

IX ENCONTRO VIRTUAL DO CONPEDI

**INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA
E INTERNACIONAL**

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFRSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Ednilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Educação Jurídica

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

I61

Internet: dinâmicas da segurança pública internacional [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Tatiana Stroppa; Valter Moura do Carmo – Florianópolis: CONPEDI, 2026.

Inclui bibliografia

ISBN: 978-65-5274-568-2

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Internet. 3. Segurança pública internacional. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34



IX ENCONTRO VIRTUAL DO CONPEDI

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

Apresentação

Apresentação

O IX Encontro Virtual do CONPEDI, realizado entre os dias 22 e 26 de junho de 2026, reafirmou o compromisso da entidade com a promoção da pesquisa jurídica de excelência, reunindo pesquisadoras, pesquisadores, docentes, discentes e profissionais do Direito de diversas instituições brasileiras e estrangeiras em um espaço dedicado ao debate científico e à difusão do conhecimento. Nesta edição, cujo tema foi "Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos", o evento proporcionou reflexões sobre os desafios contemporâneos enfrentados pelo Estado, pelas instituições e pela sociedade na concretização dos direitos fundamentais.

Inserido nesse contexto, o Grupo de Trabalho Internet: Dinâmicas da Segurança Pública e Internacional I, coordenado por Tatiana Stroppa e Valter Moura do Carmo, proporcionou um ambiente de diálogo interdisciplinar acerca de alguns dos mais relevantes desafios decorrentes da transformação digital. As discussões evidenciaram que o desenvolvimento das tecnologias da informação, da inteligência artificial e dos sistemas algorítmicos tem produzido impactos significativos sobre a segurança pública, a proteção nacional e internacional dos direitos humanos, a tutela dos direitos da personalidade e a própria conformação do Estado Democrático de Direito. Partindo desse diagnóstico, as reflexões avançaram pela análise de como equilibrar a necessária atuação estatal diante das mudanças promovidas pelas e nas plataformas digitais, dinâmicas que impõem ao Direito a necessidade de constante atualização de seus instrumentos normativos e interpretativos.

3. ECA Digital (Lei 15.211/2025): Governança, Lacunas Normativas e Justiça Interseccional na Proteção da Infância em Ambientes Digitais, de Lizeth Nataly Delgado Villota, Thaís Agnoletti Alcova e Fernando de Brito Alves;

4. O Combate ao Crime de Pornografia Infantil e o Uso de Ronda Virtual: uma Leitura a partir da Jurisprudência do Superior Tribunal de Justiça, de Henrique Bassi da Silva e Gustavo Henrique de Andrade Cordeiro;

5. Proteção de Dados Pessoais e Regulação Digital: Reflexões sobre a ANPD e as Big Techs, de Márcia Haydée Porto de Carvalho, Alexsandro José Rabelo França e Pedro Bergê Cutrim Filho;

6. Tecnificação da Violência Sexual Infantil: a Mercantilização dos Robôs Sexuais, de Isabel Borderes Motta e Jacqueline Valadares da Silva Alckmim; e

7. Violência Psicológica contra a Mulher em Ambientes Digitais: Revitimização Algorítmica e a (In)Suficiência da Resposta Jurisdicional Brasileira, de Hudson Luiz França Mancilha e Vivianne Rigoldi.

Em conjunto, os artigos demonstram que as questões relacionadas à internet e às tecnologias digitais ultrapassam os limites tradicionais dos diversos ramos do Direito, exigindo abordagens capazes de integrar perspectivas oriundas do Direito Constitucional, do Direito Digital, do Direito Penal, da proteção de dados pessoais, dos direitos humanos e da regulação econômica. Ao mesmo tempo, evidenciam que a construção de mecanismos jurídicos aptos a compatibilizar inovação tecnológica, segurança pública e proteção dos direitos fundamentais constitui uma das agendas mais relevantes da pesquisa jurídica contemporânea e que exigirá o comprometimento não apenas dos Estados, mas das próprias plataformas digitais, grupos de interesse, sociedade civil e da comunidade acadêmica na busca de modos para vivenciar

Espera-se que os estudos ora publicados contribuam para o aprofundamento das reflexões acerca das relações entre tecnologia, segurança pública, segurança internacional e direitos fundamentais, estimulando novas pesquisas e fortalecendo o desenvolvimento desse importante campo de investigação jurídica.

Boa leitura!

Profa. Dra. Tatiana Stroppa

Centro Universitário de Bauru - Instituição Toledo de Ensino

Prof. Dr. Valter Moura do Carmo

Escola Superior da Magistratura Tocantinense (ESMAT)

O COMBATE AO CRIME DE PORNOGRAFIA INFANTIL E O USO DE RONDA VIRTUAL: UMA LEITURA A PARTIR DA JURISPRUDÊNCIA DO SUPERIOR TRIBUNAL DE JUSTIÇA

COMBATING CHILD PORNOGRAPHY CRIMES AND THE USE OF CYBER PATROLS: AN ANALYSIS BASED ON THE JURISPRUDENCE OF THE SUPERIOR COURT OF JUSTICE

Henrique Bassi Da Silva ¹

Gustavo Henrique de Andrade Cordeiro ²

Resumo

O presente artigo analisa o combate ao crime de pornografia infantil no ambiente digital, com especial atenção ao uso da chamada ronda virtual e à distinção desse mecanismo em relação à infiltração policial virtual prevista no Estatuto da Criança e do Adolescente, a partir da interpretação conferida pelo Superior Tribunal de Justiça. Parte-se da constatação de que o avanço das tecnologias da informação ampliou significativamente a prática de crimes contra a dignidade sexual de crianças e adolescentes, exigindo do Estado novas técnicas investigativas compatíveis com a dinâmica do meio cibernético. Nesse contexto, a Lei nº 13.441/2017 introduziu, no ECA, a possibilidade de infiltração de agentes de polícia na internet, mediante autorização judicial, como instrumento excepcional de obtenção de provas. Paralelamente, difundiu-se o uso de softwares de varredura em redes abertas de compartilhamento de arquivos, especialmente em redes peer-to-peer, utilizados para identificar endereços IP associados ao armazenamento ou compartilhamento de material pornográfico infantil, prática denominada ronda virtual. O artigo examina se a utilização desses programas configura infiltração policial virtual e, conseqüentemente, se demandaria prévia autorização judicial. Por meio de pesquisa bibliográfica, análise legislativa e estudo da jurisprudência recente do Superior Tribunal de Justiça, conclui-se que a Corte firmou entendimento no sentido de que a ronda virtual não se confunde com a infiltração prevista no art. 190-A do ECA, por se tratar de coleta automatizada de dados disponibilizados em ambiente digital aberto e acessível a qualquer usuário.

particular emphasis on the use of virtual patrol techniques and their distinction from virtual undercover investigations provided for in the Brazilian Child and Adolescent Statute, based on the interpretation adopted by the Superior Court of Justice (STJ). It starts from the premise that technological advances have significantly increased crimes against the sexual dignity of children and adolescents, requiring the State to adopt investigative methods compatible with the dynamics of cyberspace. In this context, Law No. 13,441/2017 introduced the possibility of virtual undercover police operations, subject to prior judicial authorization, as an exceptional evidentiary technique. At the same time, law enforcement agencies have increasingly used software tools to scan open peer-to-peer networks in order to identify IP addresses associated with the storage or sharing of child sexual abuse material, a practice known as virtual patrol. The article examines whether the use of such software constitutes a form of undercover investigation and therefore requires judicial authorization. Through bibliographic research, legislative analysis, and the examination of recent case law from the Superior Court of Justice, the study concludes that the Court has held that virtual patrol does not equate to the undercover investigations regulated by Article 190-A of the Child and Adolescent Statute, as it involves the automated collection of data made publicly available in open digital environments.

Keywords/Palabras-claves/Mots-clés: Child pornography, Virtual patrol, Virtual undercover investigation, Digital evidence, Superior court of justice

Introdução

O desenvolvimento acelerado das tecnologias digitais e a ampla difusão do acesso à internet transformaram profundamente as formas de interação social, comunicação e circulação de informações.

Paralelamente aos benefícios proporcionados por esse avanço, o ambiente virtual passou a ser utilizado como espaço propício para a prática de diversas modalidades de crimes, especialmente aqueles que envolvem a exploração sexual de crianças e adolescentes.

A pornografia infantil, em particular, encontrou no meio digital um terreno fértil para sua expansão, seja pelo armazenamento e compartilhamento de arquivos ilícitos, seja pela atuação de redes organizadas que se utilizam do anonimato e da descentralização da internet para dificultar a persecução penal.

Diante dessa realidade, o enfrentamento desses crimes tornou-se um dos maiores desafios contemporâneos para o sistema de justiça criminal.

Nesse cenário, o ordenamento jurídico brasileiro passou a incorporar técnicas especiais de investigação, visando conferir maior efetividade à atuação estatal. A infiltração de agentes, já prevista em diplomas como a Lei de Drogas e a Lei de Organização Criminosa, foi adaptada ao ambiente digital por meio da Lei nº 13.441/2017, que inseriu no Estatuto da Criança e do Adolescente dispositivos específicos sobre a infiltração policial virtual.

A infiltração cibernética, entretanto, possui caráter excepcional e está condicionada a rigorosos requisitos legais, como a demonstração de sua necessidade e a prévia autorização judicial, justamente por implicar riscos relevantes aos direitos fundamentais à intimidade, à privacidade e ao devido processo legal.

Concomitantemente a esse instrumento, as forças de segurança passaram a empregar softwares capazes de realizar varreduras automáticas em redes abertas de compartilhamento de arquivos, especialmente em redes peer-to-peer, com o objetivo de identificar indícios da prática de crimes relacionados à pornografia infantil. Essa técnica passou a ser conhecida como ronda virtual.

A utilização desses programas suscitou intenso debate jurídico acerca da licitude das provas obtidas e da necessidade, ou não, de autorização judicial prévia, sobretudo diante da alegação de que tal prática configuraria uma forma disfarçada de infiltração policial virtual.

A controvérsia alcançou o Superior Tribunal de Justiça, que foi instado a se manifestar sobre a natureza jurídica da ronda virtual e seus limites constitucionais, especialmente no que se refere à distinção entre a coleta de dados em ambientes digitais abertos e a atuação infiltrada em espaços virtuais restritos.

Diante disso, o presente artigo tem como objetivo analisar a utilização da ronda virtual no combate ao crime de pornografia infantil, à luz da legislação vigente e da jurisprudência do Superior Tribunal de Justiça, buscando verificar se essa técnica investigativa se enquadra no conceito legal de infiltração policial virtual e se demanda autorização judicial prévia.

1. A infiltração de agentes para investigações de crimes no ordenamento jurídico brasileiro

A Lei 13.441, de 8 de maio de 2017, alterou o Estatuto da Criança e do Adolescente (especificamente artigos 190-A a 190-E) para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente, isto é, instituiu a infiltração da polícia virtual.

Ressalta-se que a novidade não foi a instituição da figura do agente infiltrado, eis que a figura já era prevista no art. 53, I, da Lei de Drogas, bem como no art. 10 da Lei 12.850/13 e artigo 20 da Convenção de Palermo (Decreto 5.015/04).

Logo, a alteração no ECA tratou-se de uma normatização dessa técnica investigativa contra crimes cibernéticos.

Segundo Nucci (2016, p. 724), a infiltração policial:

Representa uma penetração, em algum lugar ou coisa, de maneira lenta, pouco a pouco, correndo pelos seus meandros. Tal como a infiltração de água, que segue seu caminho pelas pequenas rachaduras de uma laje ou parede, sem ser percebida, o objetivo deste meio de captação de prova tem idêntico perfil.

Renato Brasileiro de Lima (2016, p. 571), destaca que o conceito de infiltração de agentes guarda algumas características que são inerentes, segundo o qual

O agente infiltrado é introduzido dissimuladamente em uma organização criminosa, passando a agir como um de seus integrantes, ocultando sua verdadeira identidade, com o objetivo precípuo de identificar fontes de prova e obter elementos de informação capazes de permitir a desarticulação da referida associação.

No âmbito do Direito Internacional, a Convenção das Nações Unidas contra o Crime Organizado Transnacional, conhecida como “Convenção de Palermo” (promulgada pelo Decreto 5.015/2004), menciona a infiltração de agentes através do artigo 20:

Se os princípios fundamentais do seu ordenamento jurídico nacional o permitirem, cada Estado Parte, tendo em conta as suas possibilidades e em conformidade com as condições prescritas no seu direito interno, adotará as medidas necessárias para permitir o recurso apropriado a entregas vigiadas e, quando o considere adequado, o recurso a outras técnicas especiais de investigação, como a vigilância eletrônica ou outras formas de vigilância e as operações de infiltração, por parte das autoridades competentes no seu território, a fim de combater eficazmente a criminalidade organizada.

Para o combate ao tráfico de drogas, a Lei 11.343/06 instituiu, no artigo 53, I, a possibilidade de infiltração de agentes de polícia em tarefas de investigação:

Art. 53. Em qualquer fase da persecução criminal relativa aos crimes previstos nesta Lei, são permitidos, além dos previstos em lei, mediante autorização judicial e ouvido o Ministério Público, os seguintes procedimentos investigatórios:

I - a infiltração por agentes de polícia, em tarefas de investigação, constituída pelos órgãos especializados pertinentes.

Nos crimes que envolvam organização criminosa, a infiltração de agentes policiais e seu procedimento estão previstos no capítulo II, seção III, entre os artigos 10 a 14 da Lei 12.850/2013, destacando-se o artigo 10-A, acrescentado à Lei através do “Pacote Anticrime” em 2019, prevendo que

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

Vale notar também que a infiltração de agentes para investigação de crimes pode se dar durante toda persecução penal, podendo tanto o Delegado de Polícia representar ao juiz no âmbito do inquérito policial, como o promotor de justiça (também no inquérito) e na fase processual.

Gomes e Silva (2015, p. 409) destacam que “é recomendável que ao representar pela infiltração, o delegado de polícia também represente pela autorização de que o agente encoberto proceda à apreensão de documentos, realize filmagens etc.”

Imprescindível apontar também a necessidade de sigilo com relação ao pedido de infiltração (art. 12 da Lei 12.850/2013), sob pena de responder criminalmente em caso de descumprimento (art. 20 da Lei 12.850/2013):

Art. 12. O pedido de infiltração será sigilosamente distribuído, de forma a não conter informações que possam indicar a operação a ser efetivada ou identificar o agente que será infiltrado.

§ 1º As informações quanto à necessidade da operação de infiltração serão dirigidas diretamente ao juiz competente, que decidirá no prazo de 24 (vinte e quatro) horas, após manifestação do Ministério Público na hipótese de representação do delegado de polícia, devendo-se adotar as medidas necessárias para o êxito das investigações e a segurança do agente infiltrado.

§ 2º Os autos contendo as informações da operação de infiltração acompanharão a denúncia do Ministério Público, quando serão disponibilizados à defesa, assegurando-se a preservação da identidade do agente.

§ 3º Havendo indícios seguros de que o agente infiltrado sofre risco iminente, a operação será sustada mediante requisição do Ministério Público ou pelo delegado de polícia, dando-se imediata ciência ao Ministério Público e à autoridade judicial.

Art. 20. Descumprir determinação de sigilo das investigações que envolvam a ação controlada e a infiltração de agentes:

Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa.

Por fim, a doutrina destaca que a infiltração de agentes pode ser classificada em duas modalidades: a infiltração leve, com duração máxima de seis meses e que exige menos engajamento por parte do agente infiltrado, bem como a infiltração profunda, que se desenvolve por mais de seis meses, exigindo total imersão no bojo da organização criminosa, sendo que o agente infiltrado assume outra identidade e praticamente não mantém contato nem com sua família (Masson; Marçal, 2017, p. 318).

Contudo, impende anotar que a necessidade de renovação do prazo deve ser devidamente demonstrada pela autoridade que a provocar, cabendo ao juiz decidir fundamentadamente em todos os casos, das Cortes Superiores em analogia com a Lei de Interceptação Telefônica (STJ - AgRg no AREsp: 2293848 MG 2023/0039015-3, Relator.: Ministro RIBEIRO DANTAS, Data de Julgamento: 28/11/2023, T5 - QUINTA TURMA, Data de Publicação: DJe 05/12/2023):

PENAL E PROCESSUAL PENAL. AGRAVO REGIMENTAL. AGRAVO EM RECURSO ESPECIAL. TRÁFICO DE DROGAS. INTERCEPTAÇÃO TELEFÔNICA. OBSERVÂNCIA DOS REQUISITOS LEGAIS. FUNDAMENTAÇÃO CONCRETA. NULIDADE NÃO DEMONSTRADA. LICITUDE DAS PRORROGAÇÕES. AGRAVO REGIMENTAL NÃO PROVIDO. 1. O art. 5º da Lei n. 9.296/1996 determina, quanto à autorização judicial de interceptação telefônica, que "a decisão será fundamentada, sob pena de nulidade, indicando também a forma de execução da diligência, que não poderá exceder o prazo de quinze dias, renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova". 2. Na hipótese, não se sustenta a alegação no sentido de que as decisões careceriam de fundamentação idônea, bem como que as prorrogações foram autorizadas a partir de mera reprodução da decisão antecedente, restando evidente que a medida foi deferida com fundamento na situação concreta apresentada, levando em conta, especialmente, a impossibilidade de obtenção de prova pelos meios investigativos previamente realizados. 3. Conforme tese firmada em repercussão geral pelo Supremo Tribunal Federal, no Tema n. 661/STF, "São lícitas as sucessivas renovações de interceptação telefônica, desde que, verificados os requisitos do artigo 2º da Lei n. 9.296/1996 e demonstrada a necessidade da medida diante de elementos concretos e a complexidade da investigação, a decisão judicial inicial e as prorrogações sejam devidamente motivadas, com justificativa legítima, ainda que sucinta, a embasar a continuidade das investigações". 4. Agravo regimental a que se nega provimento.

Destarte, note-se que a infiltração de agentes no combate ao crime não é novidade no ordenamento jurídico brasileiro, sendo que a Lei 13.441/17 contribuiu com avanços ao combate a pornografia infantil instituindo no Estatuto da Criança e do Adolescente a infiltração de polícia virtual, normatizando essa técnica investigativa contra crimes cibernéticos que envolvam criança e adolescente.

2. A infiltração virtual de agentes no Estatuto da Criança e do Adolescente

A infiltração de agentes, a partir da Lei 13.441/2017 – que acrescentou os artigos 190-A a 190-E no ECA – criou-se no ordenamento jurídico brasileiro mais uma modalidade, a chamada infiltração policial virtual, caracterizada por ser efetuada neste ambiente, qual seja, na *internet*.

Como exposto anteriormente, até o advento da Lei promulgada em 2017, existia apenas as modalidades de infiltração previstas na Lei de Drogas e na Convenção de Palermo, as quais discorriam sobre a infiltração em ambiente físico. Assim, a instituição de agente infiltrado no Estatuto da Criança e do Adolescente não foi novidade, mas a consolidação dessa técnica investigativa em meio cibernético.

A legislação de 2017 trouxe no artigo 190-A os crimes que o agente de polícia pode investigar no ambiente virtual e, neste ponto, a doutrina ainda discute se esse rol é taxativo ou exemplificativo. Francisco Sannini Neto (2017) elucida que é taxativo, em razão do caráter excepcional do procedimento.

Já a outra vertente, defende ser um rol exemplificativo, pois o princípio da proteção deficiente e livre iniciativa probatória justificam o emprego dessa técnica investigativa quando necessária para elucidar crimes graves cometidos no ambiente virtual (LEITÃO JUNIOR, 2017).

Segundo o artigo 190-A do Estatuto da Criança e do Adolescente, a infiltração policial virtual é admitida basicamente em três categorias de crimes: na pedofilia envolvendo fotos, registros, vídeos, armazenamento, disponibilização de conteúdo pornográfico sobre criança/adolescente, bem como o aliciamento de criança com o fim de praticar ato libidinoso (arts. 240¹, 241², 241-A³, 241-B⁴, 241-C⁵ E 241-D⁶ do ECA).

Nos delitos contra a dignidade sexual de vulneráveis: estupro de vulnerável (artigo 217-A do Código Penal), corrupção de menores induzindo a satisfazer a lascívia de outrem (artigo 218 do Código Penal), satisfação de lascívia mediante a presença de criança ou adolescente (artigo 218-A do Código Penal) e favorecimento da prostituição ou de outra forma de exploração sexual de criança ou adolescente ou de vulnerável. (artigo 218-B do Código Penal).

Ademais, admite-se também a infiltração para combater o crime de invasão de dispositivo informático (art. 154-A do Código Penal⁷).

¹ Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.

² Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.

³ Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.

⁴ Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

⁵ Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

⁶ Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

⁷ Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do

Tem-se como requisitos a infiltração policial cibernética o *fumus commissi delicti* (indícios suficientes da existência de determinado crime – àqueles previstos no art. 190-A do ECA), bem como o *periculum in mora*, ou seja, risco à investigação ou ordem pública se a medida não for realizada.

Além disso, a infiltração de agentes de polícia na *internet* não será admitida se a prova puder ser obtida por outros meios (art. 190-A, §3º, do ECA), sendo, portanto, necessário demonstrar a necessidade da medida.

Existem também mais algumas regras a serem observadas para a infiltração cibernética policial (art. 190-A, I, II e III, do ECA): será precedida de autorização judicial devidamente circunstanciada e fundamentada, que estabelecerá os limites da infiltração para obtenção de prova, ouvido o Ministério Público; dar-se-á mediante requerimento do Ministério Público ou representação de delegado de polícia e conterá a demonstração de sua necessidade, 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; não poderá exceder o prazo de 90 (noventa) dias, sem prejuízo de eventuais renovações, desde que o total não exceda a 720 (setecentos e vinte) dias e seja demonstrada sua efetiva necessidade, a critério da autoridade judicial.

A doutrina também destaca ser necessária manifestação técnica do delegado de polícia, ressaltando que a autoridade policial deve expor sua concordância (como estabeleceu o artigo 10 da Lei 12.850/2013), tendo em vista que, por ser “presidente” do inquérito policial, “pode dizer se há ou não há quadro técnico pronto para este tipo de missão” (GOMES; SILVA, 2015, p. 403).

Fábio Roque, Nestor Távora e Rosmar Rodrigues Alencar (2016, p. 626) salientam também que a autoridade policial possui:

maiores condições de aquilatar a viabilidade de uma medida desta natureza. Com efeito, de nada adiantaria as boas intenções ministeriais no sentido da autorização judicial se o delegado demonstra, por exemplo, que a possibilidade de o agente vir a ser descoberto é muito grande.

Sobre o prazo máximo, há um ponto controverso: ao mesmo tempo que a infiltração não deve ser eterna, já que nenhuma investigação tem esse condão, existe uma

usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

crítica sobre o total de 720, uma vez que as redes criminosas que envolvem pedofilia na *internet* são extremamente fechadas e restritas.

Assim, os policiais podem não conseguir se infiltrar facilmente no meio desses grupos, considerando que os criminosos se cercam de várias cautelas e não admitem participação de qualquer pessoa, salvo após um longo período para ganhar adquirir confiança (CAVALCANTE, 2016).

Além disso, a Lei de Organização Criminosa não prevê limite máximo de infiltração de agentes, permitindo que elas ocorram tantas vezes que forem necessárias (art. 10, §3º, Lei 12.850/2013): “A infiltração será autorizada pelo prazo de até 6 (seis) meses, sem prejuízo de eventuais renovações, desde que comprovada sua necessidade”.

O artigo 190-B prevê também que as informações da operação de infiltração serão encaminhadas diretamente ao juiz responsável pela autorização da medida, que zelará por seu sigilo. Seu parágrafo único dispõe que “Antes da conclusão da operação, o acesso aos autos será reservado ao juiz, ao Ministério Público e ao delegado de polícia responsável pela operação, com o objetivo de garantir o sigilo das investigações”.

Destarte, considerando o dispositivo 190-B do ECA somado a Súmula Vinculante 14 do STF⁸, podemos concluir que o “contraditório” é diferido (postergado), mormente porque somente após o encerramento da diligência a defesa técnica terá oportunidade de acessar as provas e relatórios feitos a partir da infiltração.

O artigo 190-C do ECA exclui a ilicitude do policial que oculta a sua identidade para, por meio da *internet*, colher indícios de autoria e materialidade dos crimes dispostos no art. 190-A do Estatuto. Assim, a criação de perfil *fake* continua sendo admitida sem autorização judicial para coleta de dados em fontes abertas, sobretudo porque para interagir na *internet*, o usuário aceita renunciar grande parte de sua privacidade (SILVA, 2016).

De igual maneira, não responde pelo crime previsto no art. 307 do Código Penal (falsa identidade), mormente porque o tipo penal demanda finalidade de obtenção de vantagem ou causar dano.

Para fins da presente pesquisa, destaca-se a necessidade (ou não) de autorização judicial para a obtenção de prova do crime de pornografia infantil quando a “infiltração cibernética” é feita através de *software* que “varre” continuamente a *internet* em busca de

⁸ É direito do defensor, no interesse do representado, ter acesso amplo aos elementos de prova que, já documentados em procedimento investigatório realizado por órgão com competência de polícia judiciária, digam respeito ao exercício do direito de defesa.

indícios dos crimes previstos no artigo 240-A e 240-B do ECA, atinente ao armazenamento ou compartilhamento de material de pornografia infantil.

2.1. Ronda virtual e o uso de software para coletar dados na *internet*

No âmbito do combate ao crime de pornografia infantil, a polícia usa frequentemente um tipo de software (o mais popular se trata do *Child Rescue Coalition*) para realizar uma “ronda virtual” em redes *peer-to-peer* (P2P), ou seja, redes de troca ponto a ponto.

Exemplificando, quando alguém baixa um arquivo via *torrent* está utilizando uma rede P2P. Antigamente, era comum de se baixar músicas, por exemplo, via eMule, Ares, que são programas clássicos de compartilhamento de arquivos P2P, no qual o compartilhamento é público e, em tese, voluntário, uma vez que ao baixar um arquivo o usuário está expondo esses arquivos e seu endereço de IP a todos os demais participantes da rede.

Aqui, realiza-se uma crítica: muitos usuários não fazem ideia de que baixando uma música (via eMule, por exemplo), ela fica disponível para qualquer pessoa realizar o *download*.

Por isso é importante destacar que o “compartilhamento” não é totalmente voluntário, exigindo-se um mínimo probatório e muita cautela para investigar, processar e – muito mais - condenar uma pessoa, por exemplo, pelo crime de compartilhamento (art. 241-A do ECA) se ela tão somente realizou o *download* do conteúdo pornográfico para “consumir” e/ou armazenar⁹.

Pois bem. E como funciona esse *software*? A polícia investigativa opera ele dentro das redes P2P. Assim, sem autorização judicial o *software* realiza uma varredura nas redes P2P para coletar dados de quem está consumindo/compartilhando pornografia infantil para ensinar, por exemplo, um pedido de busca e apreensão.

E desta maneira surge o problema: considerando que um policial está “operando” o *software* na rede P2P, seria uma infiltração de agente no mundo cibernético sem autorização judicial?

⁹ Esta conduta se amoldaria a prevista no art. 241-B do ECA: “adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente”, que tem uma pena menor do que a disposta no 241-A.

3. Leitura do Superior Tribunal de Justiça sobre o uso da ronda virtual no combate a pornografia infantil

A discussão chegou ao Superior Tribunal de Justiça no final de 2025.

No caso, a defesa técnica sustentou a ilicitude das provas obtidas na busca e apreensão, vez que esta medida apenas se ensejou com o uso anterior do *software* CRC - ferramenta internacional de uso restrito a agentes públicos certificados – para rastrear IPs associados ao compartilhamento de arquivos ilícitos, sem autorização judicial.

Assim, a defesa argumentou que o uso do *software* configuraria infiltração policial sem autorização judicial.

Todavia, o Superior Tribunal de Justiça fundamentou que a ronda virtual não se confunde com a infiltração policial prevista no artigo 190-A do Estatuto da Criança e do Adolescente.

O Ministro Rogério Schietti (STJ, 2025, Informativo 870 - Processo em segredo de justiça, Rel. Ministro Rogerio Schietti Cruz, Sexta Turma, por unanimidade, julgado em 14/10/2025) elucidou que na infiltração há atuação direta de agente oculto em ambiente fechado, voltado a alvos específicos. Já na ronda virtual, o *software* apenas rastreia automaticamente arquivos em redes abertas, acessando dados que qualquer usuário daquelas plataformas pode visualizar:

Não se trata, portanto, de invasão a espaço privado ou interceptação de comunicações que exigiria prévia autorização judicial, mas de coleta de informações disponíveis em ambiente compartilhado. O *software* utilizado pelos investigadores opera como qualquer outro cliente P2P, acessando apenas informações que qualquer usuário da rede poderia obter.¹⁰

Assim, restou destacado que o uso de software de ronda virtual para localização de material relacionado a pornografia infantil, como o da *Child Rescue Coalition* (CRC)

não se confunde com a figura prevista no art. 190-A do Estatuto da Criança e do Adolescente, inserida pela Lei n. 13.441/2017. A infiltração policial na internet, nos termos do ECA, consiste em uma técnica especial de investigação em que um agente policial oculta sua

¹⁰ BRASIL. Superior Tribunal de Justiça. Informativo nº 870, do dia 11 de novembro de 2025. Disponível em:

<https://scon.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=%270870%27>. Acesso em: 18 de janeiro de 2026. Tema: Pornografia infantil. Rastreamento na internet. Uso do *software* da Child Rescue Coalition (CRC). Autorização judicial prévia. Desnecessidade. Art. 10, § 3º da Lei n. 12.965/2014 (Marco Civil da Internet). Não aplicação do art. 190-A do ECA. Processo em segredo de justiça, Rel. Ministro Rogerio Schietti Cruz, Sexta Turma, por unanimidade, julgado em 14/10/2025.

real identidade e se passa por criminoso, a fim de ingressar em ambiente virtual fechado, buscando alvos, suspeitos da prática de crimes. Dessa forma, a atividade de rastreamento na internet realizada pela polícia civil, por meio do uso de um *software* de busca contínua da *Child Rescue Coalition* (CRC), trata-se de ronda contínua que não se direciona a pessoas determinadas, diferentemente do procedimento da infiltração policial. Além disso, o *software* policial atua em rede aberta, em que o compartilhamento do IP dos usuários é pressuposto da comunidade e é fato de conhecimento de todos os seus usuários, razão pela qual não se aplica a exigência de prévia ordem judicial, nos termos do art. 190-A, I, do ECA.

Além do mais, a Corte Cidadã também asseverou sobre a legalidade na atuação da Autoridade Policial que, depois de identificar o IP do suspeito com base na ronda virtual, requisita diretamente aos provedores de *internet* as informações cadastrais daquele usuário, uma vez que

A Lei n. 12.965/2014 (Marco Civil da Internet) estabelece proteções diferenciadas para diferentes categorias de dados, sendo mais rigorosa quanto ao conteúdo das comunicações e mais flexível quanto aos dados cadastrais objetivos. Conforme expressamente previsto em seu art. 10, § 3º da Lei n. 12.965/2014¹¹, o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço é permitido diretamente às autoridades administrativas competentes, sem necessidade de ordem judicial.

Portanto, diante da lacuna legislativa sobre o uso de *software* para coletar informações que são públicas, o STJ firmou o entendimento de que é prescindível a autorização judicial prévia.

Sob essa ótica, a técnica da ronda virtual qualifica-se como uma atividade de inteligência ostensiva que se harmoniza com a nova morfologia do espaço público na Era Digital.

A distinção clássica entre o 'público' e o 'privado' sofreu uma reconfiguração ontológica: no ambiente das redes P2P, a publicidade é um pressuposto funcional da

¹¹ Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

plataforma, ainda que, muitas vezes, o usuário comum careça de plena ciência técnica sobre os mecanismos de compartilhamento automático inerentes ao sistema.

Independentemente do dolo ou do conhecimento específico sobre a arquitetura da rede, o fato objetivo é que a utilização dessas ferramentas implica na exposição de dados de conexão (como o endereço de IP) a uma coletividade indeterminada de usuários.

Portanto, ao ingressar em um ecossistema de troca ponto a ponto, o indivíduo situa-se em uma zona de visibilidade pública que mitiga a expectativa legítima de privacidade sobre os rastros digitais ali deixados.

Ademais, é imperioso sublinhar que, diante da sofisticação da criminalidade cibernética e da gravidade dos delitos de pornografia infantil, o Estado possui o dever de progressividade tecnológica.

Em um cenário onde redes de exploração utilizam algoritmos para a disseminação de conteúdos atroz, seria um contrassenso jurídico impor à Polícia Judiciária amarras que ignorem o avanço da Inteligência Artificial.

Deste modo, exigir autorização judicial para a coleta de dados que, por força da tecnologia escolhida, tornaram-se públicos, representaria um entrave desproporcional à proteção da infância.

Conclusão

A análise desenvolvida ao longo do artigo permitiu constatar que a infiltração de agentes no ordenamento jurídico brasileiro não constitui novidade, tendo sido gradativamente incorporada como técnica especial de investigação em diferentes diplomas legais. A Lei nº 13.441/2017 representou um avanço relevante ao adaptar esse instrumento ao ambiente digital, especialmente para o enfrentamento de crimes contra a dignidade sexual de crianças e adolescentes.

Todavia, verificou-se que a infiltração policial virtual, tal como prevista no Estatuto da Criança e do Adolescente, possui contornos bem definidos e pressupõe a atuação direta e dissimulada de um agente em ambiente virtual fechado, direcionada a alvos específicos e condicionada à prévia autorização judicial, em razão de seu potencial lesivo a direitos fundamentais.

A ronda virtual, por sua vez, apresenta natureza distinta. Conforme consolidado pelo Superior Tribunal de Justiça, trata-se de técnica investigativa baseada na coleta automatizada de informações disponibilizadas em ambientes digitais abertos, acessíveis

a qualquer usuário da rede, não havendo interação direta do agente estatal com os investigados nem invasão de espaços privados.

Nesse sentido, o entendimento firmado pela Corte Superior afasta a equiparação entre a ronda virtual e a infiltração policial virtual, reconhecendo que o uso de softwares de monitoramento em redes públicas prescinde de autorização judicial prévia, desde que respeitados os limites legais e constitucionais.

Tal posicionamento revela-se compatível com a necessidade de conferir efetividade à persecução penal em um contexto de criminalidade digital altamente sofisticada, sem descuidar da proteção aos direitos fundamentais. Exigir autorização judicial para a simples coleta de dados públicos representaria entrave desproporcional à atuação estatal no combate a crimes de extrema gravidade.

Conclui-se, portanto, que a distinção estabelecida pelo Superior Tribunal de Justiça contribui para a segurança jurídica e para o equilíbrio entre eficiência investigativa e garantias constitucionais, reafirmando a legitimidade da ronda virtual como instrumento válido no enfrentamento da pornografia infantil no ambiente digital.

Referências

BRASIL. *Decreto nº 5.015, de 12 de março de 2004*. Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional (Convenção de Palermo). Diário Oficial da União: Brasília, DF, 15 mar. 2004.

BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Diário Oficial da União: Rio de Janeiro, RJ, 31 dez. 1940.

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

BRASIL. *Lei nº 11.343, de 23 de agosto de 2006*. Institui o Sistema Nacional de Políticas Públicas sobre Drogas. Diário Oficial da União: Brasília, DF, 24 ago. 2006.

BRASIL. *Lei nº 12.850, de 2 de agosto de 2013*. Define organização criminosa e dispõe sobre a investigação criminal. Diário Oficial da União: Brasília, DF, 5 ago. 2013.

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: Brasília, DF, 23 abril. 2014

BRASIL. *Lei nº 13.441, de 8 de maio de 2017*. Dispõe sobre a infiltração de agentes de polícia na internet para investigar crimes contra a dignidade sexual de criança e de adolescente. Diário Oficial da União: Brasília, DF, 9 maio 2017.

BRASIL. *Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal (Pacote Anticrime)*. Diário Oficial da União: Brasília, DF, 24 dez. 2019.

BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Agravo em *Recurso Especial nº 2.293.848/MG*, Relator: Ministro Ribeiro Dantas, Quinta Turma, julgado em 28 nov. 2023. Diário da Justiça Eletrônico, Brasília, DF, 5 dez. 2023.

BRASIL. Superior Tribunal de Justiça. *Informativo de Jurisprudência nº 870*, de 11 de novembro de 2025. Tema: Pornografia infantil. Rastreamento na internet. Uso do software da Child Rescue Coalition (CRC). Disponível em: <https://processo.stj.jus.br/jurisprudencia/externo/informativo/?refinar=S+INPATH%28DISP%29&acao=pesquisarumaedicao&aplicacao=informativo&livre=%270870%27.cod.&l=10>. Acesso em: 18 jan. 2026. Processo em segredo de justiça, Rel. Ministro Rogerio Schietti Cruz, Sexta Turma, por unanimidade, julgado em 14/10/2025.

CAVALCANTE, Márcio André Lopes. *Comentários à infiltração de agentes de polícia na internet para investigar crimes contra a dignidade sexual de criança e de adolescente*. Disponível em: <https://www.dizerodireito.com.br/2017/05/comentarios-infiltracao-de-agentes-de.html>. Acesso em: 18 jan. 2026.

GOMES, Luiz Flávio; SILVA, Marcelo Rodrigues. *Organizações criminosas e técnicas especiais de investigação: questões controvertidas, aspectos teóricos e práticos e análise da Lei 12.850/2013*. Salvador: Juspodivm, 2015. p. 409.

GOMES, Luiz Flávio; SILVA, Marcelo Rodrigues da. *Organizações criminosas e técnicas especiais de investigação*. Salvador: Juspodivm, 2015. p. 403.

LEITÃO JÚNIOR, Joaquim. *Infiltração policial na internet da Lei 13.441/17 (dignidade sexual de menores) pode ser usada para outros crimes*. Revista Jus Navigandi, Teresina, ano 22, n. 5063, 12 maio 2017. Disponível em: <https://jus.com.br/artigos/57640>. Acesso em: 17 jan. 2025.

LIMA, Renato Brasileiro de. *Legislação criminal especial comentada*. 4. ed. Salvador: Juspodivm, 2016. p. 571.

MASSON, Cleber; MARÇAL, Vinicius. *Crime organizado*. 3. ed. Rio de Janeiro; São Paulo: Método, 2017. p. 318.

NUCCI, Guilherme de Souza. *Leis penais e processuais comentadas*. 9. ed. v. 2. Rio de Janeiro: Forense, 2016. p. 724.

ROQUE, Fábio; TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. *Legislação criminal para concursos*. Salvador: Juspodivm, 2016. p. 626.

SANNINI NETO, Francisco. *Infiltração virtual de agentes é um avanço nas técnicas especiais de investigação criminal*. Canal Ciências Criminais, maio 2017. Disponível em: <https://canalcienciascriminais.com.br/infiltracao-virtual-agentes>. Acesso em: 17 jan. 2026.

SILVA, Danni Sales. *Da validade processual penal das provas obtidas em sites de relacionamento e a infiltração de agentes policiais no meio virtual*. Revista Brasileira de Ciências Criminais, v. 120, maio/jun. 2016.

SUPREMO TRIBUNAL FEDERAL. *Súmula Vinculante nº 14*. Diário da Justiça Eletrônico, Brasília, DF.