A INFILTRAÇÃO POLICIAL NO ORDENAMENTO JURÍDICO BRASILEIRO: LIMITES E POSSIBILIDADES NO AMBIENTE DA *DEEP WEB*

João Pedro do Nascimento Costenaro
Universidade Federal de Santa Maria (UFSM)

Otávio Augusto Milani Nunes
Universidade Federal de Santa Maria (UFSM)

Isabel Christine Silva de Gregori
Universidade Federal de Santa Maria (UFSM)

RESUMO

O presente trabalho buscou analisar, no ambiente apresentado pela *Deep Web*, em que medida o instrumento da infiltração policial pode se manifestar como uma forma de auxiliar no combate aos crimes que ocorrem nesse ambiente. Para responder a este problema de pesquisa, restou empregado o método de abordagem dedutivo. Ainda, o método de procedimento utilizado na elaboração da pesquisa foi o bibliográfico. Por sua vez, restou utilizada a técnica de pesquisa de elaboração de fichamentos. No primeiro capítulo, colecionou-se conceitos introdutórios acerca do ambiente da *Deep Web*, especialmente relacionados ao seu funcionamento, crimes cometidos e o seu anonimato. No segundo capítulo, analisou-se o arcabouço teórico-normativo da infiltração policial no ordenamento jurídico brasileiro, apontando benefícios no seu uso e dificuldades ainda existentes na sua aplicação em crimes virtuais, principalmente em crimes que ocorrem sob o manto do anonimato fornecido pela *Deep Web*. Concluiu-se que, partindo de um anonimato intrínseco à *Deep Web*, a infiltração policial desponta como uma das principais ferramentas à prevenção e repressão aos crimes virtuais.
Palavras-chave: Anonimato. D*eep web*. Infiltração policial.

POLICE INFILTRATION IN THE BRAZILIAN LEGAL SYSTEM: LIMITES AND POSSIBILITIES IN THE DEEP WEB ENVIRONMENT

ABSTRACT

The present work sought to analyze, in the environment presented by the Deep Web, to what extent the instrument of police infiltration can manifest itself as a way of helping to combat crimes that occur in this environment. In order to respond to this research problem, the deductive method of approach were used. Still, the method of procedure used in the elaboration of the research was the bibliographic one. In turn, the research technique of elaboration of records was used. In the first chapter, introductory concepts about the Deep Web environment were collected, especially related to its operation, crimes committed and its anonymity. In the second chapter, the theoretical-normative framework of police infiltration in the Brazilian legal system was analyzed, pointing out benefits in its use and difficulties still existing in its application in virtual crimes, mainly in crimes that occur under the cloak of anonymity provided by the Deep Web. It was concluded that, starting from an anonymity intrinsic to the Deep Web, police infiltration emerges as one of the main tools for the

prevention and repression of virtual crimes.
Keywords: Anonymity. Deep web. Police infiltration.

Recebido em: 30/01/2023
Aceito em: 18/05/2023

INTRODUÇÃO

A utilização da Internet no cometimento de crimes se encontra no cerne do debate acerca da política de investigação policial perante as novas modalidades de crimes que surgem com a sua popularização. Dessa forma, o estudo do anonimato fornecido pela Internet atrai sujeitos que buscam cometer crimes e precisam de um ambiente propício para suas práticas delituosas.

A *Deep Web* desponta como um cenário ideal para tais práticas criminosas, visto que o anonimato fornecido por ela é ainda maior que o anonimato conferido pela Internet convencional, ou seja, pela *Surface Web*. Para enfrentar a questão, faz-se necessário perquirir de que maneira o instrumento da infiltração policial ocorre em um contexto de dificuldade de investigação dos crimes virtuais, especialmente no âmbito dos crimes cometidos na *Deep Web*. Dessa forma, questiona-se: em que medida, tendo em vista o anonimato conferido pela *Deep Web*, a infiltração policial desponta como uma forma de investigação para os crimes cometidos nesse ambiente?

Para isto, será utilizado o método de abordagem dedutivo, pois o estudo e, consequentemente, a finalização de cada etapa permitirá a percepção de resultados que servirão como base para as etapas subsequentes, partindo de um contexto geral da *Deep Web* para, ao final, analisar um tema específico que se insere nesse ambiente, qual seja, a infiltração policial. Assim, demonstrando uma análise das reflexões que serão realizadas no decorrer dos capítulos, por sua vez, permitindo uma análise acerca da temática do presente artigo científico.

Ainda, o método de procedimento a ser utilizado na elaboração da pesquisa será o bibliográfico. Opta-se por esse método tendo em vista a necessidade de buscar em trabalhos científicos, conceitos e reflexões sobre a temática. Por fim, restará utilizada a técnica de pesquisa de elaboração de fichamentos.

No primeiro capítulo será realizada uma reflexão acerca do fenômeno da *Deep Web*, especialmente acerca do seu uso devido ao anonimato que proporciona ao cometimento de crimes virtuais. Já no segundo capítulo, analisar-se-á a infiltração policial como medida para enfrentar a criminalidade nesse ambiente.

1. A RELAÇÃO ENTRE O USO DA *DEEP WEB* E CRIMES VIRTUAIS: A RAZÃO DO ANONIMATO

Durante a Guerra Fria, período de grandes avanços tecnológicos, inclusive na área da informática, os Estados Unidos da América sentiram-se impelidos a desenvolver um sistema de comunicação entre as bases militares e os departamentos de pesquisa do governo por temerem um ataque repentino da União das Repúblicas Socialistas Soviéticas – URSS. Com efeito, outro servidor paralelo à web comum foi descoberto: a *Deep Web*. Suas origens, até hoje, restam desconhecidas, porém supõe-se que sua criação seja tão antiga quanto à criação da web convencional (ABREU; NICOLAU, 2014, p. 121-122).

A expressão *Deep Web* foi criada por Michael K. Bergman, fundador do programa *Bright Planet*, um software especializado em coletar, classificar e procurar conteúdo nessa esfera da Web. Traduzida ao português, remete ao significado de profundeza, tanto que fixada em oposição a *Surface Web*, vocábulo que visa dar a ideia de superficialidade (POMPÉO; SEEFELDT, 2013, p. 440).

Para observar o fenômeno da *Deep Web*, pode-se pensar na internet possuindo vários "níveis": acima de todos está a *Surface Web* (representada, entre outros, pelo Google). Um pouco mais abaixo, com acesso mais restrito, está a *Deep Web*. A *Surface Web* ou Internet superficial é a parte da Internet indexada pelos motores de busca, por sua vez, a parte que não é indexada chama-se *Deep Web*, dessa forma o conjunto de páginas acessíveis define a *Surface Web*. Assim, a *Deep Web* seria o nível mais profundo da Internet, o seu "lado obscuro". Não se permite, a qualquer pessoa, que tenha acesso a essa rede, pois são necessários vários programas específicos para usá-la, não se admitindo navegadores comuns como o Google. Logo, é necessário que se tenha um navegador específico, muito conhecimento de sistemas de computação e de Internet, pois existe um grande número de vírus que são testados na *Deep Web*, então, a probabilidade de avarias no computador é muito alta. Ademais, deve-se ter um programa que esconda a localização do usuário para este não ser pego, já que alguns países proíbem, expressamente, o acesso à *Deep Web*, ou seja, é crime acessá-la. A *Deep Web* não possui filtros como os disponíveis no Google, o que possibilita encontrar vídeos e fotos de crimes, assassinatos, estupros, experiências ilegais, crueldades com animais, pedofilia, venda de drogas, tutoriais de como fazer bombas, *hackers* e muitas pessoas que oferecem esses serviços (MARCON; DIAS, 2014, p. 238).

Com efeito, o que existe de mais perigoso na *Deep Web* é o seu anonimato, pois, quem a utiliza dificilmente é rastreado, posto que muitas ferramentas são usadas para esconder a verdadeira identidade e localização do usuário (ALVES, 2018, p. 126). Para que tal anonimato possa acontecer,

uma rede não se comunica com a outra, nem possuem qualquer tipo de ligação com a internet aberta, justamente com o objetivo de tornar seus usuários não rastreáveis mascarando o número de IP, isto é, a identificação de cada computador, através de tecnologias de computação distribuída e encriptação (ABREU; NICOLAU, 2014, p. 122). Assim, os endereços dos sites são compostos por letras e números desconexos, difíceis de memorizar e que podem mudar de tempos em tempos, fazendo com que seus links não sejam facilmente passados de uma pessoa para outra, além de evitar, com isso, o rastreamento. Ter acesso a um site oculto, então, depende quase sempre do compartilhamento do endereço entre usuários. Nesse contexto, surge a importância dos fóruns dentro da *Deep Web*, pois é por meio deles que tais informações e sites são propagados.

> [...] a *Deep Web* começa quando uma pessoa repassa para outra um conteúdo que não pode ser encontrado nos grandes sites de pesquisa. Ninguém terá acesso, nem que procure. Será preciso antes buscar outros conteúdos possivelmente relacionados, e conhecer pessoas que conhecem outras pessoas [...] (ABREU; NICOLAU, 2014, p. 123).

A razão do anonimato parece, então, óbvia na *Deep Web*: publicar conteúdo polêmico ou ilegal, usando o anonimato como forma de proteção da identidade dos usuários. A natureza da web invisível oferece a possibilidade de um indivíduo ou um grupo de indivíduos codificarem uma informação de maneira tão confiável que decifrá-la tornar-se uma tarefa extremamente complicada (ABREU; NICOLAU, 2014, p. 123), instrumentalizando, assim, o anonimato. Nesse sentido, essa rede profunda engloba bancos de dados cujo conteúdo não está indexado e, por essa razão, não pode ser acessado por ferramentas de busca como o Google, por isso utilizam o *Tor*. Esse browser torna o endereço do seu computador indetectável (ALVES, 2018, p. 128).

Outro termo pelo qual a *Deep Web* é conhecida é *Under Web*, que faz referência à posição entre os dois grupos, ficando a *Surface Web* por cima e a *Under Web* por baixo, com a forma de um *iceberg*. Assim, a analogia com o *iceberg* é utilizada para exemplificar a razão da dificuldade em localizar e acessar as páginas, já que se encontram camufladas, fora de visão. A *Surface Web* é representada por seu topo, de fácil acesso e que salta aos olhos, embora pequena em termos de conteúdo; enquanto a *Deep Web* é representada como a sua base, pois se sabe que existe, mas não se tem a medida exata de seu tamanho, mas especula-se que as informações publicadas na *Deep Web* são comumente de 400 a 500 vezes maiores que as definidas da *World Wide Web* (ALVES, 2018, p. 127).

Outra analogia utilizada pelos pesquisadores do tema é a analogia da cebola, pois, segundo Pompéo e Seefeldt (2013, p. 442), a *Deep Web* é usualmente classificada em camadas, como se fosse uma cebola:

> [...] quando o usuário adentra à Deep Web, ele possui acesso gradual. A primeira camada concentra a maioria das informações necessárias aos iniciantes, mas, desde que se tenha um conhecimento mais avançado de informática e outros requisitos exigidos, é possível ir mais além [...].

Todavia, tais informações também estão disponíveis na *Surface Web*, indexadas em motores de busca convencionais e em redes sociais, a exemplo de grupos no *Facebook* que ensinam a acessar a *Deep Web* e *e-books* comercializados em grandes lojas virtuais que fornecem verdadeiros "guias" para navegá-la (ALVES, 2018, p. 130-131).

Imperioso destacar, então, que, com o advento da globalização, surgiu um novo fenômeno: a "criminalidade global" dentro de um contexto de "sociedade em rede", ambos os termos cunhados por Manuel Castells. O conceito de sociedade em rede é trabalhado pelo autor a partir da ideia de que é a própria sociedade que dá forma à tecnologia de acordo com suas necessidades, valores e interesses (CASTELLS, 2005, p. 17). Nesse contexto há o aumento da prática criminosa transnacional, motivada pela necessidade das organizações criminosas em se expandir. Essa prática, conforme Castells (1999, s.p.), passa a existir de duas formas:

> [...] a primeira emana após o enraizamento em uma determinada localidade de uma organização criminosa dita tradicional, por motivos históricos, culturais, étnicos ou socioeconômicos, e expande-se para outros países para assimilar diferentes associados e aumentar sua zona de atuação. Portanto, essas organizações não enfraquecem com a globalização, mas se fortalecem. A segunda decorre da criação de operações criminosas locais, geralmente fundadas em populações de baixa renda, que vendem seu crime para mercados de todas as partes do planeta [...].

A primeira forma guarda relação com as máfias que, com a globalização e a difusão da internet e, consequentemente, da *Deep Web*, começaram a atuar em outros países, infiltrando-se por meio de fóruns e páginas ocultas, constituindo verdadeiras sucursais e mitigando a ideia da máfia como algo cultural e regional. A segunda forma de criminalidade global apresentada por Castells (1999), resta intrinsecamente conectada à necessidade dessas organizações criminosas internacionais em possuírem contatos e mão-de-obra em suas sucursais para cometerem crimes para as máfias que os empregam. Com efeito, devido à intensa supervisão das autoridades policiais, a comunicação entre essas organizações criminosas e seus "funcionários" não se dá por meio da *Surface Web*.

Por isso, muitas delas se utilizam da *Deep Web* para criptografar e enviar dados, trocar informações com seus associados e propagar suas atividades nos mais diversos cantos do mundo. Tanto que, por isso, a *Deep Web* já ostenta inúmeros casos conhecidos, a exemplo do famoso *Wikileaks* e *Anonymous*, os quais tiveram a gênese de suas atividades ligadas à invisibilidade da rede (ALVES, 2018, p. 132).

Não restam dúvidas de que essa globalização do crime, que utiliza de forma maciça a *Deep Web*, abala profundamente a segurança transnacional, as políticas nacionais, a economia e a cultura dos povos. Em destaque nesse cenário, a lavagem de dinheiro revela-se o maior mal de todo esse contexto, constituindo-se na raiz de todos os demais delitos, já que destes decorre o sustento financeiro daqueles, principalmente desde o advento da moeda virtual "*Bitcoin*". Portanto, o sucesso e a expansão de atividades criminosas transnacionais ocorrem com a versatilidade e flexibilidade de sua composição, mas, sobretudo, da *Deep Web* enquanto ferramenta que sustenta de modo invisível suas articulações. Esse cenário é extremamente fértil para o surgimento de diversos crimes, entre os principais estão: armas e terrorismo, pornografia infantil, experiência humana, divulgação de segredos de governo, matadores de aluguel, tráfico de órgãos, pessoas e de drogas. Entre esses crimes, resta imperioso apontar que os crimes envolvendo armas e terrorismo adquiriram uma importância nos últimos anos, com o Estado Islâmico (EI) tendo seu site principal hospedado na *Deep Web*. Ademais, experiências humanas divulgadas por meio da web oculta chamam a atenção por sua crueldade, onde são realizadas experiências cirúrgicas de todos os tipos em humanos vivos, que são, na maioria, pessoas desabrigadas escolhidas nas ruas, tendo nos bonecos sexuais o seu exemplo mais conhecido (ALVES, 2018, p. 132-134).

No Brasil, a Polícia Federal especializa-se no combate aos crimes praticados nesses territórios, os chamados Crimes Cibernéticos, a exemplo da exitosa "Operação *Darknet*". Logo, busca-se inibir o uso da internet para fins ilícitos, mesmo ao utilizar do anonimato fornecido pela *Deep Web*, cada vez mais esses criminosos são encontrados e responsabilizados por seus atos (MARCON, DIAS, 2014, p. 241). Para resolver a questão do anonimato da *Deep Web*, algumas sugestões são sugeridas por Duarte e Mealha (2016, p. 24), segundo os quais:

> [...] navegar na Internet terá sempre os seus riscos de invasão de privacidade, assim a solução encontrada passa por um balanço entre liberdade e segurança, bem como o anonimato e identificação constante. Kaspersky admite a criação de um "passaporte online" para cada utilizador que obriga à identificação dos dados do mesmo, em casos específicos como transações bancárias [...].

Os pesquisadores defendem uma maior transparência nas trocas de valores financeiros, justamente para combater o principal crime que alimenta os demais, qual seja, a lavagem de dinheiro. Sem o aporte financeiro, as organizações criminosas não possuem meios de recrutar outros indivíduos para cometerem seus crimes, sua rede de contatos será reduzida e, consequentemente, a possibilidade de cometerem novos crimes. A outra sugestão ventilada pelos autores refere-se à encriptação, todavia, os próprios pesquisadores reconhecem a dificuldade de implementá-la:

> [...] melhorar a arquitetura da Internet e torná-la mais resistente a estas ameaças, através da encriptação: Porém, a criptografia revela-se como uma técnica morosa e difícil de aplicar, tanto que até mesmo os utilizadores da técnica profissionalmente por vezes têm dificuldades. Além do mais, existe muito maior facilidade em encriptar uma mensagem do que a desencriptar a mesma, o que tornaria o sistema mais lento e ineficiente [...] (DUARTE; MEALHA, 2016, p. 24).

De outra senda, os defensores do uso do anonimato possuem como principais argumentos a defesa da tríade: privacidade, anonimato e segurança. Entre eles estão os que apontam a *Deep Web* como uma grande aliada para os movimentos de dissidência política, a exemplo da Primavera Árabe, cujo início ocorreu no seio da *Deep Web*, visto que os países de tais manifestantes adotavam mecanismos de censura (DUARTE; MEALHA, 2016, p. 19). Ademais, defendem a utilização de mecanismos e softwares que ocultem sua navegação na web com o intuito de não contribuir para o crescimento dos bancos de dados de empresas que monitoram as atividades de seus usuários com o objetivo de melhorar a eficácia da publicidade dirigida (ABREU; NICOLAU, 2014, p. 125).

Portanto, o anonimato fornecido pela *Deep Web* poderá ser algo benéfico, de modo a organizar manifestações sociais com o objetivo de demonstrar descontentamento com governos autoritários. Entretanto, o anonimato também poderá encorajar e facilitar práticas delituosas, logo, percebe-se que o anonimato *per si* não é o problema, mas sim como ele resta utilizado. Dessa forma, surge a importância de mecanismos para prevenir e reprimir crimes virtuais, a exemplo da infiltração de agentes e da ação controlada, novidades trazidas pela reforma na Lei de Organizações Criminosas (Lei 12.850/13) em 2019.

2. A INFILTRAÇÃO POLICIAL NO ÂMBITO VIRTUAL: UM INSTRUMENTO DE EQUILÍBRIO DIANTE DO ANONIMATO

Uma vez entendido o anonimato como prática inerente ao âmbito virtual, especialmente quando se trata da *Deep Web*, torna-se mister repensar as ferramentas tradicionais de prevenção e repressão aos delitos, uma vez que tais rotinas foram projetadas considerando a investigação precipuamente no ambiente físico. Ademais, é empiricamente verificável que os crimes praticados em ambiente virtual se caracterizam por um dinamismo sem igual, motivo pelo qual os métodos convencionais de repressão podem se demonstrar insuficientes.

Se, anteriormente, o crime de estupro tinha como pressuposto de materialização a ocorrência efetiva de conjunção carnal – entendimento que vigorou até a ampliação do tipo, promovida pela Lei 12.015/2009, a qual modificou o artigo 213 do Código Penal, atualmente não se faz necessário que exista o contato físico entre agressor e vítima. Trata-se de uma adequação da norma ao cotidiano

contemporâneo, no qual a antiga previsão demonstrava-se incapaz de proteger satisfatoriamente a dignidade da vítima. Por conseguinte, diversas situações essencialmente atípicas se tornaram crimes legalmente previstos. Com a referida atualização legislativa, se possibilitou o enquadramento no crime de estupro, por exemplo, de acontecimentos perpassados unicamente no ambiente virtual. É o caso do criminoso que se utiliza de algum artefato ilegal para exigir da vítima alguma contrapartida que configure ato libidinoso, por exemplo – como o envio de fotos explícitas. É importante destacar que "ato libidinoso" pode ser entendido como todo e qualquer gesto destinado a satisfazer a lascívia, prazer e os desejos sexuais de alguém e, indubitavelmente, o universo digital constitui um ambiente bastante propício para a prática de atos dessa natureza sem a necessidade de contato físico. Destaca-se ainda que, se na modalidade presencial, muitas vezes temos como particularidade o uso da força bruta para dominar a vítima, tipicamente a modalidade virtual é pautada pela dominação psicológica.

Em síntese, o crime cibernético é aquele praticado no âmbito de ferramentas vinculadas à internet ou mesmo de ferramentas de mídia social e, para isso, não deixa de ser um crime como qualquer outro, constituído dentro da legislação (SILVA, 2018, p. 88). Dentre as reflexões causadas pelo uso do meio virtual para cometimento do crime, está a questão probatória. Sobre o assunto, dispõe Elisa Dias (2010, s.p): "[...] o crime virtual é um crime de muito difícil prevenção, que produz enormes dificuldades de ser investigado, de perseguição bem complicada, cuja comprovação é bastante difícil e a punição quase impossível, até por conta da ausência de legislação mais específica".

Nesse sentido, frente a complexidade e extensão de determinados crimes cibernéticos, especialmente considerando que as evidências deixadas por seus autores são especialmente instáveis, motivo pelo qual podem ser facilmente apagadas, alteradas ou perdidas, surge o instituto da infiltração policial em ambiente virtual. Sob a justificativa de investigar delitos relativos à dignidade sexual de crianças e adolescentes, cuja prática delitiva se dê no ambiente virtual, a Lei nº 13.441/17 insere no Estatuto da Criança e do Adolescente os artigos 190-A, B, C, D e E, para dispor a respeito da infiltração virtual de agentes policiais (BRASIL, 2017).

Na mesma linha, a Lei das Organizações Criminosas (Lei 12.850/2013) já previa a infiltração por policiais em atividade de investigação e obtenção de provas quando diretamente relacionadas a organizações criminosas. Além desses casos, é admitida a infiltração de policiais no ambiente virtual nos crimes previstos no Código Penal como invasão de dispositivo informático, artigo 154-A, e crimes previstos nesse Código no capítulo II, referentes aos crimes sexuais contra vulnerável (CASTRO, 2017).

Nos termos do art. 10 da Lei 12.850/2013[1], a infiltração de agentes pode ser iniciada a partir de representação do delegado de polícia ou requerimento do representante do Ministério Público. Na primeira hipótese, o Juiz, antes de decidir, dará vista ao Ministério Público, titular da ação penal, que fará uma análise quanto aos pressupostos e requisitos para o deferimento ou não da infiltração. Na segunda hipótese (pedido direito do Ministério Público), a Lei disciplina que deverá haver uma "manifestação técnica do delegado de polícia", a quem caberá verificar a possibilidade fática (estrutura pessoal e material) de atender à demanda. O mesmo artigo refere-se à infiltração de agentes como "tarefa de investigação", deixando dúvida sobre a viabilidade de execução do mecanismo probatório também na fase judicial (ZANELLA, 2020). Nesse sentido, Nucci (2019, p. 96) esclarece que:

> [...] a infiltração pode ocorrer tanto durante as investigações policiais (antes da ação penal) como na fase processual, uma vez que a Lei 12.850/2013 exige manifestação do delegado de polícia quando a infiltração for pleiteada "no curso de inquérito policial", dando a entender que ela também poderia, então, ser requerida pelo Ministério Público no curso do processo (oportunidade na qual, segundo os autores, seria desnecessária a manifestação da autoridade policial) [...].

No contexto apresentado, a infiltração de agentes denota certa passividade do Estado, que deixa de agir diante da constatação de crimes graves, mas sob a justificativa de alcançar um interesse maior (reunir provas e elementos de informações sobre um crime), o que está absolutamente de acordo com o postulado da proporcionalidade, assegurando-se, assim, a eficiência da investigação criminal, nos moldes da ação controlada, prevista no Art. 8º da Lei 12.850/13[2].

De maneira geral, a infiltração policial se trata de uma técnica especial de investigação criminal, através da qual um agente, judicialmente autorizado, infiltra-se em determinada organização criminosa, fazendo-se passar por um de seus integrantes com a finalidade de recolher informações e coletar provas acerca de sua estrutura e funcionamento. Na lição de Denílson Feitoza (2009, p. 820)

> [...] infiltração é a introdução de agente público, dissimuladamente quanto à finalidade investigativa (provas e informações) e/ou operacional ("dado negado" ou de difícil acesso) em quadrilha, bando, organização criminosa ou associação criminosa ou, ainda, em determinadas hipóteses (como crimes de drogas), no âmbito social, profissional ou criminoso do suposto autor de crime, a fim de obter provas que possibilitem, eficazmente, prevenir, detectar, reprimir ou, enfim, combater a atividade criminosa deles [...].

[1]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.

[2]Art. 8º Consiste a ação controlada em retardar a intervenção policial ou administrativa relativa à ação praticada por organização criminosa ou a ela vinculada, desde que mantida sob observação e acompanhamento para que a medida legal se concretize no momento mais eficaz à formação de provas e obtenção de informações.

Considerando que nosso ordenamento jurídico não conceitua a infiltração de agentes, coube à doutrina especializada elucidar tal procedimento. Deste modo, de forma genérica, pode-se entender esse procedimento como uma técnica especial, excepcional e subsidiária de investigação criminal, dependente de prévia autorização judicial, caracterizada pela dissimulação e sigilosidade, na qual o agente de polícia judiciária é inserido no bojo de uma organização criminosa com objetivo de compreender sua estrutura. Logo, buscam-se fontes de provas para a identificação dos delitos cometidos, bem como de seus responsáveis, prevenindo, assim, a prática de novas infrações penais (SANNINI NETO, 2017).

Especificamente quando a infiltração se dá em âmbito virtual, percebe-se uma modernização no rito investigatório. Com a translocação do delito do meio físico para o meio virtual, é salutar que as ferramentas investigatórias não se restrinjam ao primeiro ambiente. A Lei nº 13.441/17 determinou requisitos para regulamentar e dar efetividade a esse instituto, modernizando os meios de acesso de evidências com uma possibilidade de expansão da infiltração e, principalmente, evitando a exposição do agente aos riscos inerentes ao ambiente físico (BRASIL, 2017).

Nesse sentido, observa-se que a infiltração virtual da polícia é uma inovação legislativa de maior amplitude na luta contra a violação da dignidade sexual de crianças e adolescentes ao possibilitar maiores oportunidades de encontrar os perpetradores desse tipo de crime. Primeiramente, demonstrar-se mais segura para os agentes, uma vez que esse ponto sempre foi considerado um fator limitante para maiores aplicações do instituto quando em ambiente, seja pelo risco direto, de ser revelado (o que ocorre na minoria dos casos), seja pelo risco indireto (exposição prolongada às condições insalubres).

Ademais, a infiltração virtual demonstra-se com um alto custo-efetividade para o Estado. Por demandar de um profissional extremamente capacitado, considerando as dimensões continentais do Brasil, é de difícil viabilidade que se proceda com a infiltração em ambientes físicos fora dos grandes centros. Os criminosos, principalmente aqueles ligados ao compartilhamento de pornografia infantil, não se encontram restritos a esses espaços metropolitanos. Nesse sentido, a investigação desses crimes é muito complexa, pois os criminosos interagem em redes sociais fechadas, principalmente pela *Deep Web*, mediante a utilização de pseudônimos e códigos, sendo extremamente difícil que a Polícia consiga descobrir onde estão ocorrendo essas comunicações e a troca de material de pedofilia. A única forma de descobrir a real identidade dos criminosos e coletar provas da materialidade é conseguir fazer com que os policiais consigam ingressar e participar por um tempo dessa rede. As dificuldades na persecução policial justificam-se, pois, se anteriormente o criminoso

tinha de "revelar" fotografias e/ou entregar pessoalmente fotos e vídeos, e posteriormente sujeitar-se à fiscalização dos correios ou da polícia, hoje consegue disponibilizar na Internet esse tipo de material simultaneamente a sua produção, se desejar, bem como alcançar compradores ou interessados em todas as partes do mundo sem a necessidade de qualquer armazenamento em mídia física (FERNANDES, 2017).

Entende-se, portanto, a inovação legal como necessária por ajustar-se à nova realidade posta, compreendendo o deslocamento dos crimes do meio físico para o meio virtual e inovadora, a partir do momento em que simultaneamente induzirá um menor custo para o Estado, tanto financeiramente como de pessoal, resultando, assim, em benefícios para a sociedade. Apesar disso, um trecho do dispositivo legal é passível de aperfeiçoamento. Trata-se da fixação de prazo máximo para a manutenção da infiltração em meio virtual. É compreensível que o objetivo da Lei, ao fixar o prazo máximo para a infiltração em 720 dias (equivalente a dois anos), foi o de impedir que houvesse medidas excessivamente duradouras a ponto de tornarem-se abusivas. Todavia, em situação análoga à interceptação telefônica, não existe previsão legal para prazo máximo, existindo apenas a necessidade de renovação periódica caso subsistam os fundamentos que induziram sua concessão. O entendimento legal, confirmado pela doutrina e jurisprudência, é de que "a complexidade das investigações possibilita diversas prorrogações da interceptação telefônica, desde que justificadas com base na peculiaridade do caso concreto, sendo legítimo o uso da técnica de fundamentação *per relationem"* (STJ, 2020).

Ademais, elencam-se três razões pelas quais se justifica a tese de não limitação temporal no caso da infiltração virtual. Primeiramente, aponta-se para o fato de que as redes criminosas em que desenvolvem a prática delitiva alcançadas pela Lei 13.441/17 caracterizam-se pela discrição e dificuldade de acesso. O agente não conseguirá se infiltrar facilmente no meio desses grupos, considerando que tais criminosos se cercam de várias cautelas e não admitem a participação de qualquer pessoa, salvo após um longo processo de aquisição de confiança, que pode sim durar anos.

Além disso, definido prazo máximo para a infiltração, é acessível ao criminoso informado limitar o acesso a determinados fóruns a usuários antigos, com mais de dois anos, o que colocaria em risco toda a investigação. Logo, limitar esse prazo a 720 dias significa dizer que, em alguns casos, a infiltração terá que ser interrompida quando o agente policial estava muito próximo de ingressar na rede criminosa ou quando havia acabado de penetrar neste submundo, mas ainda não tinha conseguido identificar a real identidade dos criminosos ou dados de informática que permitam uma medida de busca e apreensão, por exemplo. Apesar de este prazo de 720 dias parecer longo, mostra-se, para quem estuda o tema, um período insuficiente para o desmantelamento dos grandes grupos criminosos

que, quanto maiores, mais se cercam de anteparos para não serem descobertos (SANNINI NETO, 2017).

A segunda razão para contestar a imposição de um prazo limite para infiltração virtual é que, ao contrário da interceptação telefônica, aquela não relativiza de forma intensa os direitos fundamentais dos investigados. Enquanto na interceptação existe uma invasão profunda da intimidade dos interlocutores, atingindo inclusive terceiros que não estão sendo investigados, mas terão todas as suas conversas ouvidas pelo Estado, na infiltração a intervenção estatal é restrita aos investigados e terá seu conteúdo limitado ao que for exposto no respectivo ambiente.

Por fim, o terceiro motivo trata-se de uma analogia com a infiltração policial prevista na Lei do Crime Organizado (Lei 12.850/2013), situação mais similar à do caso em tela. Enquanto a infiltração física, com seus riscos majorados, conforme já discutido no presente trabalho, não prevê prazo limite para renovações, permitindo que elas ocorram tantas vezes quantas for necessário, não parece razoável que sua equivalente no meio eletrônico passe a estabelecer prazo limite.

Em síntese, para a interceptação telefônica e para a infiltração de agentes da Lei do Crime Organizado, situações de considerável relativização de direitos dos investigados ou de risco maior para os investigadores, não existe prazo máximo limite determinado em lei. No entanto, para a infiltração prevista no art. 190-A do ECA e aqui discutida, o legislador fixou o limite de 720 dias.

Portanto, percebe-se que a investigação policial no âmbito virtual se encontra em seus primeiros estágios de efetivação. Todavia, houve um aprimoramento significativo na legislação nacional que trata do tema, principalmente devido aos novos desafios impostos pela criminalidade transnacional e a popularização no uso da internet.

CONCLUSÃO

Conforme o exposto no decorrer do presente trabalho, a *Deep Web* se popularizou, juntamente com a *Surface Web* tradicional, dado o aumento no acesso à Internet e a especialização no cometimento dos mais diversos crimes virtuais. O alto grau de anonimato fornecido pela *Deep Web* desempenha um papel fundamental que transforma esse ambiente em um lugar propício para esconderem seus rastros. Ademais, a transnacionalização dos crimes, por meio da *Web* Oculta, permite que diversas organizações criminosas cometam crimes em outros países e formem uma extensa rede de contatos em diversas localidades.

Dessa forma, ao verificar a necessidade da persecução de tais crimes, observou-se que a infiltração policial se configura como um importante instrumento de combate aos crimes virtuais, principalmente aqueles que ocorrem no âmbito da *Deep Web*, sob o manto do anonimato. A legislação

brasileira, em certa medida, atualizou-se ao realizar a reforma no Estatuto da Criança e do Adolescente, normatizando a possibilidade de expansão da infiltração, antes restrita ao ambiente físico e, principalmente, protegendo o agente policial ao evitar sua exposição aos riscos inerentes ao ambiente físico.

Por sua vez, notou-se que o anonimato fornecido pela *Deep Web*, aos poucos, está sendo mitigado pelo avanço e modernização das forças policiais e da legislação nacional. Com efeito, os agentes policiais estão se especializando no combate dos crimes virtuais e os legisladores estão se conscientizando da necessidade de alteração legislativa para fazer frente à criminalidade que se instaurou no âmbito virtual.

Todavia, a utilização do instrumento da infiltração policial ainda enfrenta desafios, principalmente, relacionados à sua duração, visto que o prazo máximo de 720 dias concedido pela lei é demasiado curto, visto que a dinâmica dos crimes virtuais não é a mesma dos crimes que ocorrem em ambiente físico. Isto pois, as dificuldades inerentes à investigação e infiltração em organizações criminosas restam exponencialmente amplificadas em um ambiente ainda desconhecido como a *Deep Web*, cuja extensão, *per si*, é desconhecida e a navegação é nebulosa.

Portanto, constata-se que a investigação policial é um instrumento relevante para a investigação de crimes virtuais, especialmente os cometidos na *Deep Web*. Logo, a capacitação dos agentes policiais e a modernização da legislação nacional devem ser constantes para fazer frente às organizações criminosas que se utilizam do manto do anonimato para cometer os mais diversos crimes.

REFERÊNCIAS

ABREU, Giovanna; NICOLAU, Marcos. A estética do anonimato na Deep Web: a metáfora das máscaras e do homem invisível aplicada ao "submundo" da internet. **Culturas Midiáticas,** *[S. l.]*, v. 7, n. 1, 2014. Disponível em: https://periodicos.ufpb.br/ojs/index.php/cm/article/view/19746. Acesso em: 14 dez. 2022.

ALVES, Flaviano de Souza. A criminalidade na Deep Web. **Revista da Escola Superior de Guerra,** v. 33, n. 67, p. 123-141, jan/abr., 2018. Disponível em: https://revista.esg.br/index.php/revistadaesg/article/view/910. Acesso em: 14 dez. 2022.

BRASIL. **Lei 13.441 de maio de 2017.** Altera o Estatuto da Criança e do Adolescente. Brasília, 8 de maio de 2017. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13441.htm. Acesso em: 27 dez. 2022

CASTELLS, Manuel. A sociedade em rede: do conhecimento à política. *In*: CASTELLS, M.; CARDOSO, G. (org.). **A sociedade em rede:** do conhecimento à acção política. Portugal: Imprensa Nacional – Casa da Moeda, 2005.

CASTELLS, Manuel. **Fim do milênio:** a era da informação: economia, sociedade e cultura. São Paulo: Paz e Terra, 1999.

CASTRO, Henrique Hoffmann Monteiro de. **Lei 13.441/17 instituiu a infiltração policial virtual**. mai. 2017. Disponível em: https://www.conjur.com.br/2017-mai-16/academia-policia-lei-1344117-instituiu-infiltracao-policial-virtual. Acesso em: 28 dez. 2022.

DIAS, Vera Elisa Marques. **A problemática da investigação do cibe crime.** 2010. Monografia. (Pós-graduação aperfeiçoamento em direito da investigação criminal e da prova) - Universidade de Lisboa, Lisboa, nov. 2010. Disponível em: http://www.verbojuridico.net/doutrina/2011/veradias_investigacaocibercrime.pdf. Acesso em: 29 dez. 2022.

DUARTE, David; MEALHA, Tiago. Introdução à Deep Web. **IET Working Papers Series.** 2016. Disponível em: https://run.unl.pt/handle/10362/18052. Acesso em: 14 dez. 2022.

FEITOZA, Denílson. **Direito processual penal:** teoria, crítica e práxis. 6ª. ed. Niterói: Impetus, 2009.

FERNANDES, Simone dos Santos Lemos. Do reflexo do desenvolvimento das novas tecnologias de informação na prática de crimes contra crianças e adolescentes. *In*: SILVA, Ângelo Roberto Ilha da. (coord.). **Crimes Cibernéticos.** Porto Alegre: Livraria do Advogado, 2017.

MARCON, João Paulo Falavinha; DIAS, Thais Pereira. Deep Web: O Lado Sombrio da Internet. **Conjuntura Global,** Vol. 3, n. 4, out/dez., 2014, p. 233-243. Disponível em: https://revistas.ufpr.br/conjgloblal/article/view/40071. Acesso em: 14 dez. 2022.

NUCCI, Guilherme de Souza. **Organização criminosa** 4. ed. Rio de Janeiro: Forense, 2019.

POMPÉO, Wagner Augusto Hundertmarck; SEEFELDT, Joao Pedro. Nem tudo está no Google: Deep Web e o perigo da invisibilidade. *In*: **Anais do Congresso Internacional de Direito e Contemporaneidade**, 2, 2013, Santa Maria. p. 436-449. Disponível em: http://coral.ufsm.br/congressodireito/anais/2013/3-11.pdf. Acesso em: 14 dez. 2022.

SANNINI NETO, Francisco. Infiltração virtual de agentes é um avanço nas técnicas especiais de investigação criminal. *In*: **Canal Ciências Criminais**. 2017. Disponível em: https://canalcienciascriminais.com.br/infiltracao-virtual-agentes. Acesso em: 29 dez. 2022.

SILVA, Ângelo Roberto Ilha da. **Crimes Cibernéticos**. 2 ed. Porto Alegre: Livraria do Advogado, 2018.

STJ. Superior Tribunal de Justiça (5. Turma). **Agravo Regimental no Recurso Especial nº 1.346.390/RS.** Processo Penal. Agravo Regimental no Recurso Especial. Inépcia da denúncia. Sentença condenatória proferida. Cognição Exauriente. Prejudicado. Interceptação telefônica. Prorrogações sucessivas. Fundamentação concreta. Técnica *per relationem*. Possibilidade. Agravo desprovido. Relatora: Min. Ribeiro Dantas, 14 de fevereiro de 2020. Disponível

em:https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1910507&num_registro=201202067813&data=20200214&formato=HTML. Acesso em: 29 dez. 2022.

ZANELLA, Everton Luiz. Infiltração de agentes. *In*: CAMPILONGO, C. F.; GONZAGA, A. de A.; FREIRE, A. L. (coords.). **Enciclopédia jurídica da PUC-SP**. 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/442/edicao-1/infiltracao-de-agentes. Acesso em: 27 dez. 2022.

AUTORES

João Pedro do Nascimento Costenaro
Advogado. Mestrando em Direito pelo Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria (UFSM). Pós-Graduado em Direito Constitucional. Bacharel em Direito (UFSM). Pesquisador no Grupo de Pesquisa em Propriedade Intelectual na Contemporaneidade (GPPIC/UFSM).
E-mail: jpcostenaro1@hotmail.com
Orcid: 0000-0003-0516-2263

Otávio Augusto Milani Nunes
Mestrando em Direito pelo Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria (UFSM). Advogado. Pesquisador do Grupo de Pesquisa em Propriedade Intelectual na Contemporaneidade (GPPIC/UFSM).
E-mail: otavioamnunes@gmail.com
Orcid: 0000-0003-2777-034X

Isabel Christine Silva de Gregori
Doutora em Direito. Professora no Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria (UFSM). Coordenadora do Grupo de Pesquisa em Propriedade Intelectual na Contemporaneidade (GPPIC/UFSM).
E-mail: isabelcsdg@gmail.com
Orcid: 0000-0002-3251-946X