

KAYLAINE DE OLIVEIRA TONETTE
CLEITON DELEPRANI DO NASCIMENTO

**A INFILTRAÇÃO POLICIAL VIRTUAL COMO INSTRUMENTO DE
ENFRENTAMENTO À EXPLORAÇÃO SEXUAL DE CRIANÇAS E
ADOLESCENTES NA INTERNET: LIMITES LEGAIS E DESAFIOS PROBATÓRIOS**

Artigo Científico apresentado a Afya
Centro Universitário de Ji-Paraná – Afya Ji-
Paraná, para obtenção de nota na
disciplina Trabalho de Conclusão de Curso
– TCC, sob orientação da Profa. Esp.
Valdinéia Moretti Andrade.

Ji-Paraná
2026

Dados Internacionais de Catalogação na Publicação - CIP

T664i Tonette, Kaylaine de Oliveira.

A infiltração policial virtual como instrumento de enfrentamento à exploração sexual de crianças e adolescentes na internet: limites legais e desafios probatórios. / Kaylaine de Oliveira Tonette; Cleiton Deleprani do Nascimento. – Ji-Paraná, 2026.

29 p.

Artigo Científico (Curso de Direito) – Afya Centro Universitário de Ji-Paraná, 2026.

Orientadora: Prof.^a Esp. Valdineia Moretti Andrade.

1. Infiltração Policial Virtual. 2. Exploração Sexual Infantojuvenil. 3. Crimes Cibernéticos. 4. Prova Digital. 5. Cadeia de Custódia I. Nascimento, Cleiton Deleprani do II. Andrade, Valdineia Moretti. III. Título.

CDU 364.63-053.6:681.51

A INFILTRAÇÃO POLICIAL VIRTUAL COMO INSTRUMENTO DE ENFRENTAMENTO À EXPLORAÇÃO SEXUAL DE CRIANÇAS E ADOLESCENTES NA INTERNET: LIMITES LEGAIS E DESAFIOS PROBATÓRIOS

Kaylaine de Oliveira Tonette¹

Cleiton Deleprani do Nascimento²

Valdinéia Moretti Andrade³

Resumo

O crescente uso da internet por crianças e adolescentes transformou seus modos de interação, estudo e comunicação, mas também ampliou significativamente os riscos relacionados à exploração sexual no ambiente digital. A combinação entre anonimato, perfis falsos e ferramentas de ocultação favoreceu a prática de delitos que violam a dignidade sexual infantojuvenil, impondo desafios cada vez mais complexos ao Direito Penal e ao sistema de proteção integral previsto no Estatuto da Criança e do Adolescente. Diante da insuficiência dos métodos tradicionais de investigação para acompanhar a dinâmica da criminalidade cibernética, a infiltração policial virtual, prevista na Lei nº 13.441/2017, surgiu como técnica essencial para identificar autores, coletar provas e interromper práticas ilícitas. Contudo, sua aplicação envolve importantes questões constitucionais e legais, especialmente no que se refere à intimidade, à privacidade, à inviolabilidade das comunicações e à preservação da cadeia de custódia da prova digital. Este artigo analisou a infiltração policial virtual como instrumento de enfrentamento à exploração sexual infantojuvenil na internet, destacando seus fundamentos normativos, seus limites jurídicos e os desafios probatórios inerentes ao ambiente digital. A reflexão desenvolvida buscou oferecer

¹Acadêmica do 8º período do Curso de Direito, Afya Centro Universitário de Ji-Paraná, Ji-Paraná, RO, Brasil. E-mail: kaylainetonette@gmail.com;

²Acadêmico do 8º período do Curso de Direito, Afya Centro Universitário de Ji-Paraná, Ji-Paraná, RO, Brasil. E-mail: Delepranicleiton@gmail.com;

³Professora orientadora, especialista em Direito Processual Civil pela Universidade do Sul de Santa Catarina, 2009; pós-graduada em Direito e Processo do Trabalho pela Universidade Cândido Mende, 2006; pós-graduada em Direito Público pela Universidade Anhanguera-UNIDERP, 2012; graduada em Ciências Contábeis pela Universidade Federal de Rondônia, 1995; bacharel em Direito pela Universidade Luterana do Brasil, 2004. E-mail: valdineia.andrade@afya.com.br.

compreensão crítica e atualizada acerca da utilização dessa técnica no contexto contemporâneo da criminalidade virtual.

Palavras-chave: Infiltração Policial Virtual. Exploração Sexual Infantojuvenil. Crimes Cibernéticos. Prova Digital. Cadeia de Custódia.

VIRTUAL POLICE INFILTRATION AS A TOOL FOR COMBATING THE SEXUAL EXPLOITATION OF CHILDREN AND ADOLESCENTS ON THE INTERNET: LEGAL LIMITS AND EVIDENTIARY CHALLENGES

Abstract

The increasing use of the internet by children and adolescents has transformed their modes of interaction, study, and communication, but has also significantly amplified the risks related to sexual exploitation in the digital environment. The combination of anonymity, fake profiles, and concealment tools has favored the practice of crimes that violate the sexual dignity of children and adolescents, imposing increasingly complex challenges on Criminal Law and the comprehensive protection system provided for in the Statute of Children and Adolescents. Given the inadequacy of traditional investigation methods to keep pace with the dynamics of cybercrime, virtual police infiltration, provided for in Law No. 13.441/2017, has emerged as an essential technique for identifying perpetrators, collecting evidence, and interrupting illicit practices. However, its application involves important constitutional and legal issues, especially regarding intimacy, privacy, the inviolability of communications, and the preservation of the chain of custody of digital evidence. This article analyzed virtual police infiltration as a tool to combat child sexual exploitation on the internet, highlighting its normative foundations, its legal limits, and the evidentiary challenges inherent to the digital environment. The reflection developed sought to offer a critical and up-to-date understanding of the use of this technique in the contemporary context of cybercrime.

Keywords: Virtual Police Infiltration. Child Sexual Exploitation. Cybercrimes. Digital Evidence. Chain of Custody.

1. Introdução

O uso cada vez mais intenso da internet por crianças e adolescentes tem transformado profundamente a forma como esse público interage, estuda, se comunica e se relaciona. Embora represente um importante espaço de aprendizagem e convivência, o ambiente virtual também ampliou significativamente os riscos aos quais crianças e adolescentes estão expostos, sobretudo no que diz respeito à exploração sexual. A facilidade de acesso às plataformas digitais, combinada ao anonimato, à possibilidade de criação de perfis falsos e ao uso de ferramentas de ocultação, tem favorecido a disseminação de práticas ilícitas que violam de forma grave a dignidade sexual infantojuvenil.

Nesse cenário, o Direito, especialmente no campo penal e no âmbito da proteção integral prevista no Estatuto da Criança e do Adolescente, passou a enfrentar desafios cada vez mais complexos. As formas tradicionais de investigação mostraram-se, muitas vezes, insuficientes para acompanhar a dinâmica dos crimes cometidos em meios digitais, principalmente porque os autores dessas práticas utilizam recursos tecnológicos que dificultam sua localização e identificação. A infiltração policial virtual, introduzida pela Lei nº 13.441/2017, surgiu como resposta a essa nova realidade. Apesar de sua relevância prática e de sua previsão legal expressa, ainda existem lacunas significativas quanto à compreensão dos limites constitucionais e legais da infiltração policial no ambiente digital, especialmente no que se refere à proteção da intimidade, da privacidade, da inviolabilidade das comunicações e da preservação da cadeia de custódia da prova digital. Esse cenário evidenciou a necessidade de aprofundar a análise dessa técnica investigativa à luz do Estado Democrático de Direito, ponderando suas potencialidades, riscos e desafios na persecução penal contemporânea.

A escolha do tema se justificou pela crescente incidência de crimes de natureza sexual contra crianças e adolescentes praticados na internet e pela urgência em aprimorar os instrumentos investigativos capazes de enfrentar essa realidade. Além disso, compreender como a infiltração policial virtual pode ser aplicada de maneira legítima e segura contribui para o fortalecimento das políticas de proteção infantojuvenil e para a busca de respostas mais efetivas diante da criminalidade cibernética.

Dessa forma, o objetivo deste artigo foi analisar a infiltração policial virtual como instrumento de enfrentamento à exploração sexual de crianças e adolescentes na internet, destacando seus fundamentos legais, seus limites constitucionais e os desafios probatórios relacionados à coleta e preservação da prova digital. A partir desse enfoque, buscou-se oferecer uma reflexão crítica e atualizada sobre a aplicação dessa técnica no contexto da criminalidade virtual contemporânea.

2. Materiais e métodos

A metodologia adotada neste estudo fundamenta-se nos princípios da pesquisa científica aplicada ao Direito, estruturada a partir de uma abordagem qualitativa, de natureza teórico-bibliográfica e documental. A escolha por essa abordagem decorre da necessidade de compreender, por meio da análise normativa e doutrinária, como a infiltração policial virtual se consolida como instrumento legítimo de enfrentamento à exploração sexual de crianças e adolescentes na internet, observando os limites constitucionais, legais e probatórios que permeiam sua aplicação.

Trata-se de um estudo descritivo e analítico, conduzido pelo método dedutivo, que parte da análise das normas jurídicas e dos fundamentos teóricos da investigação criminal em ambiente digital, para, então, examinar os aspectos específicos da infiltração policial virtual prevista na Lei nº 13.441/2017. A pesquisa foi desenvolvida a partir da leitura, interpretação e análise de legislações pertinentes, como o Estatuto da Criança e do Adolescente, o Código de Processo Penal, o Marco Civil da Internet e a Lei de Organizações Criminosas, bem como de doutrina jurídica especializada, especialmente nas áreas de Direito Penal, Processo Penal e crimes cibernéticos relacionados ao ambiente digital, com ênfase nas técnicas especiais de investigação e na proteção infantojuvenil.

A metodologia incluiu também a análise de documentos oficiais, como relatórios da SaferNet Brasil e da Internet Watch Foundation, que oferecem dados sobre a incidência de crimes sexuais infantojuvenis no ambiente digital e contribuem para contextualizar a relevância da infiltração policial virtual como técnica de combate a essas práticas. Além disso, a pesquisa se apoiou em decisões jurisprudenciais recentes do Superior Tribunal de Justiça e do Supremo Tribunal Federal, especialmente aquelas relacionadas à validade da prova digital, à cadeia de custódia e aos limites da atuação

policial em ambientes virtuais, permitindo avaliar como os tribunais têm interpretado a aplicação da técnica investigativa.

A seleção das fontes ocorreu de forma criteriosa, priorizando obras atualizadas e documentos oficiais que tratam diretamente do tema. Como complemento, foram consideradas contribuições de profissionais da área policial que atuam em investigações cibernéticas, cujas experiências práticas auxiliam na compreensão dos desafios operacionais e psicológicos enfrentados pelos agentes infiltrados.

A investigação foi desenvolvida de forma sequencial e integrada, iniciando-se com o levantamento e a leitura das principais fontes normativas, doutrinárias e jurisprudenciais relacionadas ao tema. Em seguida, procedeu-se à análise crítica do material selecionado, com atenção aos aspectos legais, constitucionais e probatórios que envolvem a infiltração policial virtual. As informações foram então organizadas conforme os eixos temáticos definidos para o estudo, permitindo estruturar uma compreensão coerente e aprofundada da problemática. Por fim, elaborou-se a discussão analítica, articulando os resultados da pesquisa com o referencial teórico adotado, de modo a garantir consistência argumentativa e rigor metodológico.

Assim, a metodologia utilizada permitiu integrar teoria, legislação e decisões judiciais, possibilitando uma reflexão aprofundada sobre a infiltração policial virtual como técnica investigativa no enfrentamento da exploração sexual de crianças e adolescentes no ambiente digital. Essa abordagem garante consistência analítica ao estudo e oferece bases sólidas para compreender os limites e desafios dessa técnica no contexto do Direito brasileiro contemporâneo.

3. Resultados e discussão

3.1 A exploração sexual infantojuvenil no ambiente virtual

A exploração sexual de crianças e adolescentes no ambiente virtual é um fenômeno que desafia não apenas o Direito Penal, mas também a sociedade contemporânea. Com o avanço tecnológico e a crescente presença infantojuvenil nas redes, surgem novos espaços para a prática de condutas criminosas que antes se restringiam ao meio físico. O ambiente digital, marcado pelo anonimato, uso de perfis falsos, criptografia e ferramentas de ocultação, tornou-se um território fértil para

práticas ilícitas, dificultando significativamente a atuação dos órgãos de persecução penal.

No contexto brasileiro, dados divulgados pela SaferNet Brasil (2025) indicam que cerca de 60% das denúncias de crimes na internet envolvem abuso infantil. Esse número apresentou aumento significativo de 114% após o influenciador Felipe Bressanim Pereira, mais conhecido popularmente como Felca, divulgar um vídeo denunciando perfis que usam crianças e adolescentes para promover a adultização infantojuvenil. Essa realidade desafia os métodos tradicionais de investigação criminal, exigindo estratégias adaptadas à lógica digital e à anonimização dos agentes policiais.

3.2 A infiltração policial virtual: base legal, características e controvérsias

Diante desse quadro, a Lei nº 13.441/2017 introduziu no ordenamento jurídico brasileiro a infiltração policial virtual como instrumento específico de investigação voltado aos crimes contra a dignidade sexual de crianças e adolescentes. Essa técnica permite que agentes especializados atuem disfarçadamente em ambientes virtuais, infiltrando-se em grupos, fóruns, chats e plataformas digitais utilizados para o compartilhamento de material ilícito, com o objetivo de identificar autores, coletar provas e interromper práticas criminosas.

Todavia, apesar de sua eficácia operacional, a infiltração policial virtual envolve delicadas questões jurídicas e constitucionais. Seu uso implica restrições a direitos fundamentais, como a intimidade, a privacidade, a inviolabilidade das comunicações e o devido processo legal, exigindo controle judicial rigoroso, fundamentação adequada e respeito aos princípios da proporcionalidade e da subsidiariedade.

Para parte da doutrina, a infiltração virtual é compreendida como uma espécie do gênero infiltração policial, aplicável nas mesmas hipóteses em que seria cabível a infiltração presencial do agente. Nesse sentido, CASTRO (2017, s.p.) explica que

A infiltração policial consiste em técnica especial e subsidiária de investigação, qualificada pela atuação dissimulada (com ocultação da real identidade) e sigilosa de agente policial, seja presencial ou virtualmente, face a um criminoso ou grupo de criminosos, com o fim de localizar fontes de prova, identificar criminosos e obter elementos de convicção para elucidar o delito e desarticular associação ou organização criminosa, auxiliando

também na prevenção de ilícitos penais. A infiltração policial é gênero do qual são espécies a presencial (física) e a virtual (cibernética ou eletrônica).

Essa medida também encontra respaldo na Lei nº 12.850/2013, que autoriza a infiltração de agentes públicos no contexto de organizações criminosas, inclusive no meio virtual. Além disso, o Marco Civil da Internet (Lei nº 12.965/2014) estabelece diretrizes sobre a proteção de dados pessoais, guarda de registros e responsabilidade dos provedores, o que influencia diretamente a legalidade da obtenção de provas durante as investigações cibernéticas.

No entanto, embora a técnica se revele eficiente na persecução penal, ela suscita debates sobre seus limites legais e constitucionais. A infiltração virtual envolve riscos de violação a direitos fundamentais, como a intimidade, a privacidade e o devido processo legal.

Além disso, há controvérsias quanto à validade das provas produzidas por meio dessa técnica. O agente infiltrado pode, por exemplo, estimular ou induzir o crime, o que caracteriza o chamado flagrante preparado, vedado pelo ordenamento jurídico brasileiro. Nesse ponto, torna-se essencial diferenciar a atuação passiva e meramente observadora do policial da conduta provocadora que pode contaminar a licitude da prova. O art. 190-A, § 3º, da Lei nº 13.441/2017 consagra o caráter excepcional e subsidiário da infiltração policial virtual, ao estabelecer que essa técnica não deve ser utilizada quando a prova puder ser obtida por outros meios menos invasivos, dispondo que “a infiltração de agentes de polícia na internet não será admitida se a prova puder ser obtida por outros meios”.

A jurisprudência ainda é vacilante quanto à extensão da infiltração, o papel do agente público e a renovação sucessiva da autorização judicial. Tais aspectos demonstram a necessidade de uma delimitação mais clara do instituto e de parâmetros objetivos para sua utilização, sob pena de abrir margem para abusos estatais e insegurança jurídica.

3.3 Crimes cibernéticos e ciberpedofilia

A evolução tecnológica das últimas décadas transformou profundamente o cenário da criminalidade no ambiente digital, ampliando não apenas o número de práticas ilícitas, mas também a complexidade dos mecanismos utilizados pelos infratores.

Os crimes cibernéticos passaram a ocupar o papel central das discussões jurídicas contemporâneas, especialmente quando relacionados à violação de direitos fundamentais das crianças e adolescentes.

Como explica Crespo (2011, p. 65), há uma distinção essencial entre crimes informáticos próprios e impróprios. Assim, afirma que

Nesse sentido, podemos dizer que todas as condutas praticadas contra bens jurídicos informáticos (sistemas, dados) são delitos de risco informático ou próprios, ao passo que aquelas outras condutas que se dirigirem contra bens jurídicos tradicionais (não relativos à tecnologia) são crimes digitais impróprios.

No campo da exploração sexual infantojuvenil, a internet ampliou práticas já conhecidas e possibilitou o surgimento de novas modalidades delitivas. A pornografia infantil, tipificada nos art. 240 a 241-D do Estatuto da Criança e do Adolescente (ECA), abrange desde a produção até o armazenamento e o compartilhamento de material de natureza sexual envolvendo crianças e adolescentes.

Segundo dados da Internet Watch Foundation (IWF, 2024), houve um expressivo aumento das páginas contendo pornografia infantil na web, que quadruplicaram em relação aos anos anteriores. Entre as 531 URLs da dark web (anteriormente denominadas “sites ocultos”) identificadas como distribuidoras de cenas de abuso sexual infantil, aproximadamente 82% possuem caráter comercial. O Brasil ocupa, atualmente, a quinta posição mundial em disseminação desse tipo de conteúdo, atrás apenas de grandes potências tecnológicas, o que evidencia a gravidade e a complexidade do problema.

Devido à ausência de barreiras geográficas, ao anonimato, à criptografia, ao uso de VPNs e a ambientes de difícil rastreamento, como a dark web, os métodos tradicionais de investigação ficam inviabilizados e impulsionam a necessidade de técnicas sofisticadas, entre elas a infiltração policial virtual. Dentro desse cenário surge o fenômeno da ciberpedofilia, definido como

O conjunto de ações de natureza sexual praticadas contra crianças e adolescentes com a mediação das tecnologias de informação e comunicação (TICs), notadamente a internet, abarcando desde o aliciamento até a exploração sexual propriamente dita. (BOAVENTURA; FIGUEIREDO, 2025, p. 7 apud CAVALCANTE, 2020, p. 3).

Esse fenômeno não se limita ao consumo de conteúdo pornográfico, mas abrange diversas práticas, como grooming (aliciamento), sextorsion (extorsão sexual), sexting coercitivo (coerção sexual), transmissão ao vivo de abusos (livestreaming sexual), manipulação psicológica e aliciamento para encontros presenciais. A exposição online pode ocorrer tanto de forma involuntária, quando os pais divulgam conteúdos de seus filhos sem refletir sobre os riscos, quanto de forma voluntária, quando as crianças e adolescentes utilizam as redes sem supervisão adequada. Ambas as formas de exposição deixam crianças e adolescentes suscetíveis diante da ação dos infratores.

A crescente normalização da presença infantojuvenil no ambiente virtual, aliada à facilidade de comunicação com desconhecidos, contribui para o aumento dos índices de exploração. Estudos demonstram que, durante a pandemia, o tempo de exposição online de crianças e adolescentes aumentou substancialmente, acompanhado pela intensificação dos casos de pedofilia virtual, como observam Rovinski e Pelisoli (2020, p. 27), ao afirmarem que “uma das características da violência sexual no mundo contemporâneo é aquela perpetrada pelos recursos tecnológicos e pela Internet”.

Nesse mesmo sentido, Bilches (2020) destaca que, durante o período de isolamento social, houve aumento dos crimes cibernéticos relacionados à exploração sexual infantojuvenil, em razão da maior permanência de crianças e adolescentes no ambiente digital, o que ampliou sua vulnerabilidade diante de abusadores.

Diante desse contexto multifatorial envolvendo psicologia, tecnologia, criminologia e direito, torna-se indispensável compreender que a exploração sexual online constitui crime altamente estruturado, como redes internacionais de compartilhamento, mecanismos profissionais de anonimização e grande capacidade de regeneração. A resposta estatal a esse fenômeno, portanto, exige instrumentos de investigação compatíveis com sua complexidade, entre eles a infiltração policial virtual, regulada pela Lei nº 13.441/2017.

3.4 Aspectos jurídicos, operacionais e constitucionais da infiltração policial virtual

A infiltração policial virtual representa uma das mais relevantes e sofisticadas técnicas de investigação contemporânea voltada ao enfrentamento da exploração sexual de crianças e adolescentes na internet. Sua utilização decorre diretamente da incapacidade dos métodos tradicionais de investigação em acompanhar a velocidade, o anonimato e a arquitetura transnacional dos crimes cibernéticos. Logo, trata-se de uma técnica especial de investigação que se diferencia de todas as demais pela natureza dissimulada da atuação estatal e pela sua aplicação específica a crimes de alta complexidade.

Do ponto de vista jurídico, a infiltração policial possui regulamentação geral na Lei nº 12.850/2013, aplicável às organizações criminosas, mas ganha disciplina própria e mais rigorosa na Lei nº 13.441/2017, que introduziu os arts. 190-A a 190-E no Estatuto da Criança e do Adolescente. Essa última legislação determina que a infiltração virtual pode ocorrer mediante autorização judicial fundamentada, com finalidade claramente definida, prazo limitado e relatórios periódicos submetidos ao Ministério Público e ao Poder Judiciário. A previsão dessa normativa demonstra a preocupação do legislador em compatibilizar a necessidade de eficiência investigativa com o respeito às garantias constitucionais, especialmente a intimidade e a inviolabilidade das comunicações, conforme previsão constitucional

Art. 5º. [...]

X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

A finalidade principal da infiltração policial é permitir que o agente, protegido pelo anonimato, tenha acesso a condutas criminosas que jamais seriam descobertas por meios convencionais. Isso ocorre porque os grupos que compartilham pornografia infantil operam em comunidades fechadas, protegidas por camadas de anonimização, criptografia, sistemas de convites e mecanismos rigorosos de verificação de confiança.

Sob a perspectiva jurídica, a infiltração é considerada medida excepcional, subsidiária e proporcional, sendo autorizada somente quando não houver outro meio menos invasivo de obter as informações necessárias. Isso decorre do fato de que a técnica envolve restrições significativas a direitos fundamentais e possui risco inerente de contaminação probatória, sobretudo quando há possibilidade de atuação provocadora do agente. Por essa razão, o Supremo Tribunal Federal, desde o precedente clássico da Súmula 145, afirma que “não há crime quando a preparação do flagrante pela polícia torna impossível a sua consumação”.

O aspecto técnico-operacional também desempenha papel central na definição da infiltração virtual. Para que o agente policial atue na investigação virtual, exige-se conhecimento avançado sobre segurança digital, criptografia, uso da rede TOR (The Onion Router) e mecanismos de manipulação social, sem os quais a persona criada pode ser facilmente desmascarada. A investigação, portanto, depende de equipes multidisciplinares envolvendo policiais, analistas de inteligência, peritos em informática forense e profissionais de saúde mental, considerando o risco psicológico inerente à exposição repetida a material de abuso sexual infantil.

Outro fundamento essencial da infiltração é o princípio da proteção integral da criança e do adolescente, previsto legalmente na Constituição Federal de 1988.

Art. 227. 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.

Assim, a legitimidade da infiltração decorre não apenas da lei, mas da necessidade e proporcionalidade em impedir a continuidade das vitimizações.

3.5 Limites constitucionais, riscos jurídicos e excepcionalidade da técnica

A infiltração policial virtual, apesar de essencial para o enfrentamento da exploração sexual infantil na internet, encontra limites rigorosos estabelecidos pela Constituição Federal e pela legislação infraconstitucional. Trata-se de técnica altamente intrusiva, que implica restrições a direitos fundamentais, especialmente à privacidade, à intimidade, à imagem e à inviolabilidade das comunicações. Por essa razão, sua

utilização deve sempre se submeter aos princípios da legalidade estrita, proporcionalidade, necessidade e subsidiariedade, sendo vedada qualquer forma de atuação estatal que extrapole os limites autorizados judicialmente.

A Constituição Federal, ao garantir a inviolabilidade das comunicações e o sigilo da vida privada (art. 5º, X e XII), impõe que qualquer técnica de investigação que interfira nessas esferas somente pode ser realizada mediante decisão judicial fundamentada.

A infiltração policial virtual, ao possibilitar que um agente estatal atue sob falsa identidade digital, se insira em grupos fechados e acompanhe conversas privadas, exige controle rigoroso do Poder Judiciário. A infiltração não pode ocorrer sem que haja autorização específica e fundamentada, sob pena de violação direta aos direitos fundamentais protegidos pela Constituição. A Lei nº 12.850/2013 estabelece que

Art. 10. A infiltração de agentes de polícia em tarefas de investigação, representada pelo delegado de polícia ou requerida pelo Ministério Público, após manifestação técnica do delegado de polícia quando solicitada no curso de inquérito policial, será precedida de circunstanciada, motivada e sigilosa autorização judicial, que estabelecerá seus limites.

Art. 10-A. Será admitida a ação de agentes de polícia infiltrados virtuais, obedecidos os requisitos do caput do art. 10, na internet, com o fim de investigar os crimes previstos nesta Lei e a eles conexos, praticados por organizações criminosas, desde que demonstrada sua necessidade e indicados o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas.

A excepcionalidade da técnica decorre do fato de que ela permite ao agente atuar dentro de esferas de intimidade que, em circunstâncias normais, jamais estariam acessíveis ao Estado. Essa intrusão só se justifica porque a integridade física, psicológica e sexual de crianças e adolescentes é considerada como prioridade absoluta. No entanto, mesmo diante dessa proteção reforçada, o Estado não está autorizado a atuar de maneira ilimitada. Um dos principais limites da infiltração é a vedação absoluta ao flagrante preparado.

Além disso, a infiltração deve obedecer ao princípio da proporcionalidade em sentido estrito. A medida só é admissível quando houver demonstração concreta de que outros instrumentos investigativos, como quebras de sigilo, análise de IP, cooperação internacional, busca e apreensão ou monitoramento de dados, são insuficientes para a obtenção das provas necessárias. Isso decorre do fato de que a infiltração

representa uma forma de vigilância personalizada e sigilosa, que se aproxima das técnicas de inteligência, mas, por gerar prova judicial, exige fundamento reforçado.

A legislação específica introduzida pela Lei nº 13.441/2017 estabelece limites materiais e procedimentais à infiltração policial virtual. O art. 190-A do Estatuto da Criança e do Adolescente dispõe que essa técnica somente poderá ser autorizada quando houver indícios da prática de infração penal relacionada aos crimes previstos nos arts. 240 a 241-D do próprio ECA, todos vinculados à exploração sexual de crianças e adolescentes no ambiente virtual. Ademais, o dispositivo impõe limites temporais à medida, ao prever que a infiltração será autorizada por prazo máximo de 90 dias, admitida sua renovação sucessiva, desde que devidamente fundamentada, até o limite total de 720 dias, sob controle e supervisão do Poder Judiciário.

Dessa forma, a lei busca compatibilizar a efetividade da investigação criminal com a proteção das garantias fundamentais, especialmente quanto à excepcionalidade, à proporcionalidade e ao controle judicial da infiltração policial virtual.

3.6 Prova digital, cadeia de custódia e autenticidade dos elementos probatórios

A infiltração policial virtual, por ocorrer integralmente em ambiente digital, produz uma modalidade de prova com características distintas da prova tradicional. Sua natureza volátil, facilmente replicável, fragmentada e suscetível à adulteração impõe ao Estado a necessidade de observância de protocolos técnicos rigorosos, especialmente no que se refere à preservação da cadeia de custódia, disciplinada pelos arts. 158-A a 158-F do Código de Processo Penal, com redação dada pela Lei nº 13.964/2019. O art. 158-A do Código de Processo Penal conceitua cadeia de custódia como

O conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.

A partir desse conceito, compreende-se que a observância das etapas da cadeia de custódia, que envolvem o reconhecimento, a coleta, o acondicionamento, o transporte, o armazenamento e o processamento dos vestígios, é fundamental para garantir a integridade e a confiabilidade da prova digital produzida no contexto das investigações que se utilizam da infiltração policial virtual.

Dessa forma, a cadeia de custódia configura-se como elemento essencial para a credibilidade da prova digital, na medida em que assegura que os elementos colhidos em ambiente virtual não tenham sido alterados, manipulados ou comprometidos. Tal cuidado se revela ainda mais relevante nos crimes de exploração sexual de crianças e adolescentes, cuja gravidade exige provas robustas, íntegras e passíveis de verificação pericial.

A prova digital envolve, em regra, arquivos multimídia (fotos, vídeos), registros de conversas, metadados, capturas de tela, históricos de navegação, endereços IP e informações armazenadas em nuvens computacionais. Entretanto, ao contrário de objetos físicos, tais como armas ou documentos, a prova digital não possui forma estável, pois pode ser modificada com extrema facilidade, muitas vezes sem deixar rastros aparentes. Por isso, a doutrina contemporânea destaca a necessidade de procedimentos padronizados de preservação, extração e análise. A volatilidade das informações digitais exige que a coleta ocorra mediante ferramentas apropriadas que capturem metadados e gerem códigos de verificação (hash).

A cadeia de custódia compreende um conjunto de atos sucessivos que garantem a integridade da prova desde sua obtenção até sua análise no processo. Cada etapa, desde a coleta, acondicionamento, preservação, processamento, armazenamento, transporte e descarte, deve ser documentada de forma clara e cronológica. Isso inclui a identificação do agente responsável, dia, hora, equipamento utilizado e método de extração. No contexto da infiltração virtual, essa documentação deve ser ainda mais rigorosa, pois o agente atua de maneira dissimulada e, muitas vezes, precisa registrar interações complexas com os investigados.

É por isso que as capturas de tela simples (prints), amplamente utilizadas nas fases iniciais de investigação, possuem valor probatório limitado se não acompanhadas de verificação pericial. O Superior Tribunal de Justiça, ao tratar da hipótese de quebra da cadeia de custódia na extração de dados de aparelho celular, assentou que a confiabilidade das evidências digitais depende da observância de critérios técnicos que assegurem sua autenticidade, integridade e rastreabilidade, especialmente diante da volatilidade e da suscetibilidade a alterações desses dados.

PROCESSUAL PENAL. AGRAVO REGIMENTAL NO HABEAS CORPUS. TRÁFICO DE DROGAS. APREENSÃO DE CELULAR. EXTRAÇÃO DE DADOS. CAPTURA DE TELAS. QUEBRA DA CADEIA DE CUSTÓDIA. INADMISSIBILIDADE DA PROVA DIGITAL. AGRAVO REGIMENTAL PROVIDO.

O instituto da cadeia de custódia visa a garantir que o tratamento dos elementos probatórios, desde sua arrecadação até a análise pela autoridade judicial, seja idôneo e livre de qualquer interferência que possa macular a confiabilidade da prova. (STJ, no AgRg no HC n. 828054/RN, 5ª Turma, Rel. Min. Joel Ilan Paciornik, 2024).

Sob essa perspectiva, a validade de registros digitais requer a preservação de seus metadados e a adoção de procedimentos periciais aptos a demonstrar que o conteúdo apresentado corresponde, de forma fiel, àquele originalmente visualizado, afastando-se a possibilidade de adulterações posteriores. Assim, um mero print de tela, desacompanhado de mecanismos técnicos de verificação e de adequada documentação da cadeia de custódia, não atende plenamente às exigências processuais, devendo sua aptidão probatória ser analisada com cautela, sob pena de comprometimento da confiabilidade do material probatório.

Outro elemento essencial na produção da prova digital é a utilização de hashes criptográficos (como SHA-256 e SHA-512), que funcionam como uma espécie de impressão digital do arquivo. Esses códigos garantem que qualquer alteração, por menor que seja, seja identificada de imediato, assegurando a integridade do material, uma vez que a função hash consiste em mecanismo matemático capaz de transformar dados em uma sequência única, cuja mínima modificação resulta em alteração completa do código gerado.

Nesse contexto, o hash não apenas preserva a integridade do conteúdo, mas também viabiliza a verificação da autenticidade da prova digital, permitindo que peritos e autoridades confirmem que o material analisado em juízo corresponde exatamente àquele originalmente coletado no ambiente investigado. Tal mecanismo assume papel central na cadeia de custódia, na medida em que possibilita o controle de integridade em todas as fases do tratamento da prova, desde a coleta até o armazenamento e posterior análise. Além disso, a utilização de funções hash contribui para a rastreabilidade dos elementos probatórios, pois cada verificação realizada gera um registro técnico que pode ser documentado no laudo pericial, reforçando a transparência e a confiabilidade da prova. Essa prática é especialmente relevante em investigações digitais, nas quais a facilidade de manipulação de dados exige mecanismos robustos

de validação. Os documentos encaminhados indicam que a prova digital somente alcança confiabilidade plena quando acompanhada de hash que permita verificar sua integridade em todas as fases da cadeia de custódia, garantindo que o material não sofreu alterações desde sua obtenção até sua apresentação em juízo (FISBERG, 2025).

A infiltração policial virtual também exige que o agente realize registros cronológicos de todas as etapas da investigação, descrevendo cada interação, cada arquivo acessado e cada ato necessário para manter o disfarce. Esses registros são fundamentais para a reconstrução judicial da operação e para demonstrar que o agente não atuou de maneira provocadora. A atuação deve ser limitada ao necessário para não comprometer a investigação, mas jamais deve estimular condutas criminosas, sob pena de nulidade da prova e responsabilização estatal.

Além da coleta, outro desafio crítico da prova digital é o armazenamento seguro. Conteúdos de pornografia infantil exigem nível elevado de proteção, com ambientes criptografados e acesso restrito apenas a profissionais autorizados. A legislação brasileira prevê responsabilização penal para qualquer pessoa, inclusive servidores públicos, que compartilhe este tipo de conteúdo fora das hipóteses autorizadas. Por esse motivo, o armazenamento de material ilícito deve ser feito exclusivamente em ambientes controlados, evitando risco de vazamento ou exposição indevida.

Por fim, a infiltração virtual demanda constante atuação de peritos em informática forense, que devem acompanhar o processo desde o início, para que a extração da prova seja tecnicamente válida. Não se trata apenas de verificar a existência do arquivo, mas também de determinar sua origem, identificar o fluxo de compartilhamento, reconstruir conversas apagadas, rastrear endereços IP e analisar padrões de comportamento digital. Esse trabalho multidisciplinar é indispensável para a responsabilização efetiva dos criminosos e para a proteção das vítimas, seguindo a orientação de que a prova digital deve ser interpretada no contexto de um conjunto complexo de elementos, e nunca de forma isolada.

Dessa forma, a prova digital gerada pela infiltração policial virtual exige atenção integral às normas jurídicas, técnicas e procedimentais, assegurando integridade, autenticidade e confiabilidade. A observância da cadeia de custódia, aliada à atuação

pericial especializada, constitui o alicerce da validade da infiltração no processo penal e da proteção das vítimas, garantindo que a atuação estatal atenda tanto à eficiência investigativa quanto às garantias fundamentais.

3.7 Desafios tecnológicos, operacionais e psicológicos da infiltração virtual

A infiltração policial virtual enfrenta uma combinação de desafios que envolvem tecnologia, prática investigativa, estrutura institucional e impactos psicológicos sobre os agentes responsáveis. Esses desafios decorrem da própria natureza da internet e da complexidade crescente das redes criminosas especializadas na exploração sexual de crianças e adolescentes.

No plano tecnológico, o primeiro obstáculo é o anonimato estrutural da internet, amplificado pelo uso de VPNs, servidores proxy e redes de anonimização, como a The Onion Router (TOR). Essas ferramentas ocultam a localização e dificultam o rastreamento dos usuários, impedindo métodos tradicionais de identificação. Além disso, muitos fóruns de compartilhamento de pornografia infantil estão hospedados na dark web, exigindo que o agente infiltrado domine técnicas de navegação avançada e compreenda o funcionamento de ambientes protegidos por múltiplas camadas de criptografia. Os criminosos utilizam plataformas replicadas em diferentes servidores, o que dificulta a derrubada e redistribui o conteúdo ilícito em pouco tempo.

Outro desafio tecnológico reside no uso de plataformas com mensagens efêmeras, como Telegram e aplicativos que apagam automaticamente conversas após a visualização. Tais mecanismos tornam a coleta de provas ainda mais delicada, já que o agente deve capturar o conteúdo no instante exato em que ele é exibido, e essa captura deve ser validada por meios periciais. Os criminosos também se valem de técnicas de fragmentação de arquivos, criptografia de ponta a ponta e armazenamento em nuvem com autenticação multifatorial, tornando a coleta da prova um processo que depende tanto do agente infiltrado quanto da perícia especializada.

No plano operacional, a infiltração policial virtual exige habilidades que vão além do conhecimento jurídico e técnico. O agente deve criar e manter uma identidade digital absolutamente convincente, capaz de se inserir em ambientes hostis que frequentemente exigem testes de confiança, como o envio prévio de material ilícito, o que é vedado pela legislação brasileira. Se a identidade fictícia apresentar qualquer

inconsistência, os demais membros podem desconfiar da autenticidade e expulsar o agente, comprometendo toda a operação e até colocando em risco sua segurança digital.

A duração das investigações também representa desafio significativo. Operações de infiltração podem durar meses ou até anos, exigindo monitoramento constante, relatórios periódicos e avaliação judicial contínua. Esse tempo prolongado demanda grande dedicação do agente e trabalho coordenado entre as equipes de polícia, perícia e Ministério Público. Além disso, o agente deve estar preparado para reconhecer rapidamente situações de risco.

Do ponto de vista psicossocial, os desafios são ainda mais sensíveis. A infiltração virtual é uma das atividades mais desgastantes dentro da persecução penal, uma vez que expõe o agente repetidamente a conteúdos extremamente violentos, perturbadores e emocionalmente corrosivos. A exposição a esse tipo de conteúdo pode desencadear impactos psicológicos relevantes, como estresse, ansiedade e outros prejuízos à saúde mental do agente, além de sentimento de impotência.

A possibilidade de dessensibilização progressiva, fenômeno no qual o agente, para lidar com a carga emocional dos conteúdos, reduz involuntariamente sua sensibilidade diante das cenas, pode gerar efeitos psicológicos graves a longo prazo. Também há risco de isolamento social, já que o trabalho é sigiloso e o agente não pode compartilhar com familiares ou amigos os acontecimentos vividos. Assim, a necessidade de manter o disfarce e a impossibilidade de expressar o impacto emocional da operação agravam o desgaste psicológico do agente infiltrado, afetando sua integridade psíquica (PEREIRA, 2022).

Tal cenário é corroborado por estudos recentes, que evidenciam a profundidade dos impactos psicológicos decorrentes da atuação policial em contextos envolvendo abuso sexual de menores. Conforme destaca Henriques (2025), policiais que atuam em ocorrências envolvendo abuso sexual de menores apresentam sintomas recorrentes de fadiga por compaixão, trauma secundário, sentimento de impotência e revolta, especialmente em razão do contato frequente com situações de extrema vulnerabilidade das vítimas, além de que a ausência de formação específica e o déficit de apoio

psicológico institucional contribuem significativamente para o agravamento do desgaste emocional desses profissionais, evidenciando a necessidade de medidas estruturais voltadas à proteção da saúde mental no contexto da atividade policial.

A resposta institucional a esses desafios ainda é insuficiente, embora o agente passe por rotinas obrigatórias de acompanhamento psicológico. A falta de mecanismos de proteção não apenas prejudica a saúde dos profissionais, mas também pode comprometer a eficácia da operação, pois agentes mentalmente esgotados tornam-se mais suscetíveis a erros e a falhas na condução da infiltração.

Assim, os desafios tecnológicos, operacionais e psicossociais demonstram que a infiltração policial virtual é uma técnica de investigação que demanda aparato estatal altamente especializado, suporte psicossocial contínuo e estrutura multidisciplinar robusta. A atuação adequada depende de interação constante entre tecnologia, perícia, psicologia e direito, reforçando que seu uso exige planejamento detalhado, estrita legalidade e suporte institucional permanente.

3.8 A desterritorialidade dos crimes digitais e necessidade de cooperação internacional

Os crimes de exploração sexual de crianças e adolescentes praticados no ambiente digital possuem uma característica essencial: a desterritorialidade. Diferentemente das infrações tradicionais, que possuem um local físico claro de ocorrência, os delitos cometidos na internet rompem fronteiras geográficas e legais. Um agressor pode estar em um país, utilizando um servidor localizado em outro, trocando material ilícito com usuários distribuídos por diversos continentes.

A natureza desterritorializada e anônima da internet impõe desafios hercúleos à persecução penal, demandando uma releitura dinâmica dos institutos jurídicos penais e processuais penais para efetivar a proteção integral da criança e do adolescente, prevista no artigo 227 da Constituição Federal. (BOAVENTURA; FIGUEIREDO, 2025, p. 7 apud GONÇALVES et al, 2025, p. 2653).

A pornografia infantil digital, especialmente aquela que circula na dark web, geralmente se organiza em redes transnacionais, muitas vezes hierarquizadas e invisíveis aos mecanismos de fiscalização tradicionais. Os grupos de agentes criminosos operam em comunidades distribuídas em diversos países, com servidores espelha-

dos, backups automáticos e camadas avançadas de criptografia, tornando quase impossível o rastreamento isolado por uma autoridade nacional. Diante disso, torna-se essencial a cooperação jurídica internacional, conduzida por meio de instrumentos como Tratados de Assistência Jurídica Mútua (MLATs), acordos multilaterais, atuação conjunta de agências como Interpol, Europol, Homeland Security e, sobretudo, por meio da parceria com o National Center for Missing & Exploited Children (NCMEC). O NCMEC desempenha papel crucial na comunicação imediata de casos envolvendo material de abuso sexual infantil, atuando por meio da CyberTipline, sistema centralizado que recebe denúncias encaminhadas principalmente por provedores de serviços eletrônicos. Tais comunicações incluem dados relevantes como informações sobre arquivos suspeitos, contas de usuários, endereços IP, registros de acesso e outros elementos técnicos que auxiliam na identificação dos envolvidos e na reconstrução da dinâmica dos fatos investigados (NCMEC, 2025).

Nesse contexto, destaca-se que plataformas digitais como Google, Meta, Discord, entre outras, desempenham papel ativo na detecção de conteúdos ilícitos, seja por meio de sistemas automatizados de identificação, seja por denúncias de usuários. Uma vez identificados indícios de material relacionado à exploração sexual infantojuvenil, essas empresas encaminham relatórios ao NCMEC, contendo informações técnicas detalhadas que subsidiam a atuação das autoridades competentes. Além disso, os dados da CyberTipline demonstram que as denúncias não se limitam a um único país, mas frequentemente envolvem múltiplas jurisdições, sendo encaminhadas às autoridades competentes em diferentes localidades para investigação. Esse fluxo contínuo de informações evidencia que a atuação das plataformas digitais constitui uma das principais portas de entrada para a identificação de crimes dessa natureza, ao passo que o NCMEC funciona como um elo intermediário essencial entre empresas privadas e órgãos de persecução penal, promovendo a organização, triagem e distribuição das informações recebidas. Ademais, a centralização dessas comunicações permite não apenas a identificação de autores, mas também o reconhecimento de padrões de atuação criminosa, a vinculação entre diferentes investigações e a localização de vítimas em contextos distintos, o que evidencia a imprescindibilidade da inteligência compartilhada em nível internacional. A atuação coordenada, nesse sentido,

revela-se indispensável diante da velocidade de propagação do material ilícito no ambiente digital e da facilidade com que os agentes se deslocam entre diferentes jurisdições virtuais (NCMEC, 2025).

Sob essa perspectiva, a análise dos dados reforça que a repressão à exploração sexual infantojuvenil no ambiente digital depende de um sistema integrado de comunicação e cooperação internacional, no qual a troca rápida de informações é essencial para a identificação de vítimas e autores, bem como para a interrupção da circulação de material ilícito em escala global.

O Marco Civil da Internet (Lei nº 12.965/2014) também influencia diretamente esse processo. O art. 11 estabelece que empresas estrangeiras com atividade no Brasil devem obedecer à legislação nacional no tocante à proteção de dados e cumprimento de ordens judiciais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Na prática, isso reforça a capacidade brasileira de exigir que empresas como Google, Meta e Twitter forneçam registros de acesso e conteúdo armazenado, mesmo que os servidores estejam no exterior. Entretanto, apesar desse avanço normativo, o tempo de resposta de provedores internacionais se torna um dos maiores entraves à investigação, sobretudo em casos em que o risco à vítima é imediato.

A infiltração policial virtual, nesse cenário, tem papel estratégico. Ela permite identificar usuários em qualquer parte do mundo, gerando elementos informativos indispensáveis para acionar mecanismos internacionais de cooperação. Para além da identificação dos autores, os agentes infiltrados também atuam no reconhecimento de vítimas reais, cuja localização pode ser determinada a partir de pistas deixadas no ambiente digital, como objetos, sotaques, marcas arquitetônicas ou metadados de arquivos.

No entanto, apesar dos avanços, persistem importantes desafios. A lentidão no cumprimento de cartas rogatórias, a necessidade de tradução de documentos, os diferentes padrões de preservação de logs e as políticas internas de privacidade

adotadas por plataformas estrangeiras muitas vezes retardam a investigação. Além disso, muitos países não possuem legislação clara sobre pornografia infantil digital, dificultando a responsabilização dos autores quando localizados em territórios com leis permissivas.

Assim, a desterritorialidade dos crimes digitais impõe ao Estado brasileiro uma dependência inafastável da cooperação internacional, tornando impossível uma resposta eficaz sem articulação global. A infiltração policial virtual, por sua vez, atua como ponto de partida para a maioria desses processos, permitindo a identificação inicial de criminosos e subsidiando pedidos de cooperação. Dessa forma, a técnica revela-se não apenas compatível com o cenário transnacional, mas indispensável para enfrentá-lo adequadamente.

3.9 A diferença entre infiltração policial virtual e ronda virtual

A distinção entre infiltração policial virtual e ronda virtual é fundamental, tanto para a compreensão dogmática da técnica de investigação quanto para a sua validade jurídica. Embora ambos os métodos sejam utilizados para o enfrentamento da criminalidade digital, especialmente no contexto da exploração sexual infantojuvenil, eles apresentam finalidades, graus de intrusão, pressupostos legais e consequências probatórias completamente distintos. A confusão entre essas técnicas pode levar à nulidade das provas colhidas e, em alguns casos, à responsabilização do agente público.

A infiltração policial virtual consiste na atuação dissimulada do agente de polícia, que cria uma identidade digital falsa com o objetivo de se inserir em ambientes restritos, como grupos privados, salas de bate-papo fechadas, fóruns da dark web e canais criptografados, onde ocorre o compartilhamento de material de abuso sexual infantil. A atuação exige autorização judicial prévia, fundamentada e delimitada, conforme previsto nos arts. 190-A a 190-E do Estatuto da Criança e do Adolescente. Assim, a infiltração envolve, necessariamente, interação ativa, ainda que limitada, e ingresso em ambientes privados, o que justifica o grau elevado de controle judicial.

Já a ronda virtual, conhecida também como patrulhamento digital ou varredura cibernética, consiste no monitoramento de ambientes abertos ao público, tais como redes sociais, perfis públicos, comentários visíveis, transmissões ao vivo e sites

indexados. Nessa modalidade, o agente policial não cria identidade falsa nem interage dissimuladamente com suspeitos, mas limita-se a observar comportamentos e coletar informações que estão ao alcance de qualquer usuário comum da internet. Por essa razão, a ronda virtual não exige autorização judicial, desde que respeite os limites da legalidade e permaneça dentro do ambiente público. Recentemente, o STJ expressou esse entendimento de forma clara. A Sexta Turma do Superior Tribunal de Justiça, em julgamento realizado em outubro de 2025, reconheceu que

Não se trata, portanto, de invasão a espaço privado ou interceptação de comunicações, que exigiriam prévia autorização judicial, mas de coleta de informações disponíveis em ambiente compartilhado. Trata-se de ronda contínua que não se direciona a pessoas determinadas, diferentemente do procedimento da infiltração policial.

A distinção entre as duas técnicas não é apenas teórica, possui impacto direto sobre a licitude das provas. Sempre que o agente, mesmo durante uma ronda virtual, passa a interagir com suspeitos, criar perfis falsos, entrar em grupos fechados ou utilizar artifícios de engano, sua atuação deixa de ser simples monitoramento e se converte em infiltração. Nesse ponto, torna-se obrigatória a autorização judicial prévia. Caso contrário, configura-se violação da intimidade e das comunicações, resultando em prova ilícita.

Outro aspecto que diferencia as técnicas é o grau de intrusão. Enquanto a ronda virtual é comparável ao patrulhamento de rua, em que o agente circula em locais públicos para observar comportamentos suspeitos, a infiltração é análoga ao ingresso do policial em uma organização criminosa sob identidade falsa. Por isso, somente a infiltração admite a obtenção de provas diretamente relacionadas ao conteúdo ilícito compartilhado privadamente. A ronda, ao contrário, gera meramente indícios ou informações preliminares, servindo como base para solicitar medidas mais invasivas, como quebra de sigilo, busca e apreensão ou a própria infiltração.

A diferença também se manifesta no plano psicológico e operacional. A ronda é atividade de risco reduzido, enquanto a infiltração expõe o agente a conteúdo extremamente violento e a ambientes psicologicamente corrosivos.

Diante disso, conclui-se que infiltração e ronda virtual não são métodos intercambiáveis, mas sim técnicas complementares: a ronda identifica suspeitos, enquanto a infiltração aprofunda a investigação e coleta provas de difícil acesso. No

entanto, cada uma possui disciplina jurídica própria, devendo ser aplicada com respeito absoluto aos limites legais, sob pena de nulidade da investigação e violação aos direitos fundamentais envolvidos.

4. Conclusão

Diante de todo o exposto, fica evidente que a infiltração policial virtual se consolidou como uma das mais relevantes técnicas investigativas no enfrentamento aos crimes de exploração sexual de crianças e adolescentes na internet, sobretudo diante da crescente complexidade dos ambientes digitais e da sofisticação das redes criminosas transnacionais. A análise das bases conceituais, normativas, constitucionais e jurisprudenciais demonstrou que essa técnica não pode ser compreendida como um instrumento meramente operacional, mas como uma medida jurídico-investigativa de caráter excepcional, cuja legitimidade depende da estrita observância dos limites legais e das garantias fundamentais.

Além do mais, quanto à evolução dos crimes cibernéticos e às especificidades da ciberpedofilia, é notório que a estrutura descentralizada, anônima e desterritorializada da internet impôs novos desafios ao sistema de justiça criminal, exigindo a adequação das estratégias de investigação. Nesse contexto, a infiltração policial virtual surge como resposta necessária à dificuldade de acesso a ambientes fechados e protegidos, nos quais se desenvolvem práticas altamente lesivas à dignidade sexual de crianças e adolescentes.

Contudo, também se demonstrou que a utilização dessa técnica não está isenta de riscos jurídicos e probatórios. A possibilidade de violação à intimidade, o perigo do flagrante preparado, a fragilidade das provas digitais e a necessidade de preservação rigorosa da cadeia de custódia são elementos que impõem uma atuação extremamente cautelosa por parte do Estado. Assim, a infiltração, para que seja legítima e eficaz, deve ser necessariamente condicionada à autorização judicial fundamentada, ao princípio da proporcionalidade, à atuação não provocadora do agente e ao cumprimento integral dos protocolos técnico-periciais.

Ademais, os desafios tecnológicos e psicossociais enfrentados pelos agentes infiltrados, bem como a imprescindibilidade da cooperação internacional, evidenciam que o enfrentamento da exploração sexual infantil no ambiente digital ultrapassa o

campo estritamente jurídico, exigindo uma resposta multidisciplinar que envolva tecnologia, psicologia, políticas públicas de proteção infantojuvenil e fortalecimento das instituições de segurança e justiça.

Em vista disso, a infiltração policial virtual, quando corretamente aplicada, representa importante instrumento de proteção da infância e da adolescência, sem afastar, contudo, os limites impostos pelo Estado Democrático de Direito e pelos direitos fundamentais.

5. REFERÊNCIAS

BILCHES, William. Alerta aos pais: pedofilia virtual aumenta no Brasil em meio à pandemia. Gazeta do Povo, Curitiba, 20 maio 2020. Disponível em:

<https://www.gazetadopovo.com.br/vida-e-cidadania/alerta-aos-pais-pedofilia-virtual-aumenta-no-brasil-em-meio-a-pandemia/>. Acesso em: 10 out. 2025.

BOAVENTURA, F. E.; FIGUEIREDO, A. L. A. Crimes sexuais virtuais contra crianças e adolescentes. Observatório de la Economía Latinoamericana, [S. l.], v. 23, n. 11, p. e12112, 2025. DOI: 10.55905/oelv23n11-020. Disponível em:

<https://ojs.observatoriolatinoamericano.com/ojs/index.php/olel/article/view/12112>. Acesso em: 1 nov. 2025.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em:

http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 10 out. 2025.

_____. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Brasília, DF: Presidência da República, 1941. Disponível em:

https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 11 out. 2025.

_____. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente. Brasília, DF: Presidência da República, 1990. Disponível em:

https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 10 out. 2025.

_____. Lei nº 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal. Brasília, DF: Presidência da República, 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 10 out. 2025.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 out. 2025.

_____. Lei nº 13.441, de 8 de maio de 2017. Altera o Estatuto da Criança e do Adolescente para dispor sobre a infiltração de agentes de polícia na internet. Brasília, DF: Presidência da República, 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13441.htm. Acesso em: 10 out. 2025.

_____. Lei nº 13.964, de 24 de dezembro de 2019. Altera o Código Penal, o Código de Processo Penal e a Lei de Execução Penal. Brasília, DF: Presidência da República, 2019.

Disponível em: https://www.planalto.gov.br/ccivil_03/ato2019-2022/2019/lei/l13964.htm. Acesso em: 20 out. 2025.

_____. Superior Tribunal de Justiça. Agravo regimental no habeas corpus n. 828054/RN. Relator: Min. Joel Ilan Paciornik. 5. Turma. Julgado em 23 abr. 2024. DJe 29 abr. 2024. Disponível em:

https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=242041837®istro_numero=202301896150&peticao_numero=202300906480&publicacao_data=20240429&formato=PDF. Acesso em: 30 out. 2025.

_____. Superior Tribunal de Justiça. Sexta Turma valida ronda virtual contra pornografia infantil feita por software da polícia. Brasília, DF, 30 out. 2025. Disponível em:

<https://www.stj.jus.br/sites/portalt/Paginas/Comunicacao/Noticias/2025/30102025-Sexta-Turma-valida-ronda-virtual-contr-pornografia-infantil-feita-por-software-da-policia.aspx>. Acesso em: 15 nov. 2025.

_____. Supremo Tribunal Federal. Súmula nº 145. Brasília, DF, 13 dez. 1963. In: SUPREMO TRIBUNAL FEDERAL. Súmulas do STF. Brasília, DF: STF, 1963. Disponível em: <https://portal.stf.jus.br/jurisprudencia/sumariosumulas.asp?base=30&sumula=2119>. Acesso em: 13 out. 2025.

CASTRO, Henrique Hoffmann Monteiro de. Lei 13.441/17 instituiu a infiltração policial virtual. Revista Consultor Jurídico, São Paulo, 16 maio 2017. Disponível em:

<https://www.conjur.com.br/2017-mai-16/academia-policia-lei-1344117-instituiu-infiltracao-policial-virtual/>. Acesso em: 4 nov. 2025.

CRESPO, Marcelo Xavier. Crimes digitais. São Paulo: Saraiva, 2011.

FISBERG, Yuri. Função 'hash' e a integridade da prova digital. Revista Brasileira de Direito Processual Penal, v. 11, n. 3, 2025. Disponível em:

<https://revista.ibraspp.com.br/RBDPP/article/view/1227/590>. Acesso em: 11 out. 2025.

HENRIQUES, Júlia Nunes. Trabalhar com crianças abusadas: reflexos na saúde física e psicológica dos policiais. 2025. Dissertação (Mestrado em Segurança Pública) – Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa, 2025. Disponível em:

<https://comum.rcaap.pt/entities/publication/18c1c02a-f683-47fa-b5ce-c00f7fd4e7e0#:~:text=ACESSO%20ABERTO-,http%3A//hdl.handle.net/10400.26/58413,-Utilize%20este%20identificador>. Acesso em: 30 out. 2025.

INTERNET WATCH FOUNDATION (IWF). Commercial dark web URLs. 2024. Disponível em: <https://www.iwf.org.uk/annual-data-insights-report-2024/data-and-insights/commercial-dark-web-urls/>. Acesso em: 13 out. 2025.

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN (NCMEC). CyberTipline Data. 2024. Disponível em:

<https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata>. Acesso em: 11 out. 2025.

PEREIRA, Maria Clara Hage. Infiltração policial e investigação da criminalidade organizada: garantismo e eficiência. 2022. Dissertação (Mestrado em Direito Processual) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2022. Disponível em: <https://teses-dev.sc.usp.br/teses/disponiveis/2/2137/tde-16112022-125116/publico/10670192MIO.pdf>.

Acesso em: 01 nov. 2025.

ROVINSKI, S. L.; PELISOLI, C. D. Violência sexual contra crianças e adolescentes: testemunho e avaliação psicológica. São Paulo: Vetor, 2020.

SAFERNET BRASIL. Relatório anual 2024: denúncias de exploração sexual infantil online no Brasil. São Paulo: SaferNet Brasil, 2025. Disponível em: <https://new.safernet.org.br/content/denuncias-safernet-de-abuso-e-exploracao-sexual-infantil-na-internet-aumentam-114-apos-video>. Acesso em: 7 set. 2025.