DÉBORA DE SOUZA TURIAL

A EFETIVIDADE DAS OPERAÇÕES POLICIAIS PARA O COMBATE A PORNOGRAFIA INFANTIL NO BRASIL

Orientador: Professor Sandro Lúcio Dezan

FACULDADE DE DIREITO DO CENTRO UNIVERSITÁRIO DE BRASÍLIA

BRASÍLIA
2025

DÉBORA DE SOUZA TURIAL

A EFETIVIDADE DAS OPERAÇÕES POLICIAIS PARA O COMBATE A PORNOGRAFIA INFANTIL NO BRASIL

Artigo apresentado como requisito parcial para a obtenção do grau de Bacharel em Direito, do Centro Universitário de Brasília. Orientador: Prof. Sandro Lúcio Dezan

BRASÍLIA
2025

DÉBORA DE SOUZA TURIAL

A EFETIVIDADE DAS OPERAÇÕES POLICIAIS PARA O COMBATE A PORNOGRAFIA INFANTIL NO BRASIL

Artigo apresentado como requisito parcial para a obtenção do grau de Bacharel em Direito, do Centro Universitário de Brasília.

BRASÍLIA
2025

Banca Examinadora

Prof. Sandro Lúcio Dezan

Orientador

Examinador

Examinador

RESUMO

A expansão do acesso à internet no Brasil intensificou a ocorrência de crimes digitais, dentre os quais a disseminação de pornografia infantil se destaca como uma grave problemática para a proteção de crianças e adolescentes. Em 2023, a Central Nacional de Denúncias da SaferNet Brasil registrou 71.867 denúncias únicas de imagens de abuso e exploração sexual infantil, representando um aumento de 77,13% em relação a 2022. Esse crescimento reflete tanto a sofisticação das redes criminosas quanto as fragilidades institucionais no enfrentamento desses delitos. Este artigo objetiva avaliar a eficácia de determinadas iniciativas operacionais conduzidas pelas forças policiais brasileiras, voltadas ao enfrentamento da pornografia infantil no ambiente virtual. identificando gargalos e propondo soluções que envolvam o aprimoramento das técnicas investigativas e o fortalecimento da cooperação internacional. A análise dos casos revela que, apesar de avanços significativos nas operações, persistem entraves tecnológicos e estruturais que comprometem a eficácia plena das medidas adotadas, indicando a necessidade de modernização das políticas públicas de segurança digital e de investimentos contínuos em tecnologia investigativa. A pesquisa adota uma abordagem qualitativa, baseada em análise de dados secundários, revisão de literatura especializada e estudo de casos emblemáticos, de modo a oferecer uma visão crítica sobre as limitações atuais e apontar diretrizes para o aprimoramento das práticas institucionais.

Palavras-chave: Pornografia infantil; investigação cibernética; legislação; segurança digital.

ABSTRACT

The expansion of internet access in Brazil has increased the occurrence of digital crimes, among which the dissemination of child pornography stands out as a serious problem for the protection of children and adolescents. In 2023, SaferNet Brasil's National Reporting Center registered 71,867 unique reports of images of child sexual abuse and exploitation, representing an increase of 77.13% compared to 2022. This growth reflects the sophistication of criminal networks and institutional weaknesses in combating these crimes. This article aims to evaluate the effectiveness of certain operational initiatives carried out by Brazilian police forces aimed at combating child pornography in the virtual environment, identifying bottlenecks, and proposing solutions that involve improving investigative techniques and strengthening international cooperation. The analysis of the cases reveals that, despite significant advances in operations, technological and structural obstacles persist that compromise the measures' effectiveness, indicating the need to modernize public digital security policies and make continuous investments in investigative technology. The research adopts a qualitative approach, based on secondary data analysis, review of specialized literature, and study of emblematic cases, to offer a critical view of current limitations and point out guidelines for improving institutional practices.

Keywords: Child pornography; cyber investigation; legislation; digital security.

1- INTRODUÇÃO

A consolidação da internet como espaço central de sociabilidade, informação e entretenimento revelou, de forma contundente, os limites dos mecanismos tradicionais de controle penal e prevenção de delitos. Entre os fenômenos mais inquietantes que emergem nesse ambiente, destaca-se a disseminação de material envolvendo abuso e exploração sexual de crianças e adolescentes, frequentemente impulsionada por redes transnacionais que operam com alto grau de anonimato e sofisticação técnica. De acordo com a SaferNet Brasil (2025), (Organização Não Governamental Brasileira que atua na promoção e defesa dos direitos humanos na internet), somente no segundo semestre de 2024, observou-se um crescimento de 78% nos grupos e canais ativos no Telegram dedicados à veiculação desse tipo de conteúdo, atingindo uma audiência estimada em 1,4 milhão de usuários. Tal amplitude revela não apenas o alcance da criminalidade digital, mas sobretudo a fragilidade dos instrumentos institucionais destinados ao seu enfrentamento.

De modo complementar, o relatório internacional *Into the Light – Global Index of Child Sexual Exploitation and Abuse Prevalence* (CHILDLIGHT, 2024) estima que mais de 300 milhões de crianças foram vítimas de alguma forma de abuso sexual online no período de doze meses. Ademais, aproximadamente uma em cada oito crianças foi exposta, sem consentimento, a solicitações ou materiais de natureza sexual por meios digitais. Essas evidências quantitativas reafirmam o caráter

transnacional da crise, cuja resposta não pode ser limitada à repressão pontual, exigindo, ao contrário, articulação multissetorial, uso de tecnologia avançada e responsabilização efetiva dos infratores.

Diante dessa configuração, propõe-se, neste artigo, uma análise crítica do desempenho de operações policiais específicas, realizadas no Brasil, com foco no combate à pornografia infantil online. Parte-se da hipótese de que, apesar de avanços legislativos e institucionais significativos — como a ampliação das penas e a especialização de unidades investigativas —, persistem obstáculos estruturais que comprometem a eficiência das ações repressivas. Entre tais entraves, sobressaem a morosidade na cooperação jurídica internacional, a dificuldade de rastreamento de transações criptografadas e a desarticulação entre os diversos órgãos incumbidos da repressão cibernética.

Para atingir tal finalidade, adota-se uma abordagem qualitativa, fundamentada em revisão bibliográfica, análise documental e estudo de casos. O presente trabalho opera-se a partir da análise de três operações policiais brasileiras de significativa repercussão: Terabyte, Banhammer e Adolescência Segura. A primeira, realizada em 2023 pela Polícia Civil do Distrito Federal, destacou-se pelo uso intensivo de perícia digital e pela extração de provas em dispositivos eletrônicos de múltiplos alvos. A segunda, deflagrada em dezembro de 2024 também pela Polícia Civil do DF, envolveu a apreensão de um adolescente apontado como líder de um grupo de abusadores que operava por meio de redes criptografadas. Já a terceira, conduzida em abril de 2025 pela Polícia Civil do Estado do Rio de Janeiro, com o apoio do Ministério da Justiça, revelou a existência de uma organização criminosa de âmbito nacional, composta por adultos e adolescentes, dedicada a uma ampla gama de crimes cibernéticos, incluindo a disseminação de pornografia infantil, induzimento ao suicídio, apologia ao nazismo e tentativa de homicídio. E como exemplo de operação de maior envergadura e impacto, sobressai a Operação Luz na Infância, coordenada pelo Ministério da Justiça e Segurança Pública em 2017. A escolha dessas ações investigativas consolida-se em sua relevância nacional, nos diferentes níveis de articulação institucional envolvidos e na diversidade de desafios enfrentados durante a persecução penal.

No plano teórico, o artigo fundamenta-se em uma base bibliográfica multidisciplinar, composta por autores nacionais e estrangeiros que abordam, sob diferentes perspectivas, os desafios jurídicos, investigativos e tecnológicos do enfrentamento à pornografia infantil online. Apresentam-se como centrais, nesse

conjunto, os aportes de Eoghan Casey (2011) sobre a lógica da investigação forense digital; Rodrigo de Oliveira Souza (2021) e Tainá da Costa Silva (2022), quanto aos limites normativos no ciberespaço; e Alessandro Barreto (2021), ao tratar da criminalidade na deep web. Soma-se a esses, ainda, a contribuição de Higor Vinícius Jorge (2021) na delimitação das práticas de investigação criminal tecnológica, além de estudos institucionais, como os relatórios da SaferNet Brasil, da Chainalysis (2023) e do projeto internacional ChildLight (2024), que fornecem dados empíricos relevantes para a análise.

Sob o ponto de vista jurídico, são examinados os principais dispositivos legais brasileiros aplicáveis ao tema — notadamente o Estatuto da Criança e do Adolescente (Lei nº 8.069/1990), a Lei nº 13.441/2017 e o Marco Civil da Internet (Lei nº 12.965/2014) —, em diálogo com tratados internacionais como a Convenção de Budapeste. De forma complementar, são analisadas experiências estrangeiras exitosas, como o Project VIC (EUA) e as operações promovidas pela Europol, com vistas à identificação de boas práticas e lacunas estruturais no modelo nacional.

Considerando o exposto, este estudo tem por objetivo central avaliar a atuação do Estado brasileiro na repressão à pornografia infantil disseminada por meios digitais. Ao trazer à luz as contradições entre avanços normativos e ineficiências operacionais, busca-se contribuir para o aperfeiçoamento das políticas públicas de enfrentamento. A proposta está estruturada na articulação entre tecnologia forense, cooperação institucional e garantia integral dos direitos da infância frente aos desafios impostos por uma criminalidade difusa, descentralizada e, muitas vezes, invisibilizada.

2- PEDOFILIA E PORNOGRAFIA INFANTIL

2.1. A pedofilia como transtorno psiquiátrico segundo a OMS

Na Classificação Internacional de Doenças (CID-11), a pedofilia é definida como “um transtorno parafílico caracterizado por uma atração sexual persistente ou predominante por crianças pré-púberes, geralmente com idade inferior a 13 anos” (OMS, 2019). Importa destacar que, sob a ótica da psiquiatria, a existência desse transtorno não implica necessariamente a prática de atos criminosos; contudo, constitui um fator de risco relevante para condutas ilícitas, especialmente em ambientes digitais que favorecem o anonimato e a impunidade.

A literatura especializada enfatiza a necessidade de distinção entre a condição clínica da pedofilia e os comportamentos criminosos concretos, como a produção, o

compartilhamento e o consumo de material pornográfico envolvendo crianças e adolescentes. Seto (2009) demonstra que, embora nem todo indivíduo com diagnóstico de pedofilia pratique abusos, uma parcela expressiva dos ofensores sexuais manifesta esse padrão de interesse. Nesse sentido, Caramigo (2017) destaca que a pedofilia, por si só, não configura crime, sendo uma condição médica que exige abordagem terapêutica e não repressiva. Para o autor, a confusão recorrente entre desejo e ação penalmente relevante tem contribuído para uma abordagem punitivista inadequada, que falha tanto na prevenção quanto na proteção das vítimas. Ele afirma: “pedofilia não é crime, mas sim uma doença. O que é crime é o ato praticado com base nesse desejo” (Caramigo, 2017).

Essa distinção é crucial para evitar a estigmatização de indivíduos que possuem o transtorno, mas não cometem crimes, e para assegurar que a resposta penal seja direcionada à conduta delituosa, não à condição psicológica. Além disso, é importante considerar que o tratamento da pedofilia é clínico e não criminal, sendo a intervenção penal aplicável apenas quando há exteriorização da patologia por meio de atos tipificados como crimes.

No âmbito investigativo, de acordo com Lyon (2007), a identificação de perfis psicosexuais compatíveis com a pedofilia tem contribuído para a construção de algoritmos e sistemas de monitoramento comportamental, os quais buscam detectar padrões de consumo digital relacionados à pornografia infantil. Tais ferramentas, embora úteis, também suscitam discussões sobre privacidade, consentimento e os limites da vigilância em ambientes digitais.

Portanto, compreender a pedofilia como um fenômeno multidimensional — envolvendo aspectos clínicos, jurídicos, tecnológicos e sociais — é indispensável para o desenvolvimento de políticas públicas eficazes, que combinem repressão penal, acesso a tratamento e estratégias de prevenção, sobretudo no contexto hiperconectado da contemporaneidade.

2.2. A Relação entre Pedofilia e o Crime de Pornografia Infantil

Em 2024, o Brasil passou a integrar o conjunto dos cinco países que mais reportaram conteúdos relacionados ao abuso sexual infantil na internet, conforme levantamento realizado pela rede internacional InHope (Associação Internacional de Fornecedores de Linhas de Emergência na Internet). A atuação da SaferNet Brasil, enquanto canal oficial de denúncias no país, foi determinante para esse

posicionamento, sendo responsável por significativa parcela das notificações encaminhadas para remoção de material ilícito (Safernet Brasil, 2024a). Apenas no ano de 2023, foram registradas 71.867 denúncias de imagens de abuso e exploração sexual de crianças e adolescentes, configurando o maior volume já registrado desde o início da série histórica nacional (Safernet Brasil, 2024b).

Tais números, embora reflitam a crescente mobilização da sociedade civil, expõem simultaneamente a limitação estrutural da resposta estatal frente à complexidade dos crimes cibernéticos. A dinâmica digital contemporânea, marcada pela criptografia, anonimato e pulverização das redes de compartilhamento, dificulta sobremaneira a identificação dos agentes envolvidos e a obtenção de provas válidas para persecução penal. À luz dessa realidade, consolida-se um ecossistema de impunidade e reiterada violação de direitos fundamentais da infância.

Acrescenta-se a essa realidade a persistente ausência de um arcabouço jurídico plenamente adaptado às especificidades dos delitos informáticos. Como observa Atheniense (apud Câmara dos Deputados, 2006), a vedação à analogia no direito penal impede que práticas não tipificadas expressamente, como o armazenamento de arquivos ilícitos em servidores estrangeiros ou a integração a grupos criptografados de compartilhamento de CSAM (Child Sexual Abuse Material), sejam alcançadas por sanções penais. Embora dispositivos como o Estatuto da Criança e do Adolescente ofereçam certa cobertura normativa, o ordenamento jurídico brasileiro permanece carente de uma legislação integral e funcional que atenda às demandas emergentes da criminalidade digital.

A percepção de vulnerabilidade sistêmica é agravada pela ineficácia dos mecanismos de cooperação internacional, pela morosidade dos processos de extradição e pela utilização de recursos tecnológicos como criptomoedas e redes ocultas (dark web), que dificultam a rastreabilidade das transações e o rastreamento de fluxos de conteúdo ilícito. Conforme salientado pelo Deputado Federal Regis de Oliveira (apud Câmara dos Deputados, 2006), uma parcela residual, mas expressiva, dos crimes cibernéticos — justamente os mais sofisticados — permanece fora do alcance da legislação vigente, o que compromete a integridade da proteção jurídica à infância no espaço virtual.

Sob essa perspectiva, a pedofilia, enquanto parafilia de elevado potencial criminógeno, encontra no ambiente digital um vetor privilegiado para a sua manifestação delituosa. A conjunção entre impulso patológico não tratado,

oportunidade tecnológica e fragilidade normativa favorece a transição do desejo para a ação, com implicações devastadoras para as vítimas e desafios estruturais para o Estado. Compreender essa interdependência — entre subjetividade desviada, meio técnico e omissão legislativa — é condição necessária para a formulação de estratégias intersetoriais que combinem diagnóstico clínico, repressão qualificada e políticas de prevenção voltadas à erradicação da circulação de material de abuso sexual infantil na internet.

3- ANÁLISE DAS OPERAÇÕES POLICIAIS

3.1. Operação Terabyte

A escolha da Operação Terabyte para análise justifica-se por ilustrar de maneira didática a repressão qualificada aos crimes de pornografia infantil praticados em ambiente digital. Sua relevância está na articulação interestadual entre forças policiais, no emprego de tecnologia forense de ponta e na efetividade da resposta penal frente a delitos de elevada complexidade investigativa. A atuação da Polícia Civil do Distrito Federal (PCDF) nesta operação evidencia como a aplicação de inteligência cibernética e cooperação interinstitucional pode resultar na interrupção de redes de abuso sexual infantil.

Deflagrada em 25 de setembro de 2024, a Operação Terabyte foi coordenada nacionalmente pela Polícia Federal, com apoio direto da Delegacia Especial de Repressão aos Crimes Cibernéticos (DRCC/PCDF). No Distrito Federal, a operação resultou na prisão de três homens em flagrante por armazenarem e compartilharem material de abuso sexual infantil. Foram cumpridos mandados judiciais e apreendidos diversos dispositivos eletrônicos contendo grande volume de conteúdo ilícito (PCDF, 2024).

A eficiência da operação decorreu da sinergia entre as informações obtidas em cooperação com a Polícia Federal e a precisão técnica da DRCC na execução das diligências. Conforme destaca Casey (2011), a extração de evidências digitais confiáveis exige a combinação de análise de metadados, rastreamento de IPs e a utilização de softwares forenses que garantam a cadeia de custódia e a integridade da prova. Tais recursos foram empregados na operação, permitindo a análise imediata do conteúdo apreendido e a confirmação da materialidade delitiva no ato da prisão.

Ainda assim, a operação evidenciou obstáculos relevantes no âmbito investigativo. Segundo Souza (2021), a morosidade na emissão de mandados

judiciais e a falta de protocolos uniformes entre as instituições comprometem a eficiência das investigações cibernéticas no Brasil. No caso da Operação Terabyte, embora a articulação entre PCDF e PF tenha mitigado parte dessas barreiras, a natureza volátil dos dados digitais exige celeridade processual e integração normativa mais sólida entre os entes envolvidos.

No aspecto operacional, destaca-se ainda a dificuldade de identificação de usuários em plataformas que adotam sistemas de criptografia e anonimização de tráfego, como redes peer-to-peer e fóruns da dark web. Conforme observa Silva (2022), o uso de técnicas de disfarce digital desafia os instrumentos de investigação tradicionais, exigindo constante capacitação técnica de peritos e policiais para a utilização de ferramentas de extração, monitoramento e análise de dados em tempo real.

Além da responsabilização penal dos envolvidos, a operação teve impacto direto na proteção das vítimas e na interrupção do ciclo de revitimização, característico dos crimes de pornografia infantil, em que o compartilhamento contínuo de imagens perpetua o dano psicológico e social. Ademais, a visibilidade da operação reforça o papel do Estado como agente dissuasor, mostrando à sociedade que práticas delituosas no ciberespaço são alvo de monitoramento e repressão efetiva.

3.2. Operação Banhammer

A escolha da Operação Banhammer, cuja “expressão surgiu da combinação de "ban" (proibir, excluir) e "hammer" (martelo), simbolizando uma ação definitiva e implacável.” (PCDF, 2024). Apresenta-se como relevante por sua densidade investigativa, expondo a complexidade dos crimes cibernéticos ligados ao abuso sexual infantil, especialmente quando adolescentes são, ao mesmo tempo, vítimas e agentes ativos na configuração desses crimes. A operação, que envolveu a apreensão de um menor apontado como líder de um grupo dedicado à exploração sexual de outros adolescentes, destaca a natureza multifacetada do problema, refletindo a interação entre vulnerabilidade juvenil, organização criminosa e a exploração do ambiente digital.

Deflagrada em 19 de dezembro de 2024, a operação foi coordenada nacionalmente e contou com desdobramentos relevantes no Distrito Federal. A Polícia Civil, por intermédio da Delegacia de Proteção à Criança e ao Adolescente (DPCA), procedeu à apreensão de um menor envolvido na liderança de um grupo articulado

que se valia de estratégias digitais para cooptar, manipular e abusar de adolescentes. Foram recolhidos dispositivos eletrônicos contendo evidências robustas da atividade criminosa, as quais subsidiaram a responsabilização do apreendido e o desmonte da estrutura virtual de aliciamento e controle psicológico das vítimas (PCDF, 2024).

À luz dessa conjuntura, ganha relevância a atuação estratégica da DPCA, cuja expertise operacional viabilizou a execução célere dos mandados judiciais, além de propiciar uma análise preliminar do material apreendido com elevado grau de precisão técnica. Conforme observa Souza (2021), a investigação de crimes digitais exige domínio metodológico, capacidade analítica e interlocução eficaz entre as esferas policial, pericial e judiciária — elementos que, conjugados, potencializam a eficácia da resposta institucional.

De igual modo, o caso impõe uma reflexão crítica acerca da fluidez entre os papeis de vítima e autor no âmbito da delinquência infantojuvenil. O adolescente em questão, embora exercesse posição de liderança na rede criminosa, apresentava indicativos de exposição precoce a contextos de abuso e vulnerabilidade social. Tal ambivalência, como pontua Silva (2022), exige abordagens interdisciplinares que combinem responsabilização proporcional com estratégias de intervenção psicossocial, de modo a evitar a perpetuação do ciclo da violência.

Frente a essa realidade, torna-se evidente a sofisticação das ferramentas utilizadas pelos envolvidos na tentativa de ocultar suas condutas. O emprego de criptografia, a fragmentação das redes de comunicação e o uso de plataformas com comunicação efêmera constituem obstáculos técnicos consideráveis à atuação estatal. Diante desse cenário, é imprescindível o investimento contínuo em atualização tecnológica, bem como na formação especializada das equipes encarregadas da investigação cibernética.

Cumpre ainda destacar que o episódio trouxe à tona debates sensíveis no campo jurídico, sobretudo no que se refere à responsabilização de menores por condutas de extrema gravidade. Embora o Estatuto da Criança e do Adolescente (ECA) contemple mecanismos adequados para a apuração de atos infracionais, casos como o analisado desafiam os limites normativos entre proteção e responsabilização, exigindo do sistema de justiça atuações firmes, porém juridicamente equilibradas.

Por conseguinte, a operação nacional que culminou na apreensão do adolescente revela, com acentuada clareza, a complexidade da criminalidade infantojuvenil no ciberespaço. Ao mesmo tempo em que evidencia avanços

institucionais — notadamente no campo da investigação especializada —, também sinaliza as insuficiências do modelo repressivo isolado. Nesse sentido, reforça-se a premissa de que o enfrentamento qualificado da violência sexual digital exige não apenas ação estatal pontual, mas a consolidação de uma política pública contínua, multissetorial e orientada à prevenção.

3.3 Operação Adolescência Segura

A "Operação Adolescência Segura" emerge como um esforço significativo da polícia brasileira no combate a crimes cibernéticos que afetam crianças e adolescentes. A escolha da operação revela-se pertinente neste estudo em virtude de sua expressiva amplitude investigativa, natureza interestadual e pela gravidade dos crimes identificados, os quais extrapolam a mera circulação de material de abuso sexual infantil e envolvem condutas como incitação à violência extrema, aliciamento de adolescentes e promoção de desafios criminosos em plataformas digitais criptografadas. O caso assume papel estratégico para a análise da repressão cibernética no Brasil, ao demonstrar, de forma concreta, a interseção entre criminalidade juvenil, redes virtuais estruturadas e fragilidades institucionais de contenção.

Deflagrada em abril de 2025 pela Delegacia da Criança e do Adolescente Vítima (DCAV-RJ), com apoio do Ministério da Justiça por meio do Laboratório de Operações Cibernéticas (Ciberlab), a operação mobilizou forças policiais em sete estados brasileiros e resultou no cumprimento de vinte mandados de busca e apreensão, dois de prisão temporária e sete de internação provisória de adolescentes infratores. O desdobramento das ações levou à prisão de dois adultos e apreensão de sete adolescentes, todos vinculados a uma rede que atuava por meio de plataformas como Telegram e Discord, em que promoviam práticas criminosas, incluindo tentativa de homicídio, induzimento ao suicídio, incentivo à automutilação, maus-tratos a animais e apologia ao nazismo (G1, 2025).

A investigação teve como ponto de partida um episódio registrado em 18 de fevereiro de 2025, no qual um adolescente lançou dois coquetéis molotov contra um homem em situação de rua. O ataque foi transmitido em tempo real para mais de duzentos membros de um servidor digital coordenado por Miguel Felipe, adulto que registrava o crime para fins de exibição e incentivo coletivo. Segundo informações da Polícia Civil, não se tratava de um caso isolado, mas de uma organização altamente

articulada, que operava por meio de recompensas internas, segmentação temática de conteúdos e manipulação psicológica de crianças e adolescentes — características que motivaram inclusive a emissão de relatórios por agências internacionais como a HSI e o NCMEC.

À luz da literatura especializada, a operação representa um exemplo concreto de cooperação interinstitucional estratégica, indispensável à repressão qualificada de crimes digitais. Conforme observam Sobral e Couto (2023), ações articuladas entre diferentes entes da segurança pública, associadas ao uso de tecnologia investigativa, ampliam a eficácia do sistema penal frente à fragmentação e anonimato característicos da criminalidade cibernética. A articulação entre polícias civis estaduais, órgãos federais e entidades internacionais demonstrou-se crucial para a coleta de provas e contenção do grupo investigado.

Além do mérito repressivo, a operação reafirma a tese de que respostas eficazes à pornografia infantil online exigem atuação multidisciplinar e contínua. Como apontam Souza (2021) e Caramigo (2017), não basta a intervenção pontual: é necessário fomentar políticas públicas que combinem educação digital, investimento em capacitação pericial e engajamento da sociedade civil. O êxito da repressão, portanto, depende diretamente da prevenção, da vigilância sistemática e da resiliência institucional.

3.4. Análise comparativa

Quando analisadas em conjunto com os dados quantitativos recentes, as operações Terabyte, Banhammer e Adolescência Segura evidenciam a crescente pressão que os crimes sexuais digitais impõem ao sistema penal brasileiro. O número alarmante de 52.999 denúncias específicas de pornografia infantil em 2024 (SaferNet, 2025), somado à descoberta de mais de 1,25 milhão de usuários envolvidos em canais ilícitos no Telegram, atribui nova gravidade às ações repressivas. Estas cifras apontam não apenas para a escala da problemática, bem como para a sofisticação das redes criminosas, exigindo que as operações policiais avancem para além do cumprimento pontual de mandados e passem a incorporar estratégias tecnológicas permanentes, protocolos interinstitucionais integrados e atuação transnacional coordenada. Sob o ponto de vista jurídico, tal cenário desafia os limites da legalidade tradicional e pressiona o sistema judiciário brasileiro a lidar com demandas por celeridade, quebra de sigilos e responsabilização de agentes menores de idade em

contextos digitais. Do ponto de vista investigativo, reforça-se a urgência de institucionalizar capacidades forenses avançadas e consolidar centros especializados em crimes cibernéticos voltados à proteção da infância.

A análise das operações Terabyte, Banhammer e Adolescência Segura permite identificar padrões, avanços e limitações no enfrentamento da pornografia infantil digital no Brasil. Embora distintas quanto ao contexto operacional, às estruturas dos grupos criminosos envolvidos e ao perfil dos investigados, todas evidenciam a crescente sofisticação dos delitos sexuais cibernéticos e os desafios enfrentados pelas instituições responsáveis por sua repressão.

De acordo com o modelo investigativo proposto por Casey (2011), uma operação bem-sucedida no campo da criminalidade digital exige cinco elementos fundamentais: (1) identificação precisa do objeto da investigação; (2) preservação e extração segura de provas digitais; (3) análise técnica com suporte forense; (4) correlação contextual dos dados; e (5) apresentação juridicamente válida dos resultados. À luz desses critérios, as três operações apresentaram êxito parcial, com avanços expressivos na análise forense e coleta de evidências, mas ainda enfrentando entraves estruturais nos momentos de cooperação interinstitucional, judicialização e prevenção.

A Operação Terabyte, por exemplo, destacou-se pela utilização de recursos técnicos avançados, como extração de metadados e rastreamento de arquivos multimídia, além de ter adotado metodologia de identificação com base em padrões de conduta digital dos suspeitos. Em contrapartida, sua limitação residiu na dificuldade de articulação entre estados e na lentidão processual para obtenção de mandados judiciais, aspecto já identificado por Souza (2021) como recorrente nas investigações digitais brasileiras.

A Operação Banhammer introduziu um elemento inédito: a apreensão de um adolescente enquanto principal administrador de um grupo de abusadores, o que reforça a tese de que jovens também ocupam posições de comando em redes pedófilas organizadas. O caso demandou atenção específica à responsabilização penal de menores e à perícia de dispositivos utilizados por adolescentes, com desafios éticos, técnicos e jurídicos adicionais. Como observa Caramigo (2017), a atuação de adolescentes em crimes sexuais digitais exige abordagem diferenciada, tanto no processo investigativo quanto na intervenção socioeducativa.

Já a Operação Adolescência Segura ampliou ainda mais o espectro investigativo ao revelar uma organização criminosa multitemática e altamente estruturada, operando em diversos estados e utilizando estratégias de aliciamento psicológico em plataformas criptografadas. A integração entre forças estaduais e federais, com apoio de agências internacionais como a HSI e o NCMEC, conferiu à operação uma dimensão inédita de cooperação internacional. Entretanto, a multiplicidade de crimes e a presença de adolescentes como ofensores centrais revelaram a complexidade das redes contemporâneas de exploração digital — muitas vezes sobrepostas a outras manifestações de violência e ódio online.

Do ponto de vista institucional, observa-se que todas as operações se beneficiaram, em alguma medida, da existência de unidades especializadas, como delegacias de repressão a crimes contra a infância e laboratórios de perícia cibernética. No entanto, persistem gargalos relacionados à formação continuada dos profissionais, à limitação de recursos técnicos e à morosidade judicial, elementos que enfraquecem a efetividade global das ações. A ausência de um protocolo nacional unificado de investigação digital, aliado à desarticulação entre as instâncias de repressão e prevenção, fragiliza o combate de longo prazo, conforme alertam Sobral e Couto (2023).

Além do desempenho técnico, cabe destacar o impacto simbólico das operações. A divulgação midiática de suas etapas e resultados teve papel importante na conscientização social, ainda que também exponha a urgência de políticas públicas mais integradas. A repressão, por si só, é insuficiente para enfrentar um fenômeno cuja origem está no enfraquecimento das redes de proteção social, na erotização precoce e na banalização da violência no ambiente digital.

4- LEGISLAÇÃO E POLÍTICAS PÚBLICAS DE COMBATE AO CRIME CIBERNÉTICO

A complexificação dos delitos cometidos no ambiente digital, sobretudo aqueles relacionados à exploração sexual de crianças e adolescentes, impôs ao Direito Penal contemporâneo o imperativo de repensar seus mecanismos tradicionais à luz das transformações tecnológicas. A arquitetura descentralizada da internet, a volatilidade das redes comunicacionais e o emprego crescente de criptografia dificultam a identificação dos agentes envolvidos, concomitantemente à tipificação jurídica das condutas praticadas. Como resposta inicial a essa mutação do fenômeno

criminal, o ordenamento jurídico brasileiro tem procurado, ainda que de maneira reativa e fragmentada, incorporar dispositivos normativos voltados à repressão de crimes cibernéticos que ameaçam a integridade da infância.

Nesse horizonte normativo, sobressai-se a recente manifestação do Superior Tribunal de Justiça (STJ), que, ao julgar o Tema Repetitivo nº 1.168, em 2023, firmou tese de grande relevância para a persecução penal de infrações sexuais digitais envolvendo menores de idade. A Corte entendeu que os tipos penais de posse (art. 241-B) e divulgação (art. 241-A) de material pornográfico infantojuvenil devem ser considerados autônomos, permitindo a cumulação das sanções mediante o concurso material de crimes (STJ, 2023). Tal posicionamento reconhece, de um lado, a gravidade de cada conduta em sua singularidade; de outro, amplia os horizontes da responsabilização penal e confere maior densidade jurídica à repressão especializada nesse campo.

A decisão do STJ reflete um esforço interpretativo orientado à harmonização dos princípios do Direito Penal com as singularidades da criminalidade digital, marcada por sua complexidade técnica e capilaridade transnacional. Ainda assim, permanecem evidentes as fragilidades normativas que limitam a eficácia estatal no combate à circulação de conteúdos ilícitos na internet. Como assinala Atheniense (2006), a ausência de previsão legal específica para diversas práticas correlatas à cibercriminalidade contribui para a manutenção de esferas de impunidade, dado que o sistema penal brasileiro repele analogias in malam partem. Em outras palavras, condutas que não estejam expressamente tipificadas escorregam pelas frestas da legalidade, mesmo quando sua ofensividade social é incontestável.

Tal constatação encontra respaldo empírico nos dados apresentados pelo relatório *Into the Light – Global Index of Child Sexual Exploitation and Abuse Prevalence* (CHILDLIGHT, 2024), cujos levantamentos em países como Estados Unidos, Reino Unido e Austrália revelam que entre 7% e 11% dos homens adultos entrevistados admitiram ter cometido algum tipo de abuso sexual infantil online. Ainda mais alarmante, parcela significativa desses indivíduos declarou que incorreria em abuso físico caso tivesse certeza de que não seria identificado ou punido. Esses números indicam que a impunidade — ou a percepção de sua prevalência — funciona como elemento estruturante da racionalidade criminosa, estimulando a prática reiterada desses delitos.

À luz desse diagnóstico, é indiscutível a urgência de reformas legislativas que transcendam a mera atualização de dispositivos penais e processuais. Impõe-se, com igual relevância, o fortalecimento de políticas públicas interinstitucionais, capazes de articular, de forma coerente e contínua, estratégias de prevenção, capacitação investigativa e responsabilização penal. Assume papel proeminente, nesse esforço, a atuação coordenada de entidades como o Ministério da Justiça, a Secretaria Nacional do Consumidor (SENACON), o Ministério dos Direitos Humanos e organizações da sociedade civil — notadamente a SaferNet Brasil —, cuja expertise tem contribuído para a construção de uma agenda pública voltada à salvaguarda dos direitos infantojuvenis no ciberespaço.

4.1 Marco legal brasileiro

Entre os instrumentos legislativos mais incisivos na repressão à exploração sexual infantojuvenil no ambiente digital, ressalta-se a Lei nº 13.441/2017, cuja inovação normativa reside na regulamentação da infiltração virtual como técnica especial de investigação. Ao prever a atuação dissimulada de agentes policiais em comunidades online, mediante prévia autorização judicial, o legislador incorporou uma estratégia compatível com a lógica das redes descentralizadas e dos fóruns cifrados, conferindo maior densidade probatória às ações repressivas conduzidas no ciberespaço. Como observa Silva (2022), esse recurso representa um avanço considerável, sobretudo em delitos que envolvem abordagens diretas de aliciamento e manipulação digital, nos quais o flagrante é raramente viável por métodos convencionais.

No eixo normativo central, os artigos 240 e 241 do Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) tipificam condutas relacionadas à produção, armazenamento e disseminação de material pornográfico envolvendo crianças e adolescentes. O art. 240 criminaliza a produção, enquanto o art. 241-A trata da oferta, troca, disponibilização, transmissão, distribuição, publicação ou divulgação, por qualquer meio, de fotografias ou vídeos com cenas de sexo explícito ou pornográficas com menores de 18 anos. Já o art. 241-B pune a posse intencional desse material, mesmo que não haja indícios de sua circulação. Essa ampliação do espectro punitivo visa interromper todas as etapas da cadeia de abuso e reduzir o ciclo de revitimização das crianças envolvidas (Brasil, 1990).

Embora a legislação penal concentre os dispositivos centrais de repressão, o Marco Civil da Internet (Lei nº 12.965/2014) desempenha função complementar decisiva. O artigo 15 estabelece que os provedores de aplicações de internet devem manter os registros de acesso a essas aplicações, sob sigilo e por prazos determinados, para fins de investigação criminal. Conforme destaca Souza (2021), essa obrigação é essencial à rastreabilidade de condutas criminosas em ambientes digitais, especialmente em crimes que envolvem criptografia e ocultação de IP. No entanto, a aplicação do dispositivo enfrenta limitações práticas, como a ausência de padronização entre plataformas e o uso de servidores no exterior.

No plano internacional, o Tratado de Budapeste, ratificado pelo Brasil por meio do Decreto nº 11.491/2023, constitui o principal marco jurídico multilateral no combate aos crimes informáticos. Além de estabelecer padrões mínimos de criminalização — como acesso não autorizado a sistemas, interceptação ilícita e integridade de dados —, o tratado prevê mecanismos de cooperação internacional para a obtenção de provas digitais. A Convenção também trata da pornografia infantil eletrônica, exigindo que os Estados tipifiquem condutas relacionadas à produção, distribuição e posse de material de abuso sexual de crianças (Convenção de Budapeste, 2001). Para Atheniense (2006), a adesão do Brasil representa um avanço relevante, mas sua eficácia dependerá da harmonização dos procedimentos de investigação e do fortalecimento institucional da cooperação transfronteiriça.

Paralelamente, iniciativas internacionais como o Project VIC, utilizado por agências norte-americanas, e as operações da Europol, no âmbito da União Europeia, ilustram a importância da inovação tecnológica como aliada das investigações. O Project VIC, como descreve Casey (2011), funciona como um banco colaborativo internacional de hashes, permitindo a triagem automatizada de arquivos e a identificação de conteúdos já reconhecidos como ilegais. Essa ferramenta reduz o tempo de análise pericial e evita a revitimização pela repetição da exposição dos materiais. A Europol, por sua vez, opera com unidades especializadas que empregam ferramentas de desanonimização, inteligência artificial e rastreamento de criptomoedas vinculadas à circulação de CSAM.

No Brasil, embora não haja uma estrutura institucional semelhante à do Project VIC, operações como a Terabyte, Banhammer e Adolescência Segura demonstram a gradual adoção de técnicas de análise digital avançada, incluindo extração de metadados, engenharia reversa de arquivos e rastreamento de fluxos de informação

entre dispositivos. Como observa Silva (2022), o desafio não está apenas na existência da legislação, mas na capacidade operacional de implementá-la de forma estratégica e contínua.

5- MÉTODOS DE INVESTIGAÇÃO NO AMBIENTE DIGITAL

5.1 Técnicas de identificação digital: rastreamento de linguagem, criptografia e metadados

O acesso precoce e massivo de crianças e adolescentes à internet tem reformulado profundamente os desafios enfrentados por instituições encarregadas da repressão a crimes digitais. A pesquisa TIC Kids Online Brasil 2024 revela que 93% dos brasileiros entre 9 e 17 anos estão conectados, sendo que 98% utilizam o celular como dispositivo principal, e 81% já possuem um aparelho próprio (Lima, 2024). Segundo a autora, os números não apenas evidenciam a ubiquidade do ambiente virtual no cotidiano infantojuvenil, como também alertam para a exposição contínua dessa faixa etária a riscos como aliciamento, violência simbólica e exploração sexual em plataformas de mensagens e redes sociais — preferidas por 76% dos entrevistados.

Dadas as circunstâncias observadas, a investigação criminal exige o emprego de métodos altamente especializados para a identificação e responsabilização de agentes envolvidos em crimes sexuais digitais. Entre as técnicas mais relevantes, destacam-se: o rastreamento linguístico, que permite a identificação de padrões de comunicação codificada; a análise de criptografia, que busca formas legais e técnicas de superar o bloqueio de acesso aos conteúdos armazenados; e a extração de metadados, essencial para a reconstrução de trajetórias digitais e a validação da cadeia de custódia probatória.

Além de sua relevância estatística, a imersão infantojuvenil nas redes digitais impõe uma reformulação dos métodos investigativos. Para responder aos desafios impostos pela disseminação de conteúdo ilícito em ambientes criptografados, descentralizados e interativos, a atuação policial deve se apoiar em três frentes principais de análise digital: linguagem, criptografia e metadados.

O rastreamento de linguagem, também denominado *linguistic profiling*, consiste na identificação de padrões lexicais, sintáticos e discursivos recorrentes em textos compartilhados em redes sociais, fóruns, plataformas de mensagem e servidores anônimos. Criminosos frequentemente utilizam vocabulário cifrado ou siglas

específicas para ocultar práticas ilegais, como a comercialização de material pornográfico infantil ou o aliciamento de vítimas. Conforme ressalta Casey (2011), o monitoramento da linguagem favorece tanto a detecção de conteúdos suspeitos quanto o reconhecimento de traços estilísticos característicos de indivíduos reincidentes, funcionando como uma autêntica “impressão linguística” digital. Softwares baseados em inteligência artificial e aprendizado de máquina têm sido empregados para reconhecer automaticamente padrões semânticos que indicam material de risco, mesmo em mensagens criptografadas ou parcialmente ocultas.

A criptografia, por sua natureza, representa tanto uma proteção legítima à privacidade quanto uma barreira significativa à investigação criminal. Aplicativos com criptografia ponta a ponta impedem que mesmo as plataformas intermediárias tenham acesso ao conteúdo das comunicações. No entanto, a atuação forense tem evoluído para lidar com essa restrição, recorrendo à análise de dados armazenados localmente nos dispositivos, à recuperação de cópias de segurança em nuvens não criptografadas e à extração de fragmentos de comunicação por meio de engenharia reversa. Como observa Souza (2021), a perícia digital precisa transitar de um modelo baseado na interceptação direta para abordagens indiretas, como a análise de logs de atividade, rastreamento de redes utilizadas e vinculação de perfis por meio de evidências associadas — como localização, número de série de dispositivos ou conexões simultâneas em múltiplas plataformas.

A análise de metadados, por fim, constitui uma das ferramentas mais eficazes para contextualizar o conteúdo digital apreendido. Cada arquivo digital — especialmente imagens e vídeos — carrega consigo informações técnicas invisíveis a usuários comuns, como data de criação, coordenadas geográficas, tipo de dispositivo utilizado e histórico de modificações. Essas informações são fundamentais para estabelecer a autenticidade, autoria e temporalidade dos arquivos, e podem ser cruciais para identificar redes de compartilhamento. Como ressalta Caramigo (2017), os metadados equivalem, no ambiente digital, às evidências materiais em investigações tradicionais, sendo indispensáveis para a formação de uma cadeia probatória robusta e juridicamente admissível.

A aplicação dessas técnicas foi observada em operações como a Terabyte, na qual a perícia conseguiu vincular imagens de abuso a determinados dispositivos por meio da extração de metadados e análise de nomes de arquivos correlacionados. Já nas operações Banhammer e Adolescência Segura, o rastreamento linguístico e a

análise de grupos em plataformas como Telegram e Discord revelaram padrões de comunicação organizados, uso de linguagens cifradas e categorização sistemática de conteúdo ilícito, o que permitiu constatar não apenas a sofisticação dos agentes criminosos, mas igualmente a resiliência investigativa frente aos obstáculos técnicos impostos pelo ambiente digital.

6- A DEEP WEB E A DARK WEB NO CONTEXTO DA PORNOGRAFIA INFANTIL

6.1 Características e desafios operacionais

A sofisticação técnica das redes de abuso sexual infantil que operam na dark web impõe desafios inéditos ao processo penal contemporâneo. A operação internacional que resultou no desmantelamento da plataforma Kidflix — ambiente de streaming oculto com mais de 1,8 milhão de usuários ativos em 38 países — é um retrato brutal da dimensão transnacional e estrutural dessa criminalidade. A plataforma comercializava, mediante pagamento em criptomoedas, mais de 91 mil vídeos de abuso, somando 6.288 horas de gravação, com publicações constantes e automatizadas (Cartacapital, 2025).

A partir desse caso, é evidente que os obstáculos à responsabilização penal não estão apenas na complexidade técnica da coleta de provas digitais, mas sobretudo na forma como essas redes se articulam para contornar os marcos legais vigentes. A criptografia de ponta, o uso de servidores distribuídos, o anonimato garantido por navegadores como Tor e o emprego de blockchain, também chamado de “cadeia de blocos” de dados interligados e criptografados, usado para ocultar transações transformando-as em repressivas, dependentes de alta especialização forense e de uma cooperatividade internacional eficiente e imediata.

“A Dark Web representa um território digital deliberadamente oculto, construído para impedir o rastreamento de seus usuários e proteger atividades que não resistiriam à luz da legalidade” (Barreto, 2021, p. 39). Essa definição, proposta pelo autor, revela com precisão a complexidade do ambiente virtual onde redes criminosas operam com sofisticação e relativo conforto, especialmente no que se refere à disseminação de material de abuso sexual infantil. Tais ambientes não apenas dificultam o monitoramento convencional, como desafiam diretamente os mecanismos legais e institucionais de repressão.

Para além da internet superficial – acessada por navegadores comuns e indexada por buscadores tradicionais –, a chamada Deep Web abriga um conjunto

extenso de informações não visíveis aos mecanismos de busca, como bancos de dados, arquivos institucionais e fóruns restritos. No interior desta camada encontra-se a Dark Web, cuja arquitetura técnica, acessível por softwares como o Tor, foi desenvolvida para garantir o anonimato, a criptografia e a evasão de rastros digitais. Esses elementos, embora legítimos em determinadas finalidades, têm sido instrumentalizados por redes organizadas para viabilizar a circulação de conteúdos ilícitos de maneira encoberta e persistente.

No campo da pornografia infantil, a Dark Web tornou-se um espaço estratégico de articulação criminosa. Fóruns, marketplace (comércio virtual) e canais de distribuição segmentam conteúdos, classificam materiais por faixas etárias e frequentemente integram sistemas de recompensa para usuários mais ativos. Como explica Barreto (2021), a criminalidade nesses ambientes opera com divisão de funções, mecanismos de validação interna e uso recorrente de criptomoedas, dificultando tanto o rastreamento financeiro quanto a identificação dos envolvidos. Trata-se de uma lógica descentralizada, porém altamente estruturada, que se reconfigura com agilidade diante de qualquer intervenção estatal.

Sob a ótica técnica, os desafios operacionais são numerosos. A investigação nesses espaços exige o uso de ferramentas forenses avançadas, como espelhamento de servidores ocultos, análise de logs criptografados, rastreamento de transações em blockchain e infiltração digital por meio de perfis disfarçados. A volatilidade dos dados, aliada ao tempo reduzido de permanência de páginas e à efemeridade das conexões, requer que o trabalho pericial seja ágil, contínuo e respaldado por expertise qualificada. Conforme observa Souza (2021), qualquer retardo pode inviabilizar a preservação de evidências essenciais à responsabilização penal dos ofensores.

Sob o enfoque jurídico, a dificuldade reside na harmonização entre o dinamismo da criminalidade digital e a rigidez da legislação vigente. A jurisprudência nacional ainda oferece respostas limitadas quanto à admissibilidade de provas obtidas em ambientes não convencionais, e a ausência de regulamentação específica para ações em plataformas criptografadas contribui para um ambiente de insegurança jurídica. Como adverte Caramigo (2017), o descompasso entre a sofisticação tecnológica dos ofensores e a morosidade das instituições de controle compromete a efetividade da repressão penal, favorecendo a perpetuação do anonimato como instrumento de impunidade.

Além das questões normativas, soma-se a dificuldade de localização dos servidores utilizados para hospedar conteúdos ilícitos. Muitos estão situados em países com baixa cooperação jurídica internacional ou sem arcabouço legal eficaz, o que exige atuação coordenada entre agências estatais por meio de tratados multilaterais. A Convenção de Budapeste, embora ratificada pelo Brasil, ainda carece de efetiva implementação operacional, limitando seu alcance nos casos urgentes e transnacionais.

Compreender, portanto, a estrutura, os fluxos e os bloqueios operacionais da Deep e da Dark Web configura-se como um imperativo estratégico para reorientar a atuação investigativa e normativa do Estado. A criminalidade sexual nesses espaços demanda respostas articuladas, baseadas em tecnologia, inteligência e cooperação internacional. Sem tais mecanismos, a intervenção estatal permanece fragmentada, enquanto os ofensores continuam a explorar as brechas da invisibilidade digital.

6.2 Tecnologias de desanonimização: Bitcoin, Tor e quebras de sigilo

“Investigar a criminalidade na dark web exige do investigador não apenas conhecimento técnico aprofundado, mas a compreensão de que está lidando com estruturas criminosas descentralizadas, resilientes e altamente capacitadas” (Barreto, 2021, p. 105). Essa advertência sintetiza a urgência do aperfeiçoamento metodológico das práticas investigativas frente à crescente sofisticação dos delitos cometidos em ambientes criptografados e anonimizados.

Dentre os mecanismos mais explorados por redes criminosas que atuam na disseminação de pornografia infantil online, destacam-se o navegador Tor, utilizado para acessar a camada oculta da internet, e as criptomoedas, como o Bitcoin, que permitem a realização de transações pseudônimas. Embora essas ferramentas tenham sido inicialmente concebidas para proteger a privacidade dos usuários, seu uso indevido tem servido como escudo para práticas ilícitas. Investigações avançadas, no entanto, têm conseguido explorar brechas operacionais, como a correlação temporal entre atividades, metadados de tráfego e falhas de configuração, capazes de permitir a reidentificação dos envolvidos (Furneaux, 2018, p. 228–231).

No que se refere às movimentações financeiras, a utilização do Bitcoin proporciona apenas uma aparência de invisibilidade. Para Grzywotz (2019, p. 99), a criptomoeda “não é anônima, mas confere um grau de privacidade superior ao da moeda estatal, com o contraponto de que suas transações permanecem

permanentemente registradas em um grande livro razão público – a blockchain". A partir disso, adquire viabilidade a aplicação de técnicas de blockchain forensics, como as descritas no relatório da Chainalysis (2023, p. 54), que viabilizam a identificação de padrões de movimentação financeira vinculados a crimes cibernéticos, inclusive os de natureza sexual contra crianças.

De forma complementar, no Manual do Ministério Público Federal (2023, p. 62) reconhece que a eficácia dessas investigações depende da integração entre dados financeiros e informações telemáticas. A análise coordenada de IPs de acesso, e-mails cadastrados, dispositivos conectados, registros de login e informações bancárias pode viabilizar a individualização precisa dos investigados.

Contudo, para que essas medidas sejam juridicamente válidas, exige-se respeito estrito às garantias constitucionais, em especial à legalidade e à proporcionalidade.

É nesse ponto que se insere o debate sobre a legitimidade das medidas de desanonimização digital. De acordo com Gleizer, Montenegro e Viana (2021, p. 116), as técnicas ocultas de investigação reduzem as possibilidades de reação jurídica do afetado, razão pela qual devem estar submetidas ao crivo da reserva de jurisdição. Nesse enfoque, Quito (2021) argumenta que o acesso a comunicações e dados armazenados só se justifica quando lastreado em decisão judicial fundamentada, proporcional e indispensável à persecução penal. Para Jorge (2021, p. 17), a investigação criminal tecnológica exige, acima de tudo, um novo paradigma mental por parte dos operadores do Direito, capaz de integrar ferramentas digitais sem abdicar do rigor normativo e da segurança jurídica.

A adoção dessas ferramentas tem se mostrado frutífera em diversas operações, a exemplo da Adolescência Segura, onde o cruzamento entre dados telemáticos e transações criptografadas permitiu a identificação dos principais articuladores do grupo criminoso. Como ressalta Cintra (2020, p. 183), o êxito da investigação digital está diretamente vinculado à articulação entre inteligência forense, expertise em ativos virtuais e estruturação de parcerias interinstitucionais, tanto em âmbito nacional quanto internacional.

À luz dessas considerações, observa-se que as tecnologias de desanonimização desempenham papel estratégico na contenção da criminalidade sexual digital. Seu uso, pautado por critérios técnicos e fundamentos jurídicos robustos, revela-se compatível com o Estado Democrático de Direito, sobretudo

quando se trata de proteger vítimas hipervulneráveis diante de redes transnacionais articuladas em ambientes projetados para a invisibilidade.

7- POLÍTICAS DE PREVENÇÃO E CONSCIENTIZAÇÃO

Em abril de 2025, o Ministério da Justiça e Segurança Pública anunciou o lançamento do programa “Crescer em Paz”, concebido com a finalidade de aprimorar os mecanismos de proteção digital voltados a crianças e adolescentes. Dentre as diretrizes previstas, converge como aspecto relevante a proposta de desenvolvimento de um aplicativo de controle parental, voltado à restrição automatizada de conteúdos e serviços digitais com base na classificação indicativa etária, sobretudo em plataformas amplamente utilizadas, como TikTok, Instagram e YouTube. A iniciativa contempla o uso de geradores de tokens personalizados, vinculados à data de nascimento informada no cadastro do usuário, bem como a possibilidade de implementação de sistemas de reconhecimento biométrico, com o objetivo de tornar efetiva a limitação de acesso por faixa. Em concordância com Amato (2025).

Para viabilizar a operacionalização técnica e normativa dessa política, foi instituída, por meio de portaria, uma comissão interinstitucional responsável pela definição de padrões de verificação etária online, inspirada em experiências internacionais, como a da Índia. Tal medida visa assegurar que o acesso ao ambiente virtual ocorra em consonância com o estágio de desenvolvimento do usuário, evitando a exposição precoce a conteúdos de natureza sexual, violenta, discriminatória ou economicamente nociva — como publicidade de bebidas alcoólicas, cigarros e jogos de aposta eletrônica.

Essa política pública representa uma inflexão paradigmática no enfrentamento da violência sexual digital, ao reconhecer que ações preventivas estruturadas devem preceder e complementar a atuação repressiva estatal. Em conformidade com os ditames do artigo 227 da Constituição Federal e do artigo 4º do Estatuto da Criança e do Adolescente (ECA), é incumbência prioritária do Estado, da família e da sociedade a garantia da dignidade, do desenvolvimento pleno e da proteção integral do público infantojuvenil, inclusive no ambiente digital (Brasil, 1990).

Sob tal perspectiva, sobressai a atuação da SaferNet Brasil, organização da sociedade civil responsável pela coordenação da Central Nacional de Denúncias de Crimes Cibernéticos, bem como pela execução de projetos educativos voltados à alfabetização digital e à promoção da cidadania online. Em colaboração com o

Ministério Público Federal e o Comitê Gestor da Internet no Brasil, a instituição tem promovido campanhas de conscientização voltadas à empatia, à segurança da informação e à prevenção do aliciamento virtual (Safernet, 2024).

A essas iniciativas somam-se importantes instrumentos institucionais de proteção, como o Disque 100, o Programa Escuta Protegida e o PPCAAM, os quais integram a rede de acolhimento e resposta em casos de risco ou violação de direitos. Ademais, campanhas como “Não Se Cale”, promovida pelo Governo Federal, e os pactos interinstitucionais firmados no âmbito do Conselho Nacional de Justiça, como o Pacto Nacional pela Primeira Infância, reforçam o compromisso sistêmico com a proteção de crianças e adolescentes no ecossistema digital.

Não obstante os avanços implementados, subsistem limitações estruturais que restringem a eficácia dessas políticas. A descontinuidade das campanhas educativas, a insuficiência de investimentos em capacitação profissional e a ausência de mecanismos unificados de monitoramento comprometem a consolidação de uma cultura de prevenção digital robusta. Nesse sentido, Barreto (2021) adverte que “a prevenção no ciberespaço demanda uma política pública contínua, inteligente e tecnicamente orientada, sob pena de perpetuar respostas fragmentadas e tardias”.

À vista desse panorama, é imperativo adotar uma percepção sistêmica, na qual a proteção de crianças e adolescentes ultrapasse o discurso normativo e se converta em políticas públicas baseadas em evidências, ancoradas em estratégias pedagógicas, e sustentadas por estruturas institucionais integradas.

A proteção da infância no ambiente digital não se realiza por meio de ações pontuais, mas por meio de um compromisso institucional contínuo, no qual Estado, sociedade civil, setor privado e comunidade escolar compartilhem responsabilidades na promoção dos direitos fundamentais das crianças e adolescentes em um mundo hiperconectado. Tal comprometimento revela-se ainda mais urgente diante da natureza silenciosa e insidiosa dos crimes sexuais digitais, que, frequentemente, ocorrem sem testemunhas, sem marcas físicas imediatas e atingem vítimas que não possuem recursos emocionais, cognitivos ou sociais para compreender, reagir ou denunciar os abusadores. Como adverte a UNICEF (2022, p. 18), “a violência sexual digital contra crianças é frequentemente invisível, silenciosa e carregada de culpa — fatores que inibem a denúncia e favorecem a impunidade. Em muitos casos, as vítimas sequer compreendem que foram violadas”. Nesse cenário de extrema vulnerabilidade, a prevenção deve ser entendida não como uma política acessória,

mas como uma forma de justiça antecipada, voltada a romper os ciclos de violência antes mesmo de sua eclosão.

7.1 Estudos de casos emblemáticos e suas lições

A repressão qualificada à pornografia infantil online no Brasil encontra na Operação Luz na Infância um de seus marcos institucionais mais relevantes. Desde sua deflagração em 2017 pelo Ministério da Justiça e Segurança Pública, em parceria com as polícias civis estaduais e organismos internacionais como a INTERPOL e o Homeland Security Investigations (HSI), a operação tornou-se referência na mobilização interestadual e transnacional de recursos humanos, técnicos e estratégicos voltados ao enfrentamento da exploração sexual de crianças e adolescentes em ambiente digital.

Em sua décima fase, realizada em março de 2023, a operação mobilizou 25 unidades da Federação, cumpriu 163 mandados de busca e apreensão e resultou na prisão em flagrante de 32 indivíduos. As diligências foram viabilizadas por meio do trabalho de inteligência cibernética conduzido pelo Laboratório de Operações Cibernéticas (Ciberlab), a partir da análise de evidências digitais e informações compartilhadas com provedores internacionais. O volume expressivo de materiais apreendidos reforça não apenas a magnitude da rede criminosa desmantelada, como também a relevância da articulação técnica interinstitucional na produção de resultados operacionais eficazes (MJSP, 2023).

Sob a perspectiva jurídico-social, a operação transcende seu caráter meramente repressivo, na medida em que impulsionou a construção de protocolos especializados de investigação digital, padronização de rotinas forenses e integração normativa com os tratados internacionais de proteção da infância, como a Convenção de Budapeste. Além disso, provocou o amadurecimento da agenda pública sobre os riscos cibernéticos que atingem populações infantojuvenis em um cenário de conectividade plena e mediação algorítmica das interações.

A visibilidade pública conferida à operação também exerceu papel pedagógico, ao tensionar o silêncio social que, historicamente, encobre crimes sexuais digitais praticados contra crianças e adolescentes. Em termos simbólicos, a disseminação da operação pela mídia reforçou a dissuasão penal, aumentou a percepção de risco entre ofensores potenciais e favoreceu o fortalecimento de canais de denúncia. Conforme observa Seto (2013, p. 49), “a repressão eficaz, quando acompanhada de ampla

conscientização, pode exercer função preventiva indireta, ao restringir o acesso a material ilícito e desencorajar o ingresso em redes de abuso".

Paralelamente, a Operação Luz na Infância revelou a interseccionalidade entre exploração sexual online e outras práticas delituosas que instrumentalizam os espaços digitais, como a produção de deepfakes (conteúdos falsos), a manipulação de dados, o uso de criptomoedas para ocultação de fluxos financeiros e a migração de conteúdos ilícitos para a deep e dark web — elementos que demandam constante atualização metodológica e tecnológica por parte das autoridades públicas.

Diante disso, resulta claro que o êxito da operação decorreu não apenas da repressão em si, mas da capacidade do Estado de articular inteligência, cooperação internacional e investimento institucional contínuo, transformando a repressão em ação estratégica integrada. A consolidação de boas práticas nesse contexto demonstra que a resposta à pornografia infantil online não pode ser fragmentária nem episódica: deve integrar prevenção, responsabilização efetiva e um compromisso sistêmico com os direitos humanos de crianças e adolescentes.

Em síntese, a Operação Luz na Infância consolidou-se como paradigma de atuação estatal articulada, revelando que o enfrentamento à exploração sexual digital demanda mais do que perícia investigativa: exige um modelo de governança pública intersetorial, orientado por evidências, compromissado com a proteção integral da infância e continuamente adaptado à evolução das ameaças digitais.

8- CONSIDERAÇÕES FINAIS

A pornografia infantil na internet configura-se como uma das formas mais perversas e sofisticadas de violação de direitos humanos no século XXI. Seu enraizamento em redes transnacionais, sua circulação silenciosa por canais criptografados e seu consumo cada vez mais precoce, inclusive por adolescentes, desafiam as fronteiras tradicionais do Direito Penal, da investigação criminal e das políticas públicas de proteção infantojuvenil. Longe de ser um fenômeno isolado ou episódico, trata-se de uma estrutura criminosa que opera de modo contínuo, adaptável e invisível, exigindo respostas igualmente articuladas, permanentes e tecnologicamente adequadas.

A análise realizada neste artigo permitiu concluir que, embora o ordenamento jurídico brasileiro disponha de instrumentos normativos relevantes — como o Estatuto da Criança e do Adolescente, a Lei nº 13.441/2017 e o Marco Civil da Internet —,

ainda persistem fragilidades que comprometem a eficácia da repressão penal. Entre os principais obstáculos identificados, destacam-se a lentidão nos processos de cooperação internacional, as lacunas na regulação de plataformas digitais, a limitada responsabilização dos intermediários tecnológicos e as dificuldades técnicas para a identificação de autores ocultos por sistemas de anonimização e transações criptografadas.

As três operações policiais — Terabyte, Banhammer e Adolescência Segura —, somadas à emblemática Operação Luz na Infância, demonstram a importância estratégica de ações repressivas coordenadas, sustentadas por perícia digital avançada e cooperação interinstitucional eficaz. No entanto, os limites evidenciados pelas próprias operações indicam que a repressão isolada, desvinculada de estratégias preventivas e educativas, mostra-se insuficiente frente à dimensão e à complexidade do fenômeno. A proteção infantojuvenil no ambiente digital exige, portanto, mais do que normatização penal: requer políticas públicas intersetoriais, integradas e voltadas à promoção da cidadania digital.

Adicionalmente, impõe-se a adoção de medidas educativas estruturadas, capazes de articular normas já existentes com estratégias pedagógicas eficazes. Embora a proibição do uso de celulares em salas de aula esteja formalmente instituída, sua eficácia depende da implementação rigorosa e da inserção dessa restrição em um contexto mais amplo de formação para o uso ético das tecnologias. A esse respeito, torna-se imprescindível a inclusão sistemática de conteúdos sobre ética digital, segurança informacional e cidadania online no currículo escolar, bem como o investimento contínuo em campanhas de sensibilização midiática voltadas a pais, alunos e profissionais da educação.

Paralelamente, recomenda-se a alocação de recursos públicos específicos para financiar projetos sociais e educacionais voltados à prevenção da exploração sexual infantojuvenil no ambiente virtual, assegurando uma resposta mais abrangente e proativa por parte do Estado. Programas como o “Crescer em Paz”, que propõem ferramentas de verificação etária e limitação de acesso a conteúdos inapropriados, apontam caminhos promissores — desde que acompanhados de fiscalização efetiva e engajamento das plataformas digitais.

A experiência internacional evidencia que o enfrentamento eficaz da pornografia infantil na internet pressupõe a combinação entre repressão penal especializada, fiscalização tecnológica, responsabilização institucional e prevenção

social qualificada. Superar a fragmentação das ações e consolidar uma lógica de proteção integral contínua é um imperativo da justiça e da humanidade.

Em tempos marcados pela mercantilização dos dados, pela opacidade algorítmica e pela erosão de limites éticos no ciberespaço, proteger a infância não é apenas uma obrigação jurídica — é, sobretudo, um compromisso político com a dignidade e a integridade da vida em sua fase mais vulnerável.

AGRADECIMENTOS

Primeiramente a Deus, por me conceder a oportunidade de cursar o Direito, por ter sido meu refúgio e força nos momentos mais desafiadores. Sua presença me sustentou com coragem, discernimento e serenidade ao longo desta trajetória acadêmica.

Aos meus pais, Cristina e Anderson, por todo amor, exemplo e generosidade. Agradeço pela dádiva da vida, pela educação baseada em valores sólidos e pelo apoio incansável, mesmo nos momentos em que as renúncias foram invisíveis aos olhos. Obrigada por nunca hesitarem em me amparar.

Ao meu companheiro, Luís Felipe, pela parceria. Sua paciência, cuidado e comprometimento tornaram leve até os dias mais difíceis. Obrigada por estar ao meu lado em cada etapa, dividindo o peso da jornada e celebrando cada pequena conquista com o coração inteiro.

Ao professor Sandro Lúcio Dezan, meu orientador, agradeço pela confiança, pela orientação atenta e pelas provocações intelectuais que ampliaram a profundidade desta pesquisa. Sua generosidade acadêmica foi essencial para que este artigo alcançasse consistência teórica e relevância prática.

Ao Doutor Alexandre, por seu papel fundamental desde os primeiros passos deste trabalho. Sua ajuda na delimitação do tema, nas indicações bibliográficas e nas orientações metodológicas foi decisiva para o amadurecimento da pesquisa. Sou imensamente grata por sua escuta generosa e comprometimento com a qualidade acadêmica deste estudo.

Dedico este artigo às crianças e adolescentes cujos direitos são violados em silêncio no ambiente digital. Que este estudo represente uma voz que ecoa por sua proteção e dignidade.

REFERÊNCIAS

AMATO, Fábio. Ministério planeja criar aplicativo para restringir acesso de crianças a conteúdo inadequado na internet. TV Globo, Brasília, 10 abr. 2025. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2025/04/15/policia-civil-do-rj-deflagra-operacao-adolescencia-segura.ghtml. Acesso em: abr. 2025.

ATHENIENSE, Omar Kaminski. Direito e internet: o impacto da rede mundial de computadores sobre o direito. Câmara dos Deputados, 2006.

BARRETO, Alessandro Gonçalves. Investigação criminal na deep web. São Paulo: Saraiva, 2021.

BRASIL. Estatuto da Criança e do Adolescente (ECA). Lei nº 8.069, de 13 de julho de 1990. Diário Oficial da União: seção 1, Brasília, DF, 16 jul. 1990.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.441, de 8 de maio de 2017. Altera o Estatuto da Criança e do Adolescente para dispor sobre a infiltração virtual. Diário Oficial da União: seção 1, Brasília, DF, 9 maio 2017.

CARAMIGO, Denis. Pedofilia e pornografia infantil na internet: uma análise criminal. Curitiba: Juruá, 2017.

CASEY, Eoghan. Digital evidence and computer crime: forensic science, computers and the internet. 3. ed. San Diego: Elsevier, 2011.

CHAINALYSIS. Crypto crime report. New York: Chainalysis, 2023.

CHILDLIGHT. Into the light – Global index of child sexual exploitation and abuse prevalence. Durham: WeProtect Global Alliance, 2024.

CINTRA, Pedro. Cibercrimes e investigação digital. São Paulo: Atlas, 2020.

CONVENÇÃO DE BUDAPESTE. Convenção sobre o crime cibernético. Budapeste, 2001.

FURNEAUX, Nick. Investigating cryptocurrencies: understanding, extracting, and analyzing blockchain evidence. New Jersey: Wiley, 2018.

G1. Polícia deflagra operação contra grupo que promovia crimes em plataformas digitais. G1, Rio de Janeiro, 2025. Disponível em: https://g1.globo.com. Acesso em: abr. 2025.

GLEIZER, Rafael; MONTENEGRO, Bruna; VIANA, Carlos. A desanonimização na investigação criminal digital. Revista Brasileira de Ciências Criminais, São Paulo, n. 159, p. 112–131, 2021.

GRZYWOTZ, Carolin. Bitcoin and privacy: a forensic perspective. Journal of Financial Crime, v. 26, n. 1, p. 92–104, 2019.

JORGE, Felipe. O novo paradigma da persecução penal digital. Revista de Direito Penal Contemporâneo, São Paulo, v. 7, n. 2, p. 15–33, 2021.

LIMA, Célia Fernanda. Crianças e adolescentes usam mais a internet pelo próprio celular, diz TIC Kids 2024. Lunetas, 23 out. 2024. Disponível em: https://lunetas.com.br/tic-kids-online-2024. Acesso em: mar. 2025.

LYON, David. Vigilância na sociedade: questões e controvérsias. São Paulo: Edições Loyola, 2007.

MJSP. Operação Luz na Infância: 10ª fase tem atuação em 25 estados e no DF. Brasília: Ministério da Justiça e Segurança Pública, 2023.

MPF. Manual de atuação em crimes cibernéticos. Brasília: Ministério Público Federal, 2023.

PCDF. Notícias institucionais: Operações Terabyte e Banhammer. Brasília: Polícia Civil do Distrito Federal, 2024. Disponível em: https://www.pcdf.df.gov.br. Acesso em: abr. 2025.

QUITO, Rafael. Acesso a dados digitais e direitos fundamentais. Revista de Direito Constitucional, São Paulo, v. 29, n. 3, p. 77–98, 2021.

SAFERNET BRASIL. Relatório anual 2024: dados sobre denúncias de crimes e violações aos direitos humanos na internet. São Paulo: SaferNet, 2024a.

SAFERNET BRASIL. Relatório estatístico 2023. São Paulo: SaferNet, 2024b.

SETO, Michael C. Pedophilia and sexual offending against children: theory, assessment, and intervention. Washington, DC: American Psychological Association, 2009.

SILVA, Tainá da Costa. Pornografia infantil e direito penal: limites e possibilidades da legislação brasileira. São Paulo: Saraiva, 2022.

SOBRAL, Ana Paula; COUTO, Fernando. Criminalidade digital e resposta institucional. Revista Brasileira de Políticas Públicas, Brasília, v. 13, n. 1, p. 233–251, 2023.

SOUZA, Rodrigo de Oliveira. Crimes digitais e investigação criminal no Brasil. Brasília: Thoth, 2021.

STJ (Brasil). Tema Repetitivo nº 1.168. Brasília: Superior Tribunal de Justiça, 2023.

UNICEF. Reimaginar a proteção infantil na era digital: desafios e oportunidades para combater a exploração sexual online. Nova Iorque: Fundo das Nações Unidas para a Infância, 2022.