações reforçam a necessidade de uma abordagem preventiva no reconhecimento do abuso sem distinção de gênero dos agressores, que inclua a educação digital e o uso de ferramentas de controle parental, uma vez que o perigo pode estar presente em ambientes considerados seguros. É preciso capacitar a sociedade para reconhecer os sinais de alerta e proteger as crianças de forma eficaz.

2.1.2 TIPOS DE PERFIS: ABUSADORES VERSUS MOLESTADORES

A literatura jurídica, criminológica e psicológica distingue abusadores de molestadores com base nas motivações, abordagens e intensidade de seus atos criminosos. Embora ambos estejam ligados à exploração sexual infantil, suas características comportamentais e modos de ação apresentam diferenças substanciais.

Segundo Teixeira (2022), o abusador é aquele que utiliza violência física ou psicológica para submeter a vítima, impondo sua vontade de forma direta e, muitas vezes, traumática. O autor alega ainda que o molestador geralmente atua por meio da sedução, manipulação emocional e ganho de confiança, características que tornam sua atuação menos visível e, consequentemente, mais difícil de ser detectada, sobretudo em ambientes virtuais. Ambos, entretanto, são infratores e causam graves danos psíquicos e emocionais às vítimas, independentemente do método utilizado.

A transição da fantasia para a prática delituosa, no caso do pedófilo, pode ser desencadeada por fatores estressores como crises conjugais, perdas familiares ou frustrações emocionais profundas. Nesse contexto, os pedófilos podem se manifestar

em dois perfis comportamentais predominantes: como abusadores ou como molestadores.

Segundo Serafim (2009), o pedófilo abusador costuma ser um indivíduo emocionalmente imaturo, com dificuldades em estabelecer vínculos afetivos com adultos e que, em determinado momento, descobre na criança um meio de obtenção de prazer sexual. Seu comportamento tende a ser discreto e progressivo, iniciando-se com carícias sutis que passam despercebidas pelos adultos ao redor. Esse perfil é muitas vezes solitário, socialmente retraído e tende a consumir pornografia infantil como meio de satisfazer suas fantasias sexuais. A partir do exposto, nota-se que o uso da Internet facilita o acesso a esse tipo de material, ampliando o risco de perpetuação das condutas abusivas.

Já o pedófilo molestador apresenta um comportamento mais invasivo e explícito, com episódios de agressão que podem incluir desde atos sexuais forçados até crimes letais. Dentro desse grupo, Serafim (2009) os classifica entre molestadores situacionais e molestadores preferenciais.

O autor alega que o molestador situacional não possui preferência sexual exclusiva por crianças. Seu comportamento transgressor surge a partir de contextos específicos, como estresse, frustrações ou dificuldades emocionais. Em geral, trata-se de um homem casado, com vida familiar estável, que comete o abuso de forma impulsiva. Esse tipo de molestador escolhe vítimas com base em oportunidade e vulnerabilidade, sendo que os ataques são mais frequentes contra meninas. Quando ocorrem contra meninos, levanta-se a hipótese de uma orientação homossexual latente. Molestadores situacionais, em sua maioria, pertencem a classes socioeconômicas mais baixas e têm menor nível de escolaridade. Agem por impulso e buscam, além da satisfação sexual, a compensação de carências afetivas ou o exercício de poder sobre a vítima (Serafim, 2009).

Por outro lado, Serafim (2009) destaca que o molestador preferencial possui orientação sexual voltada exclusivamente para crianças. Seu comportamento é premeditado, compulsivo e recorrente. São, em geral, indivíduos mais articulados, inteligentes e pertencentes a classes sociais mais elevadas. Costumam planejar meticulosamente suas ações, observando hábitos e rotinas das vítimas, e agindo com base em fantasias específicas. Seu grau de periculosidade é elevado, pois podem cometer agressões mais graves, mutilações e até homicídios, caso se sintam

ameaçados ou busquem ampliar o prazer pela dominação total, fato este confirmado por Machado (2013).

Portanto, a diferenciação entre abusadores e molestadores é crucial para o entendimento do ciclo do abuso sexual infantil. Essa classificação permite ações mais eficazes de prevenção, diagnóstico, investigação criminal e suporte psicológico às vítimas.

2.2 AMBIENTES *ONLINE*: INTERNET, *DEEP WEB* E *DARK WEB*

A Internet pode ser compreendida em três camadas principais: a *surface web*, a *deep web* e a *dark web*. É frequentemente comparada a um iceberg, como pode ser visto na Figura 2, sendo:

A *surface web* que corresponde à parte visível da Internet. Essa parte da rede é frequentemente comparada à ponta do *iceberg*, pois corresponde a uma pequena fração do conteúdo total disponível *online*. Ela é indexada por mecanismos de busca como Google, Bing, Yahoo entre outros. É nessa camada que ocorrem interações em redes sociais, *fóruns* abertos, *sites* de notícias e *blogs*. Apesar de sua aparente superficialidade, nela também são praticados crimes, inclusive os relacionados ao abuso e à exploração sexual infantil (Moreira, 2019).

Um exemplo de crime praticado nessa camada está na plataforma Discord, originalmente criado para comunidades de jogos *online*, mas que hoje abriga uma ampla variedade de grupos com diferentes finalidades. Embora seja uma ferramenta legítima de interação, sua estrutura técnica é baseada em canais de texto e voz, com comunicação instantânea por *Web*Socket e favorece uma comunicação direta e contínua entre usuários, o que pode ser explorado por criminosos (Fernandes, 2023).

O Discord, por permitir a criação de servidores privados e canais fechados, facilita a ação de aliciadores, abusadores e grupos que promovem discurso de ódio e violência. Segundo Carvalho (2023), há evidências de que a plataforma tem sido utilizada por pedófilos para compartilhar conteúdo ilegal, fazer contato com menores de idade e manipular emocionalmente suas vítimas, tudo isso com pouca ou nenhuma moderação em tempo real.

A gravidade da situação também é destacada por Scofield (2023), que investigou dezenas de servidores com conteúdo extremistas, incluindo incitação ao

ódio, apologia à violência sexual e aliciamento. A reportagem feita, mostra que mesmo quando denúncias são feitas, as respostas da plataforma são lentas ou ineficazes, permitindo que comunidades perigosas continuem ativas e exponham usuários vulneráveis a riscos extremos.

Além disso, conforme aponta Fernandes (2023), muitas dessas comunidades utilizam uma linguagem que mistura ironia, piadas e violência simbólica, dificultando a percepção imediata do risco por parte de jovens. Essa "normalização do absurdo" cria um ambiente permissivo, no qual o abuso pode ocorrer de forma disfarçada ou velada, tornando a educação digital uma ferramenta essencial para prevenir esse tipo de ameaça.

Diante desse cenário, torna-se evidente que a proteção da infância no ambiente digital não pode depender apenas das plataformas. É necessário integrar estratégias de educação digital crítica, com foco em orientar crianças, adolescentes e seus responsáveis sobre os riscos e formas de defesa no ciberespaço, aliadas ao fortalecimento das políticas de segurança da informação e à responsabilização das empresas de tecnologia quanto à moderação de seus serviços.

A *deep web*, por sua vez, corresponde a um conjunto de conteúdos que não são indexados pelos buscadores comuns. Isso inclui arquivos protegidos por senha, bancos de dados acadêmicos, informações sigilosas de instituições e conteúdo técnico. Embora não seja ilegal em sua totalidade, a ausência de indexação e de filtros permite que a *deep web* abrigue atividades que se camuflam da supervisão pública (NIC.br, 2022). É representada pela massa principal do *iceberg* submersa logo abaixo da linha d'água.

Antigamente, o termo era usado para designar tudo o que não estava disponível na *surface web* e embora essa camada contenha informações valiosas e legais, ela também pode ser utilizada para fins ilícitos.

Já a *dark web* é a camada mais profunda e oculta da Internet, acessada apenas por meio de *softwares* específicos. Essa camada é representada pela parte mais profunda e escura do iceberg.

Existem diversos navegadores para acessos, os mais conhecidos são: Tor (The Onion Routing) e I2P (Invisible Internet Project) que garantem o anonimato e dificultam o rastreamento de usuários. Nessas camadas, a ausência de regulamentação e o alto nível de anonimato favorecem a realização de atividades ilegais como tráfico de drogas, venda de armas, contratação de *hackers,* comércio de dados roubados, além

de crimes mais graves, como pornografia infantil, tráfico de órgãos e comércio de pessoas (Moreira, 2019; NIC.br, 2022). A estrutura descentralizada e a criptografia utilizadas na *dark web* desafiam diretamente os princípios fundamentais da segurança da informação, como a confidencialidade, integridade e rastreabilidade segundo Castro (2020) e NIC.br (2022).

A proteção do anonimato dificulta a identificação dos usuários e o rastreamento das ações realizadas, o que torna esse ambiente especialmente perigoso.

Um dos crimes mais repugnantes presentes na *dark web* é a pornografia infantil que explora a inocência de crianças e fere seus direitos fundamentais. Infelizmente, esse conteúdo é disseminado por indivíduos que se aproveitam do sigilo e da ausência de fiscalização nessas camadas ocultas da Internet. Tanto a *deep web* quanto a *dark web* são utilizadas para armazenar, compartilhar e consumir esse tipo de material, o que reforça a importância de estratégias eficazes de monitoramento e combate a crimes cibernéticos.

Segundo Peck (2021), é essencial que a Internet seja tratada com o mesmo zelo e vigilância destinados aos espaços físicos, pois os riscos digitais se manifestam com consequências reais. A autora reforça a importância do envolvimento das famílias e da sociedade como agentes ativos na proteção dos menores em ambientes digitais.

Com o avanço exponencial da tecnologia e da conectividade global, surgem também novas vulnerabilidades. A facilidade de comunicação, o anonimato e a rapidez na disseminação de informações têm sido fatores que facilitam a proliferação dos chamados crimes cibernéticos. Entre eles, destaca-se a pornografia infantil, tipificada no Estatuto da Criança e do Adolescente (Lei nº 8.069/1990), especialmente a partir do artigo 240 (Brasil, 1990).

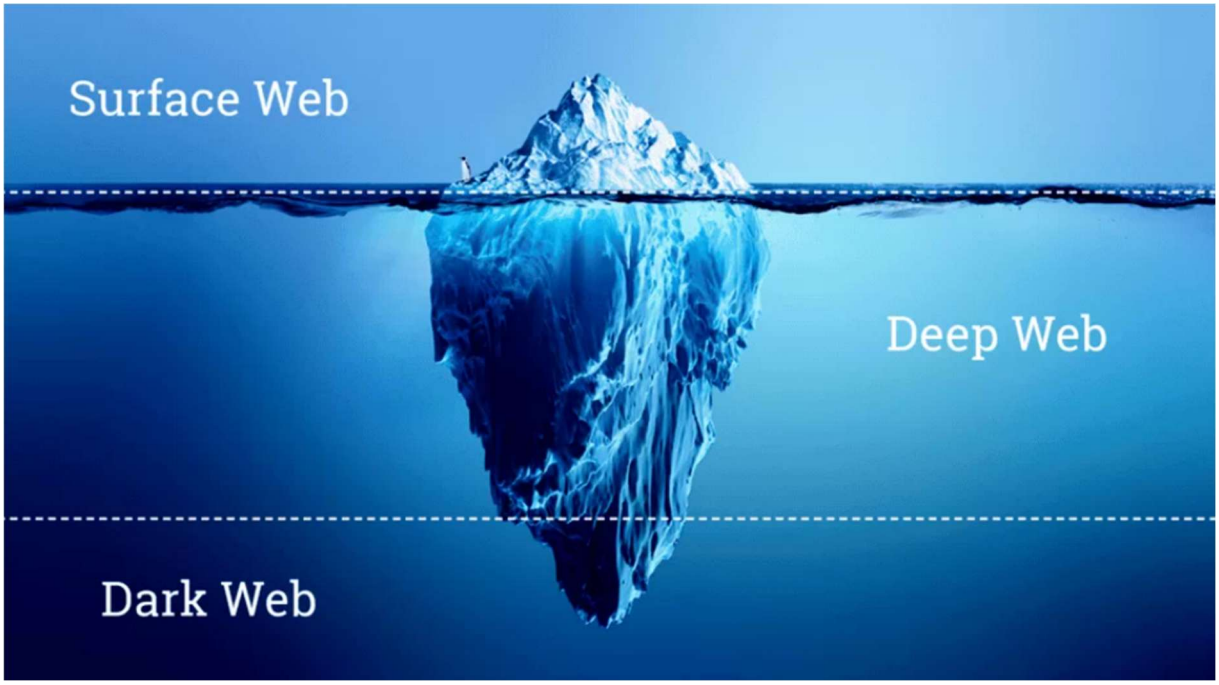
Esses crimes virtuais – também denominados como cibercrimes, delitos digitais ou informáticos – abrangem ações realizadas por meio de dispositivos eletrônicos, e a maioria deles encontra na Internet um ambiente propício para sua perpetuação (Machado, 2013; Campelo; Pires, 2024). Como pontua o relatório da Europol (2021), a rede tem sido instrumentalizada por redes organizadas de criminosos para disseminar material de abuso sexual infantil, principalmente em plataformas de difícil monitoramento.

A utilização de ferramentas tecnológicas para ocultação de identidade, como VPNs, criptografia ponta a ponta e *softwares* de navegação anônima, torna ainda mais desafiador o rastreamento e a responsabilização de criminosos. A Internet Watch

Foundation (2021) aponta um crescimento anual significativo na hospedagem de imagens e vídeos de exploração sexual infantil, reforçando a urgência de ações articuladas para o enfrentamento do problema.

Nesse contexto, torna-se fundamental compreender a arquitetura da rede e as implicações de suas camadas ocultas. A promoção de políticas públicas, o fortalecimento das ações educativas e a atuação integrada entre os órgãos de segurança, família, sociedade civil e setor privado são pilares indispensáveis para a proteção de crianças e adolescentes contra crimes praticados no ambiente virtual.

Figura 2: Representação dos níveis de profundidade: *Surface*, *Deep* e *Dark Web*



Fonte: A3A Engenharia de Sistemas – Disponível em: https://a3aengenharia.com.br/conteudo/artigos-tecnicos/world-wide-*web*/. Acesso em 11/06/2025.

2.3 DINÂMICA DA PEDOFILIA NOS AMBIENTES *ONLINE*

A facilidade de acesso, o anonimato e a ausência de fronteiras tornam a Internet um canal eficaz para a prática de crimes sexuais contra menores. Conforme dados da ONG SaferNet Brasil (2023), que atua na prevenção e combate a crimes virtuais, especialmente contra crianças e adolescentes, e promove a conscientização sobre segurança *online*, o compartilhamento de imagens, transmissões ao vivo de abuso e aliciamento em jogos *online* têm aumentado. Pedófilos utilizam fóruns, redes P2P,

redes sociais e até plataformas populares de vídeo para distribuir e consumir conteúdo abusivo.

Com a ampliação do uso da Internet e a proliferação de plataformas digitais, o ambiente *online* tornou-se um território fértil para a prática de crimes relacionados à pedofilia. A conectividade global, combinada com o anonimato proporcionado por tecnologias avançadas, permite que predadores explorem vulnerabilidades de crianças e adolescentes de forma cada vez mais sofisticada. Este tópico explora como a pedofilia se manifesta no espaço virtual, detalhando estratégias utilizadas por criminosos, as ferramentas empregadas e os desafios enfrentados na prevenção e combate a essas práticas.

2.3.1 *GROOMING* E MANIPULAÇÃO VIRTUAL

O *grooming* é uma prática na qual o agressor se aproxima da vítima com falsas intenções de amizade, buscando obter confiança para posteriormente abusar ou extorquir sexualmente. Esse processo é facilitado pela ingenuidade e vulnerabilidade emocional das crianças e adolescentes. Segundo Teixeira (2022), o *grooming* pode ocorrer ao longo de semanas ou meses e muitas vezes não é identificado imediatamente por familiares ou professores. O uso de aplicativos de mensagens e redes sociais amplia a capacidade de atuação dos criminosos. Peck (2021) reforça que os pais devem se envolver ativamente na vida digital dos filhos, sabendo com quem interagem e o que consomem *online*, já que a Internet é parte do ambiente social contemporâneo.

O *grooming*, ou aliciamento infantil *online*, é uma prática comum na dinâmica da pedofilia nos ambientes virtuais. Esse processo envolve a criação de um relacionamento de confiança entre o predador e a criança, com o objetivo de explorar sexualmente a vítima.

Segundo Ellovitch (2023), o *grooming* é um crime ilusório que se desenvolve por etapas — desde a criação de perfis falsos até a manipulação emocional, sexualização e exigência de material íntimo ou atos sexuais. Esses predadores atuam de forma calculada e gradual, muitas vezes sem que a vítima perceba, utilizando plataformas digitais como meio principal.

O contato inicial geralmente ocorre com perfis falsos, com a criação de contas em redes sociais e jogos *online*, muitas vezes com avatares e identidades falsas, simulando idades semelhantes às das vítimas. O pedófilo busca temas em comum — música, *hobbies*, problemas familiares — para iniciar uma conexão.

O criminoso investe em conversas frequentes afim de construir confiança emocional, trocando afeto, elogios e atenção personalizada, explorando a vulnerabilidade ou insatisfação da criança ou adolescente. Essa relação pode levar ao isolamento da vítima de familiares ou amigos.

Uma vez estabelecida a confiança, é feita uma introdução gradual de conteúdo sexual, iniciando sutis abordagens de temas sexuais, envio de pornografia para normalizar discursos e práticas, e questionamentos sobre a vida íntima da vítima, sempre manipulando para criar confusão emocional.

Ainda de forma sutil ou de forma manipulada, o pedófilo começa a exigir fotos ou vídeos de nudez, armazenando ou compartilhando com redes de outros agressores. Posteriormente, pode induzir ao autoerotismo, atos sexuais ou pornografia em vídeo, muitas vezes realizados sem que a vítima compreenda completamente o abuso.

Estudos mostram que redes sociais e aplicativos de mensagens, como WhatsApp, TikTok e Discord, são amplamente usados para *grooming*, devido à facilidade de comunicação e à falsa sensação de segurança experimentada pelas vítimas (Livingstone, 2020).

2.3.2 COMPARTILHAMENTO DE MATERIAL ABUSIVO INFANTIL

O compartilhamento de conteúdo pornográfico envolvendo menores é crime previsto no artigo 240 do ECA, com penas que variam de 4 a 8 anos de reclusão. As camadas *deep* e *dark web* são os principais meios utilizados para disseminar esse tipo de material, muitas vezes protegido por criptografia e anonimato. A SaferNet tem trabalhado em conjunto com provedores e a Polícia Federal para identificar e bloquear conteúdos, mas o volume é crescente e exige constante atualização tecnológica e legal (SaferNet, 2023).

Outro aspecto crucial da pedofilia *online* é o compartilhamento de material abusivo infantil, que ocorre principalmente em fóruns fechados e na *dark web*. A

Internet Watch Foundation (IWF, 2021) relatou que, em 2021, mais de 252 mil URLs continham material sexual envolvendo crianças, destacando a escala alarmante desse crime.

A Internet Watch Foundation é uma organização britânica sem fins lucrativos dedicada a combater a disseminação de imagens e vídeos de abuso sexual infantil na Internet. Tem como missão detectar, interromper, remover e prevenir a distribuição de material de abuso sexual infantil *online*. Seu objetivo é criar uma Internet livre de abuso sexual infantil, tornando-a um ambiente seguro para crianças e adultos em todo o mundo.

Ferramentas como Telegram e Signal, que oferecem criptografia ponta a ponta, são frequentemente usadas para trocar material ilícito, dificultando a interceptação pelas autoridades.

Esses grupos operam em comunidades altamente organizadas, com níveis de acesso baseados em confiança e reputação. Para participar dessas redes, é comum que os criminosos precisem produzir ou compartilhar novo conteúdo, perpetuando o ciclo de abuso (Europol, 2021).

Um outro crime grave esclarecido pela SaferNet é a sextorsão, que envolve a ameaça de divulgação de imagens íntimas para forçar a vítima a realizar ações contra sua vontade — seja pagar dinheiro, enviar mais arquivos, participar de encontro sexual ou ceder a chantagens humilhantes

As formas de ocorrência incluem ameaças por suposto acesso a fotos íntimas, sendo reais ou não; Chantagem após conversas sexuais ou envio voluntário de imagens; Golpes estruturados (como falsas oportunidades de emprego que solicitam conteúdos íntimos); Invasão de dispositivos para obter fotos e vídeos íntimos.

Os agressores frequentemente utilizam o medo, a vergonha e o isolamento da vítima como armas. Eles podem ameaçar expor as imagens em redes sociais, entre familiares, amigos, professores, ou ainda cometer violência física ou emocional caso não obedeçam.

As consequências são extremamente sérias: a vítima vive um ciclo de violência contínua, muitas vezes prolongado por anos, com impacto profundo na sua saúde mental, incluindo risco de depressão e até mesmo suicídio.

A sextorsão é uma forma real e brutal de violência sexual e psicológica que exige atenção imediata.

Os pedófilos aproveitam inovações tecnológicas para dificultar a detecção e garantir a continuidade de seus crimes. Algumas práticas incluem:

- VPNs e *proxies*: Para ocultar endereços IP e localização geográfica;
- *Bots* e identidades falsas: Usados para automatizar interações com várias vítimas ao mesmo tempo;
- Armazenamento criptografado em nuvem: Para guardar material abusivo sem risco de ser descoberto em dispositivos locais.

É essencial quebrar o silêncio, oferecer apoio, denunciar e fortalecer mecanismos de proteção, especialmente para adolescentes e crianças.

2.3.3 SÍMBOLOS DA PEDOFILIA

De acordo com Ismerim (2025) e Côrtes (2024), no ambiente digital, pedófilos frequentemente têm utilizado estratégias cada vez mais sofisticadas para compartilhar pornografia infantil em redes sociais, utilizando códigos e símbolos para se comunicar de maneira dissimulada, dificultando a identificação por autoridades e responsáveis. Entre esses códigos, destaca-se o uso de *emojis* com significados ocultos, que, à primeira vista, parecem inofensivos, mas que, em determinados contextos, assumem conotações específicas dentro de comunidades *online*.

Alguns dos exemplos são: *emoji* de pirulito (🍭), associado à pedofilia por remeter ao termo *lollypop* em inglês, que, por sua vez, faz alusão ao livro Lolita, de Vladimir Nabokov, cuja trama aborda a obsessão de um homem por uma menina de 12 anos e o *emoji* do ciclone (🌀), utilizado para sinalizar conteúdos com conotação sexual envolvendo menores.

Há também *emojis* que podem ser utilizados para falar sobre o órgão sexual masculino e feminino conforme alerta a PSP (Polícia de Segurança Pública) de Portugal (2024).

Conforme relatório do FBI (2007), ainda há comunicação com símbolos, que incluem triângulos e corações concêntricos, em que a figura maior representa o adulto e a menor, a criança. A diferença de tamanho entre as figuras pode indicar a faixa etária de preferência da vítima. Esses sinais são encontrados em *sites*, moedas, joias (como anéis e pingentes) e outros objetos.

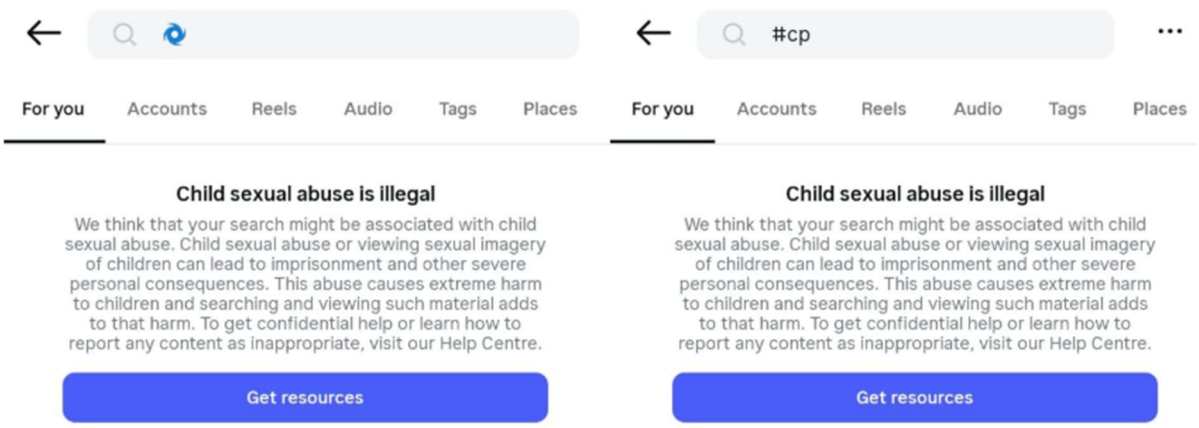
A utilização desses códigos e símbolos evidencia a necessidade de vigilância constante e da adoção de medidas de segurança eficazes para proteger crianças e adolescentes no ambiente virtual. É fundamental que pais, educadores e autoridades estejam atentos a esses sinais e promovam a educação digital como forma de prevenção e combate a esses crimes.

Entre essas estratégias, destaca-se também o uso de *hashtags* com significados ocultos como a #CP (abreviação de *Child Pornography*) que funciona como ferramenta de busca dentro dessas plataformas. Embora medidas tenham sido implementadas para bloquear esses termos e símbolos, conforme resultado apresentado na Figura 3, os infratores rapidamente os substituem por novos códigos, o que dificulta a moderação e o combate efetivo. Além disso, muitos desses conteúdos acabam sendo armazenados e disseminados de forma permanente por meio da *deep web*, evidenciando a complexidade e a urgência do enfrentamento desse tipo de crime no ambiente digital.

Além disso, estudos revelam que esses símbolos são utilizados para driblar os sistemas de moderação das plataformas digitais, permitindo que indivíduos com interesses semelhantes se conectem de forma disfarçada. O uso de *emojis,* símbolos *e hashtags* contribuem para que essas comunicações ocorram de maneira camuflada, dificultando a detecção por algoritmos de segurança.

É importante ressaltar que, embora esses *emojis* tenham significados legítimos em contextos comuns, seu uso em padrões e combinações específicas pode indicar atividades suspeitas. Por isso, a vigilância e a educação digital são essenciais para a identificação e o enfrentamento dessas práticas.

Figura 3: Pesquisas feitas no Instagram



Fonte: Próprio autor, baseado em imagens adquiridas através de pesquisas feitas no Instagram

2.4 CONSEQUÊNCIAS LEGAIS E SOCIAIS

Do ponto de vista legal, a legislação brasileira é clara ao considerar o estupro de vulnerável (art. 217-A do Código Penal) um crime hediondo, com penas de 8 a 15 anos. A produção, posse e divulgação de pornografia infantil são também criminalizadas pelo ECA. A adesão do Brasil à Convenção de Budapeste reforça o compromisso internacional no combate aos crimes cibernéticos (Migalhas, 2023). No campo social, os impactos incluem traumas psicológicos profundos nas vítimas, além da revitimização contínua causada pela circulação indefinida das imagens na Internet (Ribeiro, 2021). Peck (2021) destaca que os crimes relacionados à pedofilia configuram condutas ilícitas que devem ser combatidas com rigor, inclusive por meio de educação digital e políticas públicas de conscientização.

A pedofilia é amplamente reconhecida como um crime grave, e não é necessário que haja contato físico ou relação sexual para que alguém seja considerado pedófilo sob a legislação brasileira. De acordo com o Estatuto da Criança e do Adolescente (ECA), atos como a comercialização, o compartilhamento e até mesmo a posse de imagens ou vídeos pornográficos envolvendo crianças e adolescentes já configuram crimes relacionados à exploração sexual infantil (Brasil, 1990) e o departamento de saúde do Reino Unido, de acordo com Sanderson (2005, p.5) alega que:

> Forçar ou incitar uma criança ou um jovem a tomar parte em atividades sexuais, estejam ou não cientes do que está acontecendo. As atividades podem envolver contato físico, incluindo atos penetrantes (por exemplo, estupro ou sodomia) e atos não penetrantes. Pode incluir atividades sem contato, tais como levar a criança a olhar ou produzir material pornográfico ou a assistir atividades sexuais ou a encorajá-la a comportar-se de maneira sexualmente inapropriadas.

Esse tipo de prática – a exploração sexual infantil, tem se disseminado de forma alarmante pela Internet, utilizando as plataformas digitais como meio de troca e distribuição de material ilegal.

Conforme cita o Ministério Público de Santa Catarina [s.d.]:

> A pornografia infantil consiste em produzir, publicar, vender, adquirir e armazenar pornografia infantil pela rede mundial de computadores, por meio das páginas da *Web*, *e-mail*, *newsgroups*, salas de bate-papo (*chat*), ou qualquer outra forma. Compreende, ainda, o uso da Internet com a finalidade

> de aliciar crianças ou adolescentes para realizarem atividades sexuais ou para se exporem de forma pornográfica.

As consequências para quem se envolve nesses crimes são severas, tanto do ponto de vista legal quanto social. De acordo com a nova redação datada pela Lei nº 11.829, de 25/11/2008) do Estatuto da Criança e do Adolescente (Lei nº 8.069, de 13/07/1990), as principais denominadas pelo ECA (1990) são:

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa".
>
> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008): Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
>
> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008): Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
>
> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008): Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
>
> Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: (Incluído pela Lei nº 11.829, de 2008): Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
>
> Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso: (Incluído pela Lei nº 11.829, de 2008): Pena – reclusão, de 1 (um) a 3 (três) anos, e multa
>
> Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais.

No âmbito social, o estigma vinculado a esse tipo de crime é severo, resultando no isolamento e na rejeição por parte da comunidade e, muitas vezes, até mesmo da família. Isso pode gerar prejuízos profissionais significativos, incluindo a perda do emprego após a condenação, devido à exposição pública. Além disso, o histórico criminal pode dificultar ou até impossibilitar a reinserção no mercado de trabalho. Em alguns casos, o infrator pode ser proibido de acessar a Internet ou utilizar redes

sociais, conforme determinado na sentença, e pode ser submetido a monitoramento mesmo após o cumprimento da pena.

Por outro lado, para as vítimas, as consequências são devastadoras, com impactos psicológicos profundos e de longo prazo, como ansiedade e depressão entre outros até mais graves. A disseminação de imagens e vídeos na Internet, muitas vezes se perpetuam em função de exclusão total ser irreversível, intensificando o sofrimento das vítimas. O Estado deve estar preparado para lidar com os efeitos desses crimes, oferecendo suporte adequado para mitigar os traumas e marcas permanentes que afetam a vida das crianças.

2.5 PREVENÇÃO E COMBATE

A pedofilia já é cometida nas redes sociais a partir do momento que se consume qualquer imagem de conteúdo sexual explicito de um menor. Cabe à lei local, onde ocorreu a publicação da imagem ou até mesmo o *download,* tomar medidas, ou seja, o fato será julgado na seção jurídica do local onde ocorreu as publicações. Hoje existem leis que ajudam a combater crimes como pedofilia na Internet, tendo a polícia civil o poder de investigar os casos divulgados em redes sociais. Ou seja, a competência para julgar o delito do art. 241-A do ECA praticado por meio de WhatsApp ou *chat* do Facebook é da Justiça Estadual, pois tanto no aplicativo WhatsApp quanto nos diálogos (*chat*) estabelecido na rede social Facebook, a comunicação se dá entre destinatários escolhidos pelo emissor da mensagem. Cabe a investigação descobrir quem são os pedófilos que se escondem nas redes sociais e, muitas vezes, em perfis falsos.

Os pedófilos aproveitam-se e criam perfis falsos em redes sociais, utilizam-se de linguagem de fácil entendimento para conseguirem a confiança das crianças e adolescentes. O trabalho busca demonstrar a proteção integral assegurada pelo ECA visando defender a criança e o adolescente de atos abusivos à sua integridade, não importando o meio no qual é praticado, bastando, para isso, que possua a característica de causar dano a criança ou adolescente. (Cabette, 2015).

É de responsabilidade, por meio da polícia jurídica que deverá investigar e buscar provas e indícios, para descobrir quem está por trás das contas falsas na Internet. Nos casos de crimes envolvendo pornografia infantil, ao término do inquérito

policial, os resultados são remetidos ao Ministério Público, que possui a atribuição de apresentar a denúncia, dando início ao processo criminal. Uma das medidas repressivas necessárias para combater a pornografia infantil também é a Infiltração de Agentes Policiais nas Investigações de Cibercrimes. É importante que se entenda como deve ocorrer essa infiltração.

A inovação legislativa da Lei 13.441/17, altera e acrescenta disposições legais ao Estatuto da Criança e do Adolescente (ECA), mais precisamente os artigos 190-A a 190-E, assim apresentados:

Art. 190-A. A infiltração de agentes de polícia na Internet com o fim de investigar os crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A, 217-A, 218, 218-A e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), obedecerá às seguintes regras: [...]. Art. 190-B. As informações da operação de infiltração serão encaminhadas diretamente ao juiz responsável pela autorização da medida, que zelará por seu sigilo. [...]. Art. 190-C. Não comete crime o policial que oculta a sua identidade para, por meio da Internet, colher indícios de autoria e materialidade dos crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A, 217-A, 218, 218- A e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) [...]. Art. 190-D. Os órgãos de registro e cadastro público poderão incluir nos bancos de dados próprios, mediante procedimento sigiloso e requisição da autoridade judicial, as informações necessárias à efetividade da identidade fictícia criada. [...]. Art. 190-E. Concluída a investigação, todos os atos eletrônicos praticados durante a operação deverão ser registrados, gravados, armazenados e encaminhados ao juiz e ao Ministério Público, juntamente com relatório circunstanciado. [...]. (Brasil, 1988 e Brasil, 1990).

Ao examinar a legislação, observa-se a legitimidade da infiltração policial na Internet como medida de combate aos crimes cibernéticos, bem como o impacto significativo que essa legislação, relativamente recente, trouxe para o enfrentamento dessas práticas ilícitas.

Diante da facilidade com que as crianças acessam a Internet atualmente, seja por meio de *tablets*, computadores ou celulares, surgem lacunas no ambiente familiar pois os pais não têm conhecimento sobre o conteúdo que seus filhos acessam, com quem interagem ou quais plataformas utilizam. Por isso, é fundamental conscientizar os responsáveis sobre os materiais que as crianças e adolescentes consomem na Internet, a fim de evitar que se tornem vítimas da pedofilia virtual. Em muitos casos, o

Estado dispõe de ferramentas que podem ser implementadas para auxiliar no monitoramento e controle do que é acessado pois é responsabilidade do Estado desenvolver e implementar políticas públicas voltadas para a conscientização social e dos familiares, proteger e educar as crianças, conforme apresentado no Art. 227 (Brasil, 2010):

> É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

É igualmente importante educar e proteger tanto crianças quanto adolescentes sobre os riscos presentes no ambiente virtual. Não basta apenas acompanhar suas atividades *online*, mas também orientá-los sobre as possíveis consequências de suas interações na Internet.

A prevenção da pedofilia *online* exige ações integradas entre poder público, instituições educacionais, ONGs e famílias. A atuação de entidades como a SaferNet, a Polícia Federal e os provedores de Internet é fundamental. Entre as ferramentas disponíveis estão *softwares* de controle parental como Qustodio, Bark e Kaspersky Safe Kids, que auxiliam os pais a monitorar e restringir o uso de dispositivos por crianças (Wizcase, 2024). Além disso, a educação digital nas escolas e a orientação contínua em casa são pilares fundamentais para fortalecer a segurança das crianças na rede (Moreira *et al*., 2019). Para Peck (2021), promover uma cultura de proteção digital é papel de todos — especialmente da família, que precisa assumir a responsabilidade ativa na orientação do uso da tecnologia.

2.6 SEGURANÇA DA INFORMAÇÃO COMO ALIADA NA PREVENÇÃO E COMBATE À PEDOFILIA *ONLINE*

No contexto da era digital, os crimes contra a dignidade sexual de crianças e adolescentes assumiram novas formas, exigindo respostas igualmente inovadoras. A pedofilia virtual, enquanto prática criminosa mediada por tecnologias, impõe desafios aos sistemas legais, às plataformas digitais e, sobretudo, às estratégias de segurança da informação. Nesse cenário, os três pilares fundamentais da segurança da informação — Confidencialidade, Integridade e Disponibilidade — despontam como

elementos essenciais para garantir ambientes digitais mais seguros e eficazes na prevenção e combate à exploração sexual infantil.

O princípio da confidencialidade refere-se à garantia de que apenas pessoas autorizadas tenham acesso a determinadas informações. Quando aplicado à proteção de crianças e adolescentes, esse princípio implica em salvaguardar dados pessoais sensíveis, como localização, imagens e conversas *online*. Plataformas digitais e aplicativos que permitem interações entre crianças e terceiros precisam incorporar mecanismos robustos de criptografia, controle de acesso e anonimização de dados. A quebra dessa confidencialidade, como no caso do vazamento de informações de menores, pode colocá-los em risco direto de exposição a predadores sexuais (NIC.br, 2022).

O segundo pilar, a integridade, assegura que as informações armazenadas e transmitidas não sejam alteradas indevidamente. Isso é crucial no contexto de investigações de crimes cibernéticos, pois garante que provas digitais — como registros de conversas, imagens e IPs de acesso — permaneçam intactas e confiáveis para serem utilizadas em processos legais. Além disso, a integridade de dados impede que materiais digitais manipulados ou falsificados sejam utilizados para incriminar indevidamente indivíduos ou para encobrir crimes reais (Castro, 2020).

A disponibilidade, por sua vez, assegura que sistemas, plataformas e canais de denúncia estejam operacionais sempre que necessários. Ferramentas como o Disque 100, a Central Nacional de Denúncias da SaferNet e portais de atendimento de órgãos como o Ministério da Justiça e a Polícia Federal devem estar sempre acessíveis, permitindo denúncias rápidas e efetivas. A falha na disponibilidade desses serviços pode impedir a interrupção de abusos em tempo real, além de comprometer investigações e salvamentos de vítimas (SaferNet Brasil, 2023).

Esses três pilares, juntos, formam a base de qualquer estratégia digital voltada à proteção de menores. Seu uso não se restringe à esfera técnica, mas deve integrar políticas públicas, diretrizes escolares, projetos educacionais e ações familiares. Ferramentas de controle parental, por exemplo, são recursos baseados nos pilares da segurança da informação e, quando bem configuradas, protegem o ambiente digital doméstico contra acessos a conteúdos impróprios e contatos suspeitos.

Além disso, o uso da inteligência artificial e da automação na detecção de conteúdos ilegais — como no caso do Projeto Arachnid — só é efetivo se embasado em princípios de segurança da informação. O sistema depende da confidencialidade

dos dados denunciados, da integridade das imagens coletadas e da disponibilidade constante de servidores para rastreamento e emissão de alertas (Apolitical, 2024).

Portanto, os pilares da segurança da informação não apenas sustentam a infraestrutura tecnológica, mas também são aliados indispensáveis na luta contra a pedofilia *online*. Eles garantem a proteção dos dados das vítimas, preservam provas digitais, facilitam investigações e tornam o sistema de justiça mais eficaz. Investir em segurança da informação é investir na infância, no futuro e na dignidade humana.

2.7 CONTROLE PARENTAL

O controle parental é uma ferramenta que passa a ser cada vez mais fundamental na proteção de crianças e adolescentes no ambiente digital tão cheio de possibilidades — e de perigos também. É um cuidado necessário no dia a dia digital das famílias.

Segundo Moreira (2019), o controle parental envolve o uso de aplicativos ou sistemas que permitem aos pais e responsáveis monitorar e limitar o uso da Internet pelas crianças, filtrando o que elas acessam, controlando o tempo de uso dos dispositivos, e até mesmo acompanhando a localização em tempo real por meio de GPS. O objetivo não é apenas restringir, mas sim orientar e prevenir. Como reforça Ribeiro (2021), a presença de um adulto atento, que utiliza esses recursos com diálogo e responsabilidade, faz toda a diferença na formação de um uso mais consciente e seguro da tecnologia.

Além disso, algumas ferramentas atuais já oferecem um monitoramento mais inteligente, como é o caso do Bark, que analisa mensagens e redes sociais em busca de sinais de *bullying*, conteúdos sexuais ou qualquer interação suspeita (Allaboutcookies, 2024). Já o Qustodio, por exemplo, permite acompanhar os *sites* acessados, bloquear aplicativos e ainda controlar o tempo de tela de forma bem prática (Wizcase, 2024). Isso ajuda bastante na rotina das famílias, porque muitas vezes os pais não conseguem acompanhar tudo que os filhos estão fazendo *online* — e essas ferramentas dão um auxílio essencial.

Vale dizer que o controle parental não substitui a presença e o diálogo. Ele funciona melhor quando está aliado à conversa franca e constante entre adultos e crianças. Como destaca Teixeira (2022), o uso dessas tecnologias precisa vir

acompanhado de orientação, escuta e construção de confiança. Não se trata de vigiar ou punir, mas de proteger, educar e acompanhar de perto.

De acordo com Martins Junior (2023), o controle parental vai além do simples bloqueio de conteúdos: trata-se de um cuidado ativo e consciente que todo pai, mãe ou responsável deve adotar para proteger seus filhos no ambiente digital. O autor defende que a tecnologia inclui um conjunto de práticas e tecnologias, e quando bem orientada, pode ser aliada na formação das crianças, mas alerta que o excesso de liberdade sem acompanhamento adequado as expõe a conteúdos inapropriados, *cyberbullying*, perda de privacidade e dependência digital. Ele propõe, ainda, o uso equilibrado de ferramentas tecnológicas associadas a diálogo, escuta ativa e construção de limites saudáveis. Reforça ainda que, o verdadeiro cuidado se dá pela presença ativa e responsável na vida digital dos filhos. Essa abordagem está alinhada à ideia de que a combinação entre educação digital e monitoramento ativo forma uma das estratégias mais eficientes na proteção de crianças e adolescentes contra os perigos da Internet.

Dessa forma, o controle parental se mostra uma ferramenta essencial no mundo atual. Mais do que limitar, ele ajuda a criar uma Internet mais segura e saudável para crianças e adolescentes. E com tantas possibilidades boas na rede, nada mais justo do que garantir que esse acesso venha com cuidado, limites e, principalmente, responsabilidade compartilhada entre pais, responsáveis, escola e sociedade.

2.7.1 FERRAMENTAS DE CONTROLE PARENTAL

Diversas ferramentas de controle parental estão disponíveis atualmente, cada uma com suas particularidades e abrangência de recursos. Algumas oferecem um conjunto mais completo de funcionalidades, enquanto outras são mais focadas em aspectos específicos da segurança digital. São elas:

Norton Family:

A empresa Norton Family [s.d.], oferece um conjunto robusto de recursos, incluindo supervisão da *web*, supervisão de tempo, supervisão de pesquisas, supervisão de vídeos (YouTube), supervisão de aplicativos e relatórios de atividades.

Permite definir limites de tempo de uso por dispositivo e agendar horários específicos. Possui um portal para pais e um aplicativo móvel para gerenciamento remoto.

Seus recursos podem ser destacados em oferecer filtragem da *web*, bloqueando *sites* impróprios por idade, e gerenciamento de tempo, que limita o uso diário dos dispositivos. Supervisionando pesquisas e vídeos, pois monitora o conteúdo acessado no YouTube e em buscadores, enquanto a supervisão de aplicativos permite bloquear ou acompanhar apps específicos. Os relatórios de atividade fornecem um panorama do uso *online*.

Para a segurança física, o alerta de localização rastreia o dispositivo do filho. Por fim, a solicitação de acesso incentiva o diálogo, permitindo que as crianças peçam liberação para *sites* bloqueados. Em suma, essas ferramentas promovem um uso da Internet mais seguro, equilibrado e consciente.

Ela é considerada uma ferramenta eficiente com uma quantidade substancial de recursos para monitorar e proteger as atividades *online* das crianças. A filtragem da *web* e o gerenciamento de tempo são geralmente eficazes. A capacidade de monitorar pesquisas e vídeos no YouTube oferece uma camada extra de segurança.

Como limitação, destaca-se o monitoramento de versão não paga, que não monitora em profundidade as redes sociais. Esta funcionalidade está disponível apenas em versão paga, com recursos abrangentes.

Google SafeSearch:

O SafeSearch do Google é um filtro integrado ao mecanismo de busca que tem como objetivo principal bloquear conteúdo explícito — como nudez, atos sexuais e violência — dos resultados de pesquisa, abrangendo tanto imagens quanto vídeos.

Entre seus principais recursos, destaca-se a filtragem de conteúdo explícito, que impede a exibição de resultados de pesquisa com material adulto. O SafeSearch oferece opções de filtragem que permitem ao usuário escolher entre filtrar, desfocar ou até mesmo desativar o filtro, caso não esteja bloqueado por configurações de rede ou dispositivo. Sua aplicabilidade se estende a diversos serviços do Google, operando na Pesquisa Google, no Google Imagens e no YouTube, onde filtra os resultados de busca.

A eficiência do SafeSearch reside em sua utilidade como ferramenta para filtrar conteúdo explícito dentro do ecossistema Google. Contudo, sua proteção é limitada ao ambiente do Google, não se estendendo a outros *sites* ou aplicativos. Além disso,

o filtro pode ser desativado pelo próprio usuário, a menos que haja um bloqueio imposto pelas configurações do dispositivo ou da rede. Apesar de ser gratuito e útil, o SafeSearch funciona como uma medida complementar de segurança, e sua principal limitação é não realizar bloqueios em outros *sites* ou aplicativos fora do Google.

Open*DNS* FamilyShield:

É um serviço gratuito de *DNS* (*Domain Name System*) disponibilizado pela empresa Cisco, que oferece filtragem de conteúdo em nível de rede. Ao configurar seus dispositivos ou roteador para utilizar os servidores *DNS* do FamilyShield, o acesso a *sites* categorizados como adultos, de phishing ou maliciosos é automaticamente bloqueado.

Entre seus recursos, destaca-se a filtragem em nível de *DNS*, que bloqueia o acesso a domínios inteiros que contêm conteúdo inadequado. Além disso, o FamilyShield oferece proteção contra malware e phishing, ajudando a prevenir o acesso a *sites* perigosos. A configuração é geralmente fácil, exigindo apenas a alteração das configurações de *DNS* no roteador ou nos dispositivos.

Em termos de eficiência, o FamilyShield é uma ferramenta eficaz para bloquear categorias inteiras de *sites* indesejados em todos os dispositivos conectados à rede configurada. No entanto, ele não oferece recursos de monitoramento detalhado de atividades específicas ou gerenciamento de tempo de tela. Sua eficácia depende diretamente da correta configuração do *DNS*. Por ser totalmente gratuito, o Open*DNS* FamilyShield é ideal como uma camada adicional de proteção, mas sua limitação principal é a ausência de controle de tempo de tela ou monitoramento de atividades em redes sociais.

Microsoft Family Safety:

O Family Safety é uma solução abrangente para o gerenciamento da segurança digital familiar disponibilizado pela empresa Microsoft. É integrado ao sistema operacional Windows e disponível como aplicativo para Android e iOS, ele oferece uma série de recursos para que pais e responsáveis possam gerenciar o tempo de tela, filtrar conteúdo, monitorar atividades *online* e até mesmo rastrear a localização dos membros da família.

Entre seus principais recursos, o Family Safety permite o gerenciamento de tempo de tela, possibilitando a definição de limites de tempo para o uso de dispositivos

e aplicativos. Ele também conta com filtros de conteúdo para bloquear aplicativos e jogos inadequados para a idade das crianças. A ferramenta oferece monitoramento de atividades, que acompanha os *sites* visitados, aplicativos utilizados e o tempo gasto *online*. Para maior segurança, há o rastreamento de localização, que permite visualizar onde os membros da família estão. Além disso, são disponibilizados relatórios de atividade, fornecendo resumos minuciosos das interações *online*, e controles de gastos, que auxiliam no gerenciamento das compras das crianças na Microsoft Store.

A eficiência do Microsoft Family Safety é notável, especialmente para famílias que utilizam dispositivos Windows, dada a profunda integração com o sistema operacional. Os recursos de gerenciamento de tempo, filtragem de conteúdo e monitoramento de atividades são particularmente úteis para a proteção infantil. No entanto, sua limitação reside no fato de funcionar melhor em dispositivos Windows e Xbox, apresentando algumas restrições em plataformas Android e iOS. A versão gratuita do serviço oferece apenas recursos básicos, sendo que a versão completa e mais robusta está integrada ao pacote pago do Microsoft 365.

Kaspersky Safe Kids:

Este aplicativo de controle parental oferecido pela empresa tecnológica Russa Kaspersky, disponibiliza um conjunto abrangente de recursos para a segurança digital das crianças. Ele inclui funcionalidades como filtragem da *web*, gerenciamento de tempo de tela, monitoramento de aplicativos, rastreamento de localização por GPS e alertas em tempo real.

Entre seus recursos, destaca-se a filtragem da *web* inteligente, que bloqueia *sites* e categorias de conteúdo considerados perigosos. O gerenciamento de tempo de tela permite definir limites diários e agendamentos para o uso de dispositivos, complementado pelo controle de uso de aplicativos, que ajuda a gerenciar o tempo gasto em apps específicos. Para garantir buscas mais seguras, ele oferece pesquisa segura, filtrando resultados em mecanismos de busca populares. Há também o monitoramento do YouTube, permitindo visualizar o histórico de pesquisa e os vídeos assistidos. A segurança física é reforçada pelo localizador por GPS, que acompanha a localização do dispositivo da criança, e pelos alertas em tempo real, que notificam os pais sobre atividades suspeitas ou tentativas de acesso a conteúdo bloqueado.

A ferramenta se mostra altamente eficiente no controle parental, fornecendo uma vasta gama de recursos para proteger as crianças tanto *online* quanto *offline*. A filtragem inteligente da *web* e o gerenciamento de tempo são robustos, enquanto o monitoramento do YouTube e a localização por GPS adicionam camadas importantes de segurança. No entanto, sua limitação reside na versão gratuita, que possui funcionalidades restritas. A *interface* também pode ser um pouco confusa para alguns usuários, e os recursos mais completos estão disponíveis apenas na versão paga.

Qustodio:

Esta ferramenta é uma solução de controle parental abrangente que proporciona a pais e responsáveis uma visão aprofundada e controle sobre as atividades digitais de seus filhos. Ela oferece um leque de funcionalidades que incluem filtragem da *web* e de aplicativos, limites de tempo de tela, monitoramento de atividades (inclusive chamadas e SMS em dispositivos Android), rastreamento de localização, monitoramento do YouTube e relatórios detalhados.

Entre os recursos disponibilizados, destacam-se a filtragem da *web* e de aplicativos, que permite bloquear ou monitorar o acesso a conteúdos específicos. É possível definir limites de tempo de tela, tanto diários quanto por horários, para regular o uso dos dispositivos. O monitoramento de atividades abrange *sites* visitados, aplicativos utilizados, e um diferencial importante é a capacidade de rastrear chamadas e SMS em dispositivos Android. Para o conteúdo audiovisual, o monitoramento do YouTube acompanha os vídeos assistidos e as pesquisas realizadas. A segurança física é garantida pelo rastreamento de localização, que permite saber onde a criança está, e pelo botão de pânico (SOS), que possibilita à criança enviar um alerta de emergência para contatos predefinidos. Por fim, a ferramenta gera relatórios detalhados com informações completas sobre a atividade *online* e *offline*.

Considerando a gama de recursos disponíveis, percebe-se que este aplicativo oferece uma grande variedade de recursos e seu desempenho é confiável. A capacidade de monitorar chamadas e SMS em dispositivos Android é um recurso adicional de grande valor. Contudo, sua principal limitação é que o plano gratuito é um pouco restrito, e para acessar as funcionalidades avançadas e completas, é necessário adquirir uma assinatura paga.

3 APLICAÇÃO PRÁTICA

Após a apresentação das ferramentas disponíveis, o Qustodio se destaca por sua abrangência de funcionalidades e sua integração com os princípios de segurança da informação, oferecendo uma solução mais completa para a proteção de crianças e adolescentes em seus dispositivos e atividades online. Sendo assim, este trabalho optou por focar nesse aplicativo afim de complementá-lo ao Project Arachnid, que é uma iniciativa tecnológica e colaborativa fundamental na luta contra a disseminação de material de abuso sexual infantil na Internet. Mesmo não sendo os dois considerados similares, o Qustodio e o Projeto Arachnid se complementam pois operam em camadas diferentes de proteção, mas com o mesmo objetivo final: a segurança e proteção da criança.

A fim de testar o uso dessa ferramenta, propõe o seguinte caso:

Uma mãe chamada Marcela, tem um filho de 10 anos que tem um *tablet* para fazer as lições de casa e para se comunicar com amigos. A mãe está preocupada com a segurança *online* do filho e deseja garantir que ele não esteja acessando conteúdo inapropriado.

A mãe decide instalar o aplicativo Qustodio no *tablet* do filho para monitorá-lo em suas atividades *online* visando acompanhar visitas a *sites*, detectar palavras chaves relacionadas a conteúdos inapropriados, como violência, pornografia ou *bullying*. E para que seja enviado alertas a ela quando detectado atividades suspeitas ou impróprios.

Como resultado, a Figura 4 apresenta os resultados desse monitoramento, e a mãe descobre que o filho estava tentando acessar redes sociais não adequados para sua idade e *sites* de jogos de azar. Recebe também alertas sobre pesquisas feitas com palavras suspeitas e inapropriadas.

O objetivo principal do Qustodio é fornecer aos pais e responsáveis ferramentas para monitorar e gerenciar a atividade *online* e o uso de dispositivos de seus filhos. A ideia central é promover um ambiente digital seguro e equilibrado, permitindo que os pais protejam seus filhos de conteúdos inadequados, *cyberbullying*, predadores *online* e outros riscos associados ao mundo digital. Além disso, busca auxiliar na gestão do tempo de tela, incentivando hábitos digitais saudáveis.

Figura 4: Notificação do App Qustodio

Fonte: Próprio autor, baseado em imagens adquiridas através de pesquisas feitas no App Qustodio

3.1 QUSTODIO

O Qustodio é uma ferramenta de controle parental robusta e amplamente utilizada, cujo foco está na promoção da segurança digital e no uso consciente da tecnologia por crianças e adolescentes. A seguir, são apresentadas suas principais funcionalidades, que o tornam uma das soluções mais completas disponíveis atualmente:

a) Filtragem de conteúdo e aplicativos: O Qustodio permite bloquear ou permitir o acesso a *sites* e aplicativos com base em mais de 25 categorias temáticas, como jogos de azar, violência, redes sociais, conteúdo adulto, entre outros. Essa filtragem pode ser configurada de forma personalizada, permitindo regras específicas para cada categoria ou até mesmo para URLs individuais. Essa funcionalidade é fundamental para proteger o público infantojuvenil de conteúdos inapropriados e potencialmente prejudiciais.

b) Gerenciamento de tempo de tela: Com a crescente exposição a dispositivos digitais, o Qustodio oferece ferramentas para limitar o tempo de uso diário, tanto do dispositivo como de aplicativos específicos. É possível agendar períodos sem acesso, como durante os estudos ou à noite. Isso favorece a criação de hábitos digitais mais saudáveis e contribui para o equilíbrio entre o uso da tecnologia e outras atividades essenciais.

c) Monitoramento de atividades: O aplicativo fornece relatórios detalhados sobre as atividades realizadas no dispositivo monitorado, incluindo histórico de

navegação, uso de aplicativos e termos pesquisados. Dependendo do plano contratado, esses dados podem ser armazenados por até 30 dias. Essa função proporciona maior transparência e controle sobre os comportamentos digitais da criança ou adolescente.

d) Rastreamento de localização e *geofencing* (Tecnologia que utiliza dados de localização, como GPS, para criar cercas virtuais em torno de áreas geográficas específicas): O Qustodio também atua como ferramenta de segurança física, por meio do rastreamento em tempo real dos dispositivos e da criação de cercas geográficas (*geofencing*). Os responsáveis são notificados sempre que o dispositivo entra ou sai de áreas previamente definidas, o que é especialmente útil em rotinas escolares ou passeios.

e) Monitoramento de Chamadas e Mensagens (Android): No sistema Android, o Qustodio possibilita o monitoramento de chamadas telefônicas e mensagens de texto, com acesso a contatos e conteúdo trocado. No sistema iOS, essas funcionalidades são restritas devido às limitações de privacidade impostas pela própria Apple. Essa função é relevante no contexto da proteção contra contatos inadequados e riscos como o aliciamento *online*.

f) Botão de Pânico (SOS): Presente nos planos premium, o botão de pânico permite que a criança envie, em situações de emergência, um alerta imediato aos responsáveis, incluindo sua localização atual. Essa funcionalidade amplia a proteção, oferecendo uma resposta rápida em cenários de risco.

O Qustodio geralmente é elogiado pela sua *interface* intuitiva e facilidade de uso, tanto na configuração inicial quanto no acompanhamento diário.

a) Processo de Instalação: O processo de instalação do aplicativo nos dispositivos dos filhos e do aplicativo de controle nos dispositivos dos pais é geralmente simples e guiado por instruções claras.

b) Painel de Controle *Online*: A maior parte da gestão e visualização das informações é feita através de um painel de controle *online* acessível via navegador *web* ou por meio de um aplicativo para pais. Esse painel é geralmente bem organizado e fácil de navegar, permitindo que os pais visualizem rapidamente as informações relevantes.

c) Configurações Personalizáveis: As opções de configuração são flexíveis e permitem adaptar as regras de monitoramento e bloqueio às necessidades específicas de cada família e idade da criança.

d) Relatórios Claros: Os relatórios gerados são geralmente fáceis de entender, apresentando as informações de forma visual e resumida.

3.1.1 SEGURANÇA DA INFORMAÇÃO NO QUSTODIO

A Qustodio, como uma empresa que lida com dados sensíveis de famílias e crianças, leva a segurança da informação e a privacidade de seus clientes muito a sério. Baseado em suas políticas de privacidade e informações públicas, eles empregam uma série de medidas e princípios para tratar a segurança dos dados:

A Qustodio utiliza criptografia padrão da indústria tanto para dados "em trânsito" (quando estão sendo enviados entre os dispositivos e seus servidores) quanto para dados "em repouso" (quando estão armazenados em seus data centers). Isso significa que as informações são codificadas para que apenas partes autorizadas possam lê-las. Utilizam *data centers* de *Tier* 1 fornecidos por grandes empresas como Microsoft, Amazon e Google, que são conhecidas por seus altos padrões de segurança e resiliência. Também trata dos dados pessoais com estrita confidencialidade, de acordo com as leis aplicáveis (como o GDPR na Europa).

A Qustodio explicitamente declara que não vende nem cede a terceiros, listas com dados pessoais ou de qualquer outro tipo, mas que podem compartilhar dados com outras empresas do grupo Qoria ou com prestadores de serviços, mas apenas quando estritamente necessário para a prestação dos serviços e sob suas instruções, sem que esses terceiros possam usar os dados para seus próprios fins.

A Qustodio coleta apenas os dados pessoais que são necessários para a prestação de seus serviços. Isso inclui dados de registro (nome, *e-mail*), dados de navegação (endereço IP, tipo de navegador) e dados de atividades do dispositivo monitorado (*sites* visitados, aplicativos usados, etc.) para fins de filtragem e relatórios.

A coleta de dados via MDM (*Mobile Device Management*) em dispositivos iOS, por exemplo, garante que o tráfego do dispositivo vá apenas para os servidores da Qustodio e não seja compartilhado com terceiros. Para fins de otimização de serviço, pesquisa e análise interna, a Qustodio pode processar dados de forma agregada e não identificável. Isso significa que os dados são dissociados de qualquer informação que possa identificar um indivíduo antes de serem usados para análises ou compartilhados com terceiros para melhorias de serviço.

Em conformidade com as leis de proteção de dados, a Qustodio oferece aos usuários o direito de acessar, corrigir ou apagar seus dados pessoais. Isso permite que os clientes tenham controle sobre as informações que a empresa possui sobre eles. Também há o direito de retirar o consentimento para o processamento de dados, embora isso possa afetar a capacidade da Qustodio de fornecer certos serviços.

A Qustodio retém os dados pessoais apenas pelo tempo necessário para cumprir as finalidades para as quais foram coletados, incluindo requisitos legais, contábeis ou de relatórios. Geralmente, retêm os dados durante o período de assinatura ativa e por um período adicional (exemplo 5 anos) para fins legais/administrativos. Requerem a criação de nome de usuário e senha exclusivos, e podem exigir outras medidas de segurança como PINs. Senhas são armazenadas de forma criptografada e não são reemitidas (é preciso criar uma nova em caso de esquecimento). Não armazenam informações de pagamento diretamente, utilizando provedores de pagamento terceirizados compatíveis com PCI-DSS. Se comprometem em notificar os clientes em caso de violação de segurança de dados pessoais de forma eletrônica e em tempo hábil.

Diante dos desafios impostos pela pedofilia no ambiente digital, ferramentas como o Qustodio emergem como aliadas importantes na proteção de crianças e adolescentes. Ao oferecer funcionalidades que abrangem o monitoramento da atividade *online*, a filtragem de conteúdo, o gerenciamento do tempo de tela e o rastreamento de localização, o Qustodio se alinha aos princípios da segurança da informação para criar um ambiente digital mais seguro.

A confidencialidade é reforçada pela capacidade do aplicativo de proteger dados sensíveis das crianças, como histórico de navegação e comunicações *online*, evitando sua exposição a terceiros mal-intencionados. A integridade é garantida pelo registro preciso das atividades *online*, fornecendo aos pais informações confiáveis sobre o comportamento digital de seus filhos. A disponibilidade é assegurada pela facilidade de acesso às ferramentas de monitoramento e controle, permitindo intervenções rápidas em situações de risco.

Dessa forma, o Qustodio se mostra uma ferramenta essencial para a promoção da segurança digital no ambiente familiar, especialmente quando se trata da proteção de crianças e adolescentes. Suas funcionalidades, aliadas a um sistema de controle eficiente e políticas de privacidade robustas, garantem não apenas a integridade dos

dados coletados, mas também uma camada adicional de segurança contra ameaças como a exposição a conteúdos impróprios e o aliciamento virtual.

No entanto, é crucial reconhecer que o Qustodio, assim como qualquer ferramenta tecnológica, não é uma solução completa em si. Seu uso efetivo depende da educação digital contínua, do diálogo aberto entre pais e filhos e da implementação de políticas públicas que promovam a segurança *online*. Além disso, é fundamental que os desenvolvedores de aplicativos priorizem a segurança da informação em todas as etapas do processo de desenvolvimento, implementando medidas robustas de proteção de dados e garantindo a privacidade dos usuários.

Nesse sentido, o aplicativo contribui significativamente para o enfrentamento da pedofilia no ambiente *online*, permitindo uma atuação preventiva por parte dos responsáveis e fortalecendo a cultura da proteção infantojuvenil no espaço digital. Em última análise, o Qustodio representa um avanço promissor na luta contra a pedofilia *online*, mas seu sucesso depende de uma abordagem mista que combine tecnologia, educação e responsabilidade social.

3.2 PROJETO ARACHNID

O Project Arachnid é uma ferramenta tecnológica que busca material de abuso sexual infantil (CSAM) visitando páginas, lendo seu conteúdo e extraindo dados. Este projeto tem uma iniciativa diferente, não sendo um controle parental como o Qustodio, mas uma ferramenta vital para o combate global à pedofilia.

O Project Arachnid, é uma iniciativa canadense desenvolvida pelo Canadian Centre for Child Protection (CCCP). Utilizando tecnologias avançadas, o projeto visa identificar e remover conteúdos ilegais da Internet, contribuindo significativamente para a proteção de crianças e adolescentes no ambiente digital.

O principal objetivo é detectar e eliminar imagens e vídeos de abuso sexual infantil na Internet. Através de tecnologias como machine learning e rastreamento automatizado, o sistema monitora continuamente a *web* em busca de conteúdos ilegais, emitindo alertas e solicitações de remoção aos provedores de serviços.

Desde sua implementação, o Projeto Arachnid já contribuiu para a remoção de milhões de imagens de abuso sexual infantil da Internet, representando um avanço significativo na luta contra esse tipo de crime. O projeto colabora com organizações e

provedores de serviços de Internet para manter listas de bloqueio atualizadas, garantindo que usuários sejam protegidos contra o acesso a conteúdo nocivos e utiliza algoritmos de aprendizado de máquina para identificar e sinalizar conteúdos suspeitos em tempo real, aumentando a eficácia na detecção de materiais ilegais.

Porém os desafios desse projeto podem ser grandes, visto que criminosos costumam adotar técnicas para burlar os sistemas de detecção, como o uso de redes privadas ou criptografia, dificultando a identificação de conteúdo ilegais. A eficácia do projeto depende da cooperação internacional, pois conteúdos podem ser hospedados em servidores de diferentes países, exigindo uma ação coordenada para sua remoção. A constante evolução das tecnologias e métodos utilizados por criminosos requer que o Projeto Arachnid esteja em constante atualização para manter sua eficácia.

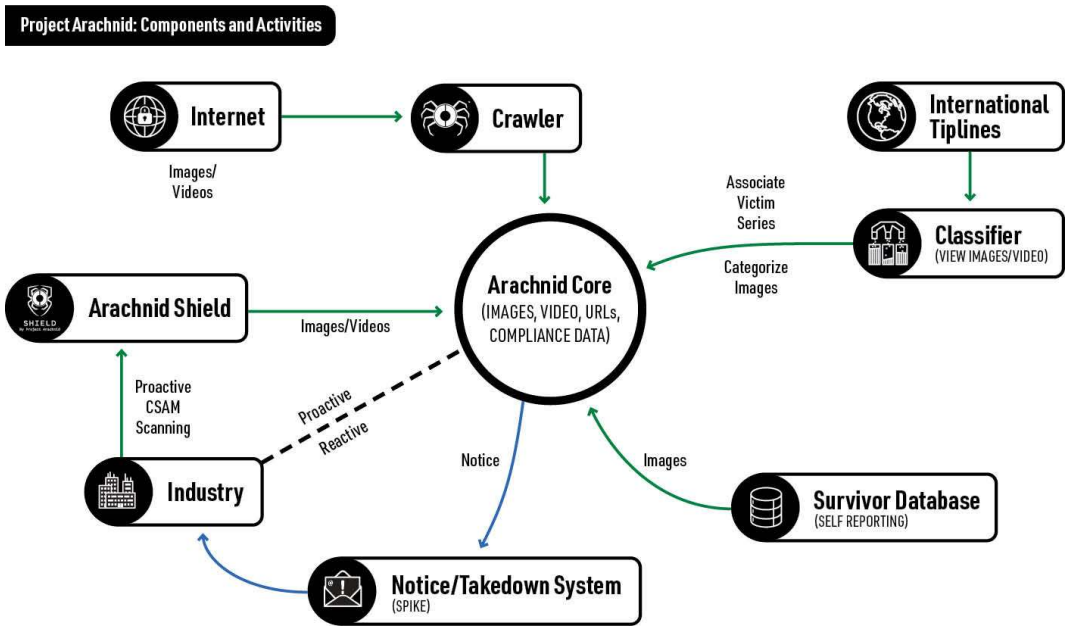
Enquanto ferramentas de controle parental como o Qustodio oferecem aos pais um controle essencial e direto sobre o ambiente digital de seus filhos, atuando na prevenção e monitoramento em nível doméstico, iniciativas globais como o Project Arachnid complementam essa proteção ao combater a fonte do problema, trabalhando para identificar e remover material de abuso sexual infantil da Internet. Juntas, essas abordagens formam uma estratégia mais robusta e abrangente para a segurança da informação e a proteção da criança no ambiente digital, enquanto uma foca na defesa do usuário, a outra foca na limpeza da rede.

A Figura 5 ilustra os componentes e as principais atividades do Project Arachnid, evidenciando seu ecossistema de combate à proliferação de Material de Abuso Sexual Infantil (CSAM) na Internet. No centro, o Arachnid Core representa o cerne do sistema, responsável pelo processamento de imagens, vídeos e URLs, além de dados de conformidade. É demonstrado que o conteúdo (imagens e vídeos) é inicialmente coletado da Internet por um *Crawler*, que envia esse material para o Arachnid Core. De forma complementar, a iniciativa Shield *by* Project Arachnid permite que a Indústria (provedores de serviços eletrônicos, ESPs) realize a varredura proativa de CSAM conhecido e imagens prejudiciais/abusivas envolvendo crianças em seus próprios sistemas, enviando esses dados diretamente para o Arachnid Core.

Uma vez no Arachnid Core, o material identificado como CSAM pode gerar um "*Notice*" (aviso) para o *Notice/Takedown System* (*SPIKE*), que por sua vez interage com a Indústria para a remoção do conteúdo. O diagrama também revela a colaboração global, com *International Tiplines* (linhas diretas internacionais, como

organizações de proteção à criança e *hotlines*) que enviam dados para um *Classifier*, que categoriza as imagens e as associa a séries de vítimas, alimentando o Arachnid Core. A menção a um "*Survivor Database*" (Banco de Dados de Sobreviventes) que envia imagens ao Core sugere a integração de informações de autodenúncia para identificação de conteúdo.

Figura 5: Project Arachnid: Componentes e Atividades



Fonte: Project Arachnid – Disponível em https://www.projectarachnid.ca/en/. Acesso em: 11 jun. 2025

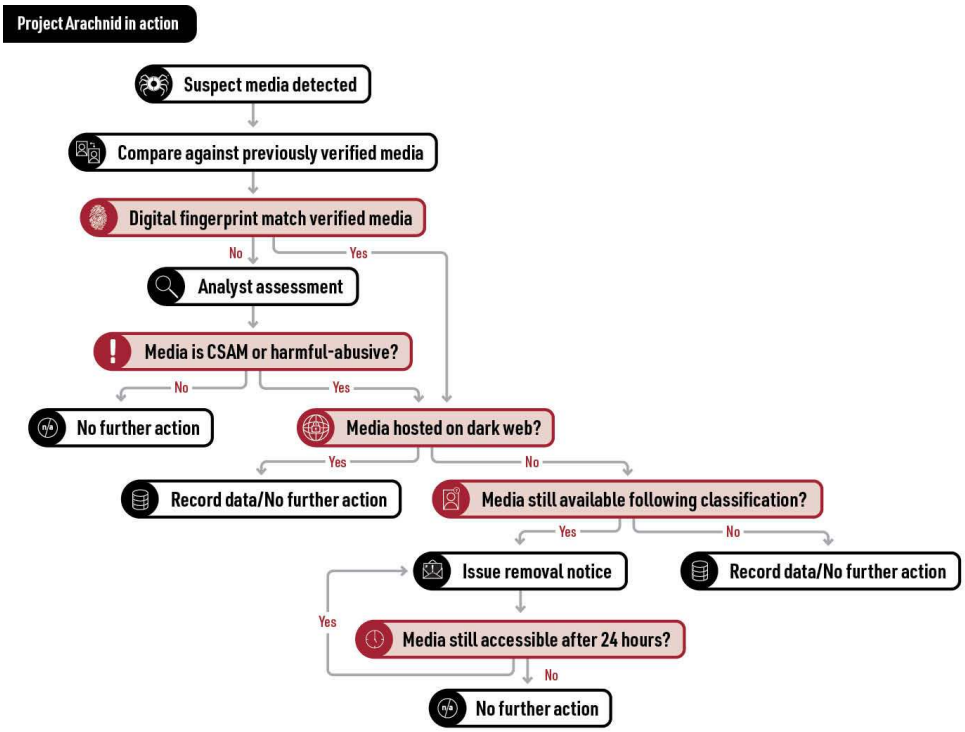
Na Figura 6, é detalha o fluxo operacional do Project Arachnid em ação, desde a detecção de mídia suspeita até a decisão de remoção ou não. O processo inicia com a detecção de "*Suspect media*" (mídia suspeita). Essa mídia é então comparada a um banco de dados de "*previously verified media*" (mídia previamente verificada), utilizando uma tecnologia fundamental de *hashing* de imagens e vídeos, que permite a correspondência precisa contra o CSAM conhecido.

Caso haja uma correspondência de impressão digital com mídia verificada, o sistema avança para a próxima etapa. Caso contrário, a mídia passa por uma "*Analyst assessment*" (avaliação do analista), indicando a importância da intervenção humana na classificação de conteúdo não automaticamente identificado. Após a avaliação (ou a correspondência direta), é determinado se a mídia é CSAM ou material prejudicial/abusivo. Se não for, nenhuma ação adicional é tomada.

Se confirmada como CSAM, o diagrama explora o caminho a seguir, incluindo a verificação se a mídia está hospedada na *dark web*. Embora a imagem sugira uma

ação de registro de dados para mídias na *dark web* sem indicação de remoção direta por esse fluxo, para mídias não hospedadas na *dark web*, o sistema verifica se o material ainda está disponível após a classificação. Se sim, um "*removal notice*" (aviso de remoção) é emitido. A imagem culmina com uma verificação crucial: se a mídia ainda está acessível após 24 horas, indicando um processo de acompanhamento da efetividade da remoção. Este fluxograma ilustra a lógica de decisão e as etapas de ação que o Project Arachnid emprega para identificar, classificar e buscar a eliminação do CSAM *online*.

Figura 6: Project Arachnid em ação



Fonte: Project Arachid – Disponível em https://www.projectarachnid.ca/en/. Acesso em: 11 jun. 2025

As ilustrações apresentadas demonstram, de forma gráfica, a complexidade e a abrangência do funcionamento do Project Arachnid, desde a detecção inicial até os processos de classificação e notificação para remoção.

Em conjunto com a análise do Qustodio, que foca na proteção em nível de usuário e família, fica evidente que a segurança digital infantil e o combate à pedofilia *online* exigem uma estratégia integrada. A atuação de ferramentas de controle parental lado a lado com iniciativas globais de "limpeza da rede" é fundamental para construir um ecossistema digital mais seguro, onde a segurança da informação e a proteção das crianças são prioridades em todas as suas camadas.

4 CONSIDERAÇÕES FINAIS

Este trabalho evidenciou a complexidade do fenômeno da pedofilia no ambiente virtual, onde a segurança da informação e a educação digital surgem como ferramentas cruciais para a prevenção e proteção de crianças e adolescentes. A pesquisa ressaltou a importância de compreender as dinâmicas desse crime, que se manifesta em diversas camadas da Internet, desde a *surface web* até a *dark web*, explorando a vulnerabilidade infantil de forma multifacetada.

Os resultados apontam para a necessidade de uma abordagem integrada, que envolva a sociedade, famílias, instituições de ensino, governos e órgãos de segurança, na promoção de um ambiente *online* mais seguro e na desconstrução da cultura de impunidade que frequentemente ocorrem os crimes virtuais. A conscientização, a informação e o desenvolvimento de habilidades digitais críticas são essenciais para capacitar crianças e adolescentes a se protegerem, bem como para munir os adultos com o conhecimento necessário para intervir e denunciar situações de risco.

A aplicação prática deste estudo demonstrou a relevância de soluções tecnológicas como o Qustodio e o Projeto Arachnid no enfrentamento dessa problemática.

O Qustodio, como ferramenta de controle parental, exemplifica a importância da defesa ativa no ambiente doméstico. Ele capacita pais e responsáveis a gerenciar o tempo de tela, filtrar conteúdos inadequados e monitorar as atividades *online*, criando uma camada essencial de proteção direta para as crianças e adolescentes em seus dispositivos. Junto a ele, o Projeto Arachnid ilustra a ação em escala global para a limpeza da rede. Ao atuar na identificação e remoção proativa de Material de Abuso Sexual Infantil (CSAM), esta iniciativa demonstra como a segurança da informação, aplicada em nível de infraestrutura e colaboração internacional, é fundamental para combater a disseminação do conteúdo pedófilo em sua origem.

A análise conjunta dessas duas abordagens ressalta que a segurança digital infantil não pode ser única. As ferramentas de proteção doméstica, como o Qustodio, são vitais para a prevenção individual e familiar, enquanto iniciativas como o Projeto Arachnid são indispensáveis para o combate e a eliminação de conteúdo ilícito da Internet. A efetividade da segurança da informação e da proteção da criança e da sociedade depende da sinergia entre essas diferentes esferas de atuação.

Uma atuação do Supremo Tribunal Federal (STF, 2025) demonstra um movimento crucial em direção à responsabilização das plataformas digitais pelo conteúdo ilegal veiculado em suas redes. A decisão de rever o Artigo 19 do Marco Civil da Internet visa exigir que as *Big Techs* aprimorem a moderação e removam proativamente materiais ilícitos, incluindo aqueles relacionados a crimes como a pornografia infantil. Essa mudança reflete a crescente urgência na regulamentação do ambiente online e sublinha a necessidade de que o conjunto de leis acompanhe a dinâmica das interações digitais para fortalecer a proteção de crianças e adolescentes.

Espera-se que este trabalho contribua para o aprofundamento do debate sobre o tema e para o desenvolvimento de estratégias mais eficazes no combate à pedofilia *online*, visando a construção de um futuro digital mais seguro e protetivo para a infância. Pesquisas contínuas e o desenvolvimento de novas tecnologias, aliadas a uma conscientização global, são os pilares para assegurar que o ambiente digital seja um espaço de aprendizado e desenvolvimento, e não de risco.

REFERÊNCIAS

ALLABOUTCOOKIES. Bark Review 2025: **A parental control app with a unique approach**, 2025. Disponível em: https://allaboutcookies.org/bark-review. Acesso em: 14 abr. 2025.

APA - American Psychistric Associstion. **Manual diagnóstico e estatístico de transtornos mentais**: DSM-5. 5. ed. Porto Alegre: Artmed, 2014. Disponível em: http://institutopebioetica.com.br/documentos/manual-diagnostico-e-estatistico-de-transtornos-mentais-dsm-5.pdf. Acesso em: 23 out. 2024.

APOLITICAL. **Conheça Arachnid**: o rastreador que caça fotos de abuso infantil na Internet. Disponível em: https://apolitical.co/solution-articles/pt/meet-arachnid-crawler-hunting-child-abuse-photos-across-*web*. Acesso em: 18 abr. 2025.

BANDEIRA, José Ricardo. **Pedofilia feminina:** quebrando os tabus psicológicos e sociais. Jusbrasil, 2022. Disponível em: https://www.jusbrasil.com.br/artigos/pedofilia-feminina/1347511167. Acesso em: 9 jun. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 03 jun. 2025.

BRASIL. **Estatuto da criança e do adolescente**. Lei nº 8.069, de 13 de julho de 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 03 jun. 2025.

CABETTE, Eduardo Luiz Santos. A **pedofilia na era digital à luz do estatuto da criança e do adolescente**. JusBrasil. Disponível em: https://www.jusbrasil.com.br/artigos/a-pedofilia-na-era-digital-a-luz-do-estatuto-da-crianca-e-do-adolescente-por-caio-tacito-griecco-de-andrade-siqueira/239700073. Acesso em: 17 nov. 2024.

CÂMARA DOS DEPUTADOS. **Relatório setorial de combate à pedofilia, da subcomissão especial de combate à pedofilia**. [s.d.] Disponível em: https://www.camara.leg.br/proposicoes*Web*/prop_mostrarintegra?codteor=1837994. Acesso em: 16 maio 2025.

CAMPELO, Larissa; PIRES, Pamela de Freitas. **Crimes virtuais**. Jus.com.br. Disponível em: https://jus.com.br/artigos/72619/crimes-virtuais. Acesso em: 17 nov. 2024.

CARVALHO, José Alfredo. **Riscos no Discord expõem crianças e adolescentes ao abuso virtual**. 2023. Disponível em: https://redept.org/blogosfera/riscos-no-discord-expoem-criancas-e-adolescentes-ao-abuso-virtual/. Acesso em: 02 jun. 2025.

CASTRO, Alexandre de. **Segurança da informação:** o uso responsável da informação. São Paulo: Érica, 2020.

CÔRTES, Tiago da Silva. **As estratégias dos "novíssimos aliciadores" para difundir material digital pornográfico**. 2024. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BJB/article/view/72688/50942. Acesso em: 03 maio 2025.

EUROPOL. **Internet organised crime threat assessment** (IOCTA), 2021. Disponível em: https://www.europol.europa.eu/publications-events/main-reports/Internet-organised-crime-threat-assessment-iocta-2021. Acesso em: 22 nov. 2024.

FBI. **Symbols and logos used by pedophiles to identify sexual preferences**. 2007. Disponível em: https://www.wikileaks.org/wiki/FBI_pedophile_symbols. Acesso em: 08 maio 2025.

FERNANDES, Juliana. Dobras #60 // **O lado obscuro do Discord:** os riscos às crianças e adolescentes em meio a servidores cada vez mais violentos. 2023. Disponível em: https://medialabufrj.net/blog/2023/09/dobras-60-o-lado-obscuro-do-discord-os-riscos-as-criancas-e-adolescentes-em-meio-a-servidores-cada-vez-mais-violentos/. Acesso em: 02 jun. 2025.

GOOGLE. **Filtrar resultados explícitos usando o SafeSearch**. [s.d.] Disponível em: https://support.google.com/*web*search/answer/510?hl=pt&prev=https://www.google.com/safesearch?hl=pt&visit_id=638852504776286841-1698566236&p=ws_settings_safesearch&rd=1. Acesso em: 14 abr. 2025.

INTERNET WATCH FOUNDATION (IWF). **Annual report**. 2021. Disponível em: https://www.iwf.org.uk/about-us/who-we-are/annual-report-2021/. Acesso em: 22 nov. 2024.

INTERNET WATCH FOUNDATION (IWF). **Internet Watch Foundation**. [s.d.] Disponível em: https://www.iwf.org.uk/. Acesso em: 03 jun. 2025.

ISMERIM, Flávio. **Entenda significado de *emojis* usados como código para crimes, ofensa e sexo.** São Paulo: CNN Brasil. Disponível em: https://www.cnnbrasil.com.br/tecnologia/entenda-significado-de-*emojis*-usados-como-codigo-para-crimes-ofensa-e-sexo/. Acesso em: 08 maio 2025.

KASPERSKY. **Kaspersky safe kids.** Disponível em: https://www.kaspersky.com.br/safe-kids. Acesso em: 14 abr. 2025.

LIVINGSTONE, S.; STOILOVA, M.; KELLY, A. *Online* risks to children: implications for policy and practice. **LSE Research *Online***, 2020.

MACHADO, Talita Ferreira Alves. **Criança vítima de pedofilia:** fatores de risco e danos sofridos. São Paulo: USP / Faculdade de Direito, 2013.

MARTINS JUNIOR, Wilson. **Controle Parental:** um cuidado que todo pai, mãe e responsável precisa ter. Clube de Autores, 2024.

MATOS, Christiano Rocha de. **Uma análise da pedofilia a partir das publicações na rede mundial de computadores**. 2013. Disponível em https://jus.com.br/artigos/24595/uma-analise-da-pedofilia-a-partir-das-publicacoes-na-rede-mundial-de-computadores. Acesso em: 02 jun. 2025.

MICROSOFT. **Microsoft family safety.** [s.d.] Disponível em: https://www.microsoft.com/pt-br/microsoft-365/family-safety. Acesso em: 14 abr. 2025.

MIGALHAS. **Convenção de Budapeste e crimes cibernéticos no Brasil**, 2023. Disponível em: https://www.migalhas.com.br. Acesso em: 14 abr. 2025.

MOREIRA, Rodrigo P. *et al*. Prevenção de crimes virtuais contra crianças e adolescentes. **Interfaces - Revista de extensão da UFMG**, v. 7, n. 2, p. 150-159, jul./dez. 2019.

MPDFT - MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS, 2025. **O que é pedofilia?** Disponível em: https://www.mpdft.mp.br/portal/index.php/conhecampdft-menu/nucleos-e-grupos/nevesca/perguntas-frequentes-mainmenu-428/3194-o-que-e-pedofilia. Acesso em: 16 maio 2025.

MPSC - MINISTÉRIO PÚBLICO DE SANTA CATARINA. [s.d.] **Navegação segura na Internet e combate à pedofilia:** Sobre a pedofilia. Disponível em: https://www.mpsc.mp.br/navegacao-segura-na-Internet-e-combate-a-pedofilia/sobre-a-pedofilia. Acesso em: 03 jun. 2025.

NIC.br. **Cartilha de segurança para Internet**. São Paulo: Comitê Gestor da Internet no Brasil, 2022. Disponível em: https://cartilha.cert.br. Acesso em: 18 abr. 2025.

NORTON. **Norton Family:** controle parental avançado. [s.d.] Disponível em: https://br.norton.com/products/norton-family. Acesso em: 14 abr. 2025.

O LENHADOR (The Woodsman). Direção: Nicole Kassell. Estados Unidos: Showtime Independent Films, 2004. Filme. 87 min.

OPEN*DNS*. **Home internet *security*.** Disponível em: https://www.opendns.com/home-Internet-security/. Acesso em: 14 abr. 2025.

PECK, Patrícia. **Direito digital**. 7. ed. São Paulo: Saraiva Educação, 2021.

PISCITELLI, Adriana; GREGORI, Maria Filomena; CARRARA, Sérgio. **Sexualidade e saberes:** convenções e fronteiras. Rio de Janeiro: Garamond, 2004.

PROJECTARACHNID. **O que é o Project Arachnid?** [s.d] Disponível em https://www.projectarachnid.ca/en/#what-is-project-arachnid. Acesso em 12 de maio 2025.

PSP – Polícia de Segurança Pública (Portugal). **ALERTA PAIS - Sabia que um emoji pode ter vários significados?**. 2024. Disponível em: https://www.instagram.com/p/DHlrGCFNcJV/?img_index=2. Acesso em: 12 maio 2025.

QUSTODIO. **Política de privacidade do Qustodio family**. 2023. Disponível em: https://www.qustodio.com/pt-br/family/privacy/ Acesso em: 03 jun. 2025.

QUSTODIO. **A solução completa de controle parental e bem-estar digital**. [s.d.] Disponível em: https://www.qustodio.com/pt-br/family/privacy/ Acesso em: 14 abr. 2025.

REDE JESUÍTA DE EDUCAÇÃO. **Como preparar crianças e adolescentes para interagir com o mundo digital.** 2023. Disponível em: https://redejesuitadeeducacao.com.br/2023/06/30/artigo-como-preparar-criancas-e-adolescentes-para-interagir-com-o-mundo-digital/. Acesso em: 16 maio 2025.

RIBEIRO, Jéssica G. M. **A pedofilia no âmbito virtual**. Rubiataba: Faculdade Evangélica, 2021.

SANDERSON, Chrstiane. **Abuso sexual em crianças**. São Paulo: M. Books, 2005.

SAFERNET Brasil. **#INDICADORESHELPLINE**. [s.d.] Disponível em: https://indicadores.safernet.org.br/helpline/helplineviz/helpchart-page.html. Acesso em: 09 jun. 2025.

SAFERNET Brasil. I**ndicadores da central nacional de denúncias de crimes cibernéticos**. 2024. Disponível em: https://indicadores.safernet.org.br/index.html. Acesso em: 14 abr. 2025.

SAFERNET Brasil. **O que é sextorsão?**. [s.d.] Disponível em https://new.safernet.org.br/content/o-que-%C3%A9-sextors%C3%A3o. Acesso em: 09 jun. 2025.

SAFERNET Brasil. **Relatório de atividades 2023**. 2023. Disponível em: https://new.safernet.org.br. Acesso em: 14 abr. 2025.

SCOFIELD, Laura. **Discord desobedece às próprias regras e permite conteúdo violento e extremista**. 2023. Disponível em: https://apublica.org/2023/04/discord-desobedece-as-proprias-regras-e-permite-conteudo-violento-e-extremista/. Acesso em: 02 jun. 2025.

SERAFIM, Antonio *et al*. **Perfil psicológico e comportamental de agressores sexuais de crianças**. 2009. Disponível em: https://www.scielo.br/j/rpc/a/vHCDkd9cw7cKpnLRLDgfLXk/. Acesso em: 23 nov. 2024.

TEIXEIRA, Isadora M. **Pornografia infantil, pedofilia e a aplicação da lei em crimes virtuais**. PUC-GO, 2022.

VEJA. STF forma maioria para aplicar leis mais duras contra redes sociais. **VEJA** Coluna Maquiavel, 2024. Disponível em: https://veja.abril.com.br/coluna/maquiavel/stf-forma-maioria-para-aplicar-leis-mais-duras-contra-redes-sociais/. Acesso em: 12 jun. 2025.

WIZCASE. **Qustodio:** free vs. premium comparison. 2024. Disponível em: https://www.qustodio.com/en/difference-between-qustodio-free-and-qustodio-premium/. Acesso em: 14 abr. 2025.