Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Direito

ANA PAULA TORRES REZENDE SANTOS

A INFILTRAÇÃO POLICIAL VIRTUAL COMO MEIO DE INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS: os limites para a obtenção de provas válidas

BRASÍLIA
2021

ANA PAULA TORRES REZENDE SANTOS

A INFILTRAÇÃO POLICIAL VIRTUAL COMO MEIO DE INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS: os limites para a obtenção de provas válidas

Monografia apresentada como requisito parcial para obtenção do título de Bacharela em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (CEUB).

Orientadora: Profa. Viviani Gianine Nikitenko.

BRASÍLIA
2021

ANA PAULA TORRES REZENDE SANTOS

A INFILTRAÇÃO POLICIAL VIRTUAL COMO MEIO DE INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS: os limites para a obtenção de provas válidas

Monografia apresentada como requisito parcial para obtenção do título de Bacharela em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (CEUB).

Orientadora: Profa. Viviani Gianine Nikitenko.

BRASÍLIA, DIA de MÊS de 2021.

BANCA AVALIADORA

_____

Professora Orientadora

_____

Professor Avaliador

Aos meus pais, Simone Torres Rezende e Joselito Santos, por serem a base da minha formação como pessoa e como profissional, investindo, apoiando e acreditando em mim.

AGRADECIMENTOS

Primeiramente, destaco que a fé foi a guia do meu caminho até aqui, por isso, agradeço a Deus por não ter me deixado desistir, por ter me abençoado e me dado força, principalmente nesse momento triste que o mundo está passando, ocasionado pela pandemia.

À minha mãe, Simone, pelo amparo e carinho que teve comigo durante toda a minha trajetória acadêmica, por sempre se preocupar comigo e acreditar em mim. Além de ser meu exemplo de força, garra e amor.

Ao meu pai, Joselito, por me incentivar nos estudos, por ser exemplo de inteligência e determinação e por sempre acreditar em mim.

Ao meu irmão, Guilherme Torres, pelos momentos de descontração.

Ao meu namorado e melhor amigo, Matheus Xavier, por ter estado comigo durante cada avanço desse trabalho, pela paciência, pelo carinho e pela compreensão nos momentos de ausência.

À minha orientadora, professora Viviani Nikitenko, pelos ensinamentos, pela orientação e pela paciência.

Ao meu professor, Tedney, pelas dicas e pelo acompanhamento durante meu processo de escrita deste trabalho.

Às minhas amigas da faculdade, em especial à Isadora e à Natália, que sempre estiveram presentes, nos momentos bons e ruins, me incentivando a estudar, me apoiando e me descontraindo.

A tantos outros, amigos, familiares, professores, que estiveram presentes durante a minha trajetória acadêmica e profissional, ainda que indiretamente.

RESUMO

Resumo: Trata-se de monografia apresentada no âmbito do curso de Direito da Faculdade de Ciências Jurídicas e Sociais do Centro Universitário de Brasília, como condição para obtenção do título de Bacharela em Direito. Pretende-se abordar a infiltração virtual de policiais nas investigações de crimes cibernéticos, demonstrando a licitude das provas colhidas durante a investigação, abordando a diferença deste instituto com o flagrante preparado e a relativização dos direitos fundamentais do investigado. Pretende-se desenvolver uma monografia dividida em quatro capítulos. Primeiramente, a fim de contextualizar o tema, aborda-se o histórico e o conceito dos crimes cibernéticos, a evolução da internet, apresentando quais os delitos mais praticados nos ambientes virtuais e quais os meios de investigação utilizados no ciberespaço. No segundo capítulo, é trazida a infiltração policial como método de investigação dos cibercrimes, abordando suas espécies, seu funcionamento, suas características e sua utilização nos ambientes mais profundos da internet. Além disso, analisa-se as leis correspondentes à infiltração policial no Brasil e demonstra-se quais os crimes que autorizam esse método, diferenciando a infiltração do meio digital e do meio físico. No terceiro capítulo diferencia-se essa técnica especial de investigação do policial disfarçado e explora-se a licitude dos elementos informativos colhidos, o infiltrado como testemunha anônima e o flagrante preparado. Além disso, aborda-se aspectos e princípios constitucionais e processuais voltados para tal infiltração. Pretende-se mostrar como funciona esse método de investigação em crimes cibernéticos, se é eficaz, se é seguro, os princípios que a norteiam e a validade das provas obtidas por essa técnica. Para o desenvolvimento da pesquisa, vale-se do método bibliográfico quali-quanti, a partir de diversas doutrinas, leis e dados estatísticos referentes ao tema.

Palavras-chave: infiltração policial virtual. crimes cibernéticos. estatuto da criança e do adolescente. flagrante preparado. provas ilícitas.

LISTA DE ABREVIATURAS E SIGLAS

Art.	**Artigo**
CEUB	**Centro Universitário de Brasília**
CRFB	**Constituição Federal de 1988**
CP	**Código Penal**
ECA	**Estatuto da Criança e do Adolescente**
IBGE	**Instituto Brasileiro de Geografia e Estatística**
IP	**Internet Protocol ou Protocolo de Internet**
MPDFT	**Ministério Público do Distrito Federal e Territórios**
nº	**Número**
ONU	**Organização das Nações Unidas**
ORCRIM	**Organização Criminosa**
p.	**Página**
STF	**Supremo Tribunal Federal**
TRF	**Tribunal Regional Federal**
§	**Parágrafo**

SUMÁRIO

INTRODUÇÃO

É sabido que o avanço da tecnologia trouxe maior facilidade de comunicação, acesso à informação, praticidade dentre diversos outros aspectos positivos para todo o mundo. Todavia, essa era digital começou a ser utilizada também por criminosos que, através dos ambientes mais profundos da internet, praticam *cybercrimes*, justamente pela facilidade de execução, pela carência de regras e pelo anonimato que ela proporciona. Como dispõe Caetano, citando Cassanti: "A internet é uma grande praça pública, o maior espaço coletivo do planeta". (CASSANTI, 2014, apoud CAETANO, 2015, p. 2)

Esses crimes praticados no ciberespaço através de um dispositivo eletrônico, por se desenvolver sem contato físico, trouxe uma dificuldade maior na investigação e obtenção de provas, tendo em vista que é obstruída pelos recursos tecnológicos.

Essa nova roupagem da criminalidade desenvolvida ao longo dos anos fez, então, com que fosse necessário aperfeiçoar as técnicas de investigação, utilizando também a tecnologia a seu favor. Esse método é um novo tipo de investigação já existente há muitos anos, porém, sua diferença é o meio em que é operado, sendo o mais antigo no meio físico e o mais recente no ambiente virtual, a fim de trazer uma solução para a obtenção de provas na investigação dos crimes cibernéticos.

Esse meio de investigação é chamado de infiltração policial, previsto primeiramente em 2001, pela inserção no art. art. 2º, I, pela Lei nº 10.217/2001, na Lei de Organizações Criminosas. Em 2002 passou-se a prever essa técnica na Lei nº 10.409/2002, que tratava sobre o combate aos crimes relacionados a drogas, que foi revogada pela atual Lei nº 11.343/2006. A Convenção de Palermo (ratificada pelo Brasil em 2004), também abordou a infiltração como técnica especial de investigação. Contudo, a figura do agente infiltrado virtual somente foi prevista no ordenamento brasileiro em 2017 pela Lei nº 13.441/17 que inseriu dois artigos no Estatuto da Criança e do Adolescente, com a finalidade precípua de investigar crimes relacionados à dignidade sexual de crianças e adolescentes. Em 2019, a Lei nº 13.964, conhecida como "pacote anticrime" inseriu a figura do agente infiltrado virtual na Lei de Organização Criminosa (12.850/13).

O presente trabalho, portanto, tem como objetivo estudar as dificuldades da persecução penal de crimes praticados no ambiente virtual, trazendo como possível solução a figura do

agente infiltrado virtual, analisando os requisitos para a sua aplicação, as consequências, as dificuldades e as regras legais do método, assim como, demonstrar a diferença entre tal método e o flagrante preparado e com o agente disfarçado, analisando a licitude das provas colhidas a partir da relativização de direitos fundamentais do investigado.

O primeiro capítulo versará sobre o histórico e evolução dos crimes virtuais, assim como abordará os diversos meios de investigação no ambiente cibernético. O segundo capítulo conceituará a infiltração policial como gênero e abordará sua evolução no direito brasileiro e suas espécies. Ademais, serão trazidas as principais características e requisitos deste método especial de investigação e, ainda, como ele funciona nos ambientes mais profundos da internet, como a Dark Web e a Deep Web.

O terceiro retratará a legalidade das provas obtidas por meio da infiltração virtual de agentes, fazendo diferenciações entre o agente provocador e o agente infiltrado, assim como trazendo a discussão da possibilidade de o agente atuar como testemunha anônima no processo. Além disso, será falado a respeito dos direitos fundamentais do investigado que são relativizados nessa espécie de investigação e diversos princípios que devem ser observados para a realização da infiltração.

Para tanto, será realizada uma pesquisa teórica sobre o assunto, a partir de livros, artigos, sites, a fim de conhecer os diversos pensamentos acerca do tema. Ademais, será apresentada algumas jurisprudências para analisarmos como o judiciário está enfrentando as questões relacionadas a essa técnica de investigação.

I - CRIMES CIBERNÉTICOS

I.I - Conceito de crimes cibernéticos e sua evolução

Os crimes cometidos no ambiente virtual possuem diversas denominações, dentre elas: cibercrime, crime informático, crime digital, crime virtual, crime cibernético, dentre outros. A definição de crime cibernético é bastante ampla, cada doutrinador conceitua de uma forma, de acordo com cada ponto de vista. Para Cassanti esses crimes "são delitos praticados através da internet que podem ser enquadrados no Código Penal Brasileiro resultando em punições como pagamento de indenização ou prisão." (CASSANTI, 2016, apoud CARDOSO, 2017, p. 4). Já Guilherme Schmidt (2013), conceitua o cibercrime de acordo com o conceito analítico finalista de crime, concluindo que é toda conduta típica, antijurídica e culpável praticada através da informática ou contra ela. E por fim, Diana de Simas (2014) traz a conceituação dividida em dois sentidos, o amplo e o estrito. Para ela, o crime informático é toda conduta criminosa que é cometida por meios informáticos, já em sentido estrito, explica que são "os crimes quem que o meio informático surge como parte integradora do tipo legal, ainda que o bem jurídico protegido não seja digital." (SIMAS, 2014. p.12).

A internet surgiu em meados da Guerra Fria, porém, a discussão a respeito de uma data certa e do objetivo de sua criação são controversos. Alguns doutrinadores acreditam que a internet foi criada com o objetivo de auxiliar a comunicação dos militares durante a guerra. Já outros acreditam que o objetivo foi científico, para ligar universidades dos Estados Unidos.

Ao longo dos anos a internet ultrapassou seu objetivo inicial, chegando a toda a população mundial e proporcionando um ambiente globalizado e facilitador do acesso às informações, comunicação, relações sociais etc. Por causa disso, as pessoas foram se tornando cada vez mais dependentes da informática, tornando-a indispensável no dia a dia da população. Ocorre que, tal avanço não trouxe somente benefícios, muitos criminosos passaram a utilizar o ambiente cibernético para o cometimento de delitos, aproveitando-se do anonimato que a internet pode trazer, o número de vítimas que é possível acessar e a facilidade de ultrapassar as barreiras nacionais. Ademais, a internet alimentou ideias e opiniões antigas e esquecidas, por alguns grupos, trazendo à tona questões preconceituosas e perigosas, que fundamentam os crimes de ódio.

Nos dias atuais, a criminalidade cibernética está extremamente avançada. Segundo dados do IBGE, o percentual de domicílios que utilizavam a Internet em 2018 no Brasil foi de 79,1%, ou seja, ao arredondarmos, percebe-se que somente 20% das residências não possuem tal acesso. Isto é, o número de pessoas conectadas à internet é imenso. E, portanto, a dependência dos indivíduos com a rede tornou o crime virtual uma conduta frequente, perigosa e transnacional. Segundo estimativa de Rodrigo Fogagnolo, coordenador do Núcleo Especial de Combate a Crimes Cibernéticos (NCyber), do Ministério Público do Distrito Federal e Territórios (MPDFT), os crimes cibernéticos podem movimentar em torno de R$ 80 bilhões ao ano no Brasil. (GONDIM, 2019)

I.II - Classificação dos crimes cibernéticos

Os crimes cibernéticos podem ser divididos entre aqueles praticados visando os próprios computadores (crimes próprios) e aqueles que utilizam os computadores para cometer diversos outros crimes (crimes impróprios). Na primeira hipótese, encaixam-se principalmente aqueles praticados por malwares, os quais objetivam infectar os dispositivos eletrônicos para danificar e impedir que serviços funcionem, assim como para furtar dados. (KASPERSKY).

Dentre os impróprios, podemos citar como exemplos os crimes de tráfico ilícito de entorpecentes, organização criminosa, pornografia infantil, ciberterrorismo, difamação, calúnia, injúria, dentre outros cometidos no ambiente virtual.

> Valem destacar os crimes mais praticados no universo online, que são: calúnia; insultos; difamação; atos obscenos; apologia ao crime; perfis falsos em redes socias; preconceito e discriminação; pedofilia; estupros virtuais e crimes de ódio que aterrorizam o âmbito social. (GUERRA, 2019, pág. 10)

Os crimes contra a honra são espécies de crimes que evoluíram demasiado com o avanço da tecnologia. A internet desencadeia uma força muito maior para esses delitos, tendo em vista que a propagação da mensagem é mais rápida e alcança mais pessoas, aumentando, portanto, o "potencial de divulgação que uma informação injuriosa, difamatória ou caluniosa tem, quando posta na Rede". (JUNIOR, 2018, pág. 25). Esses crimes estão previstos nos arts. 138, 139 e 140, do Código Penal. Todos eles podem ser cometidos tanto fisicamente, quanto em ambientes virtuais, entretanto, caso o crime ocorra por um meio que facilite a divulgação (por exemplo,

redes sociais), a pena será aumentada de um terço, conforme preceitua o art. 141 do mesmo códex.

Outro exemplo que produz danos extremamente graves no universo digital são os crimes de ódio. São delitos que podem ser praticados por organizações criminosas ou por pessoas específicas e que utilizam dos benefícios que a internet proporciona para disseminar discursos discriminatórios, intimidando aqueles que são considerados “minorias sociais” pelo histórico preconceito sofrido. A difusão das opiniões e de conhecimentos por meio da internet faz com que opiniões preconceituosas sejam imputadas às pessoas com facilidade, tendo em vista o anonimato, a sensação de impunidade, a facilidade e a proporção que pode chegar, fazendo com que crimes motivados pelo preconceito cresçam. Não há no Brasil diplomas legais específicos para esses crimes.

A Lei nº 7.716/89 dispõe que serão punidos os crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. Porém, essa lei não engloba todos os tipos. O Correio Braziliense, em um artigo acerca do tema, citando a antropóloga Adriana Dias, explica que crime de ódio é “aplicar a uma outra pessoa qualquer coisa que seja crime motivado por um ódio. De injúria até homicídio. Todos esses crimes, se forem feitos por ódio, são crimes de ódio. Crime de homofobia é ódio, racismo é ódio". (FORTUNA, 2019)

Os crimes contra a dignidade sexual de crianças e adolescentes sempre existiram, contudo, foram extremamente facilitados com a evolução da internet, pois, através da rede, não há mais a necessidade, por exemplo, de revelar uma foto, basta tê-la no computador, tornando mais ágil o repasse. O Estatuto da Criança e do Adolescente, portanto, pune aquele que vende ou expõe à venda materiais pornográficos infanto-juvenis, também aquele que oferece, troca, disponibiliza, transmite, distribui, publica ou divulga por qualquer meio materiais pornográficos, assim como assegura o armazenamento e o acesso destes materiais por rede de computadores, além daqueles que adquirem, possuem ou armazenam, por qualquer meio, materiais pornográficos. Apesar dessas condutas serem realizadas pelos criminosos pelas redes sociais como e-mail, mensagens e blogs, os ambientes em que mais é cometido esse tipo de crime são aqueles criptografados, como o WhatsApp e a *Deep Web*, dificultando a investigação. (SILVA, 2017)

Além disso, o tráfico ilícito de entorpecentes é um crime amplamente praticado via internet, principalmente nos ambientes profundos, tais como *Deep Web* e *Dark Web*. Uma das maiores redes desse comércio ilegal é uma página na *Deep Web*, chamada de *Silk Road*, onde

ocorre diversas vendas de mercadorias ilegais e eram adquiridas por bitcoin, uma moeda criptografada. Após muitas investigações, inclusive através da infiltração policial, o responsável pela rede, cujo *nickname* era Dread Pirate Roberts, foi preso pela polícia federal americana. (SILVA, 2017).

As organizações criminosas atuam na internet cometendo diversos crimes, tais como crimes contra a honra, estelionato, crimes contra a dignidade sexual de crianças e adolescentes, tráfico de drogas, dentre outros. Entende-se por organização criminosa, segundo o art. 1, § 1º da Lei nº 12.850/13, toda

> associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional. (BRASIL, 2013)

A atuação dessas organizações se sofistica e evolui de acordo com os avanços tecnológicos, fazendo com que o Estado necessite acompanhar a fim de reprimir com agilidade os delitos praticados por elas. Um método bastante utilizado hoje para a repressão ao crime organizado é a infiltração policial, na qual o agente de polícia ingressa em uma organização, com uma identidade fictícia a fim de conquistar a confiança dos membros e, com isso, obter provas das infrações cometidas pela organização criminosa. (RUSSO; NEGRÃO, 2020).

I.III - A investigação no ciberespaço

É notório que grande parte da legislação brasileira foi criada antes da evolução da internet. Dessa forma, percebe-se que os mecanismos investigativos previstos dos dispositivos penais e processuais penais em sua maioria não foram previstos para combater os delitos da atual realidade.

Como já abordado anteriormente, o surgimento e a evolução da internet proporcionaram facilidades para a vida em sociedade. Isso porque, a busca por informações, conhecimentos e aprendizagens passou a ser exercida de maneira muito mais simples e rápida, necessitando de apenas um dispositivo eletrônico como celular, tablet, computador etc. No entanto, tal facilidade não foi utilizada somente para o bem. A rapidez na propagação e compartilhamento

de dados, o anonimato, a sensação de impunidade, são características que incentivaram criminosos a utilizar a tecnologia para o cometimento de crimes.

Dessa forma, foi necessário, ao longo dos anos, repensar os métodos investigativos presentes e adaptá-los à realidade hodierna. Diante disso, para que as investigações nesses ambientes virtuais sejam eficazes, deve-se, primeiramente, aprender a linguagem e os sistemas de operação. Portanto, a capacitação dos profissionais do Direito, especialmente das autoridades policiais (que são quem investigam os crimes) e dos juízes (que para julgar determinado caso, deverão ter conhecimento da linguagem informática) é o primeiro passo para o alcance do combate à criminalidade digital. (JUNIOR, 2018, pág. 32).

> Apesar da falta de compreensão que porventura enfrentem com a linguagem técnica dessa tecnologia, os sujeitos atuantes na persecução penal aos crimes cibernéticos precisam conhecê-la. (JUNIOR, 2018, pág. 32)

Além do conhecimento informático, outros aliados das investigações no ambiente cibernético são a matemática e a física. Muitas fórmulas e conceitos dessas áreas estão sendo estudados a fim de conseguir identificar as principais peças da atuação das organizações criminosas. (Dom Total, 2020)

Percebe-se, portanto, que a investigação no meio digital demanda muito conhecimento tecnológico e científico, em que, é necessário que se aproxime a ciência e a apuração policial para que haja eficiência da investigação.

Apesar de a evolução tecnológica trazer facilidade para o cometimento de crimes na rede, essa mesma tecnologia é utilizada pela polícia judiciária na colheita de provas. Muitas vezes a investigação é feita através de provedores de Internet ou com os gerenciadores do site acessado que rastreiam o IP (número de protocolo exclusivo de cada computador, que permite a comunicação das máquinas na rede) do computador utilizado pelo criminoso, o problema desse método é que muitos criminosos utilizam ferramentas para mascarar o número do IP. Além disso, existe a possibilidade de, através de autorização judicial, obter a quebra de sigilo telemático e interceptação de comunicações telefônicas dos dispositivos eletrônicos, conforme dispõe a Lei nº 9.296/96.

Outro método utilizado pelos investigadores para a obtenção de elementos informativos em crimes cibernéticos é a chamada engenharia social. Essa modalidade consiste em atos realizados pelo investigador a fim de influenciar o investigado a realizar alguma ação. Uma

forma de conseguir tal feito seria com a utilização de "*phishing*", em que através do envio de um e-mail, obtém informações, ou através do telefone, pelo *"vishing"*. Ocorre que, para ocorrer essa investigação, é necessário que a polícia crie contas falsas na internet, como no e-mail e nas redes sociais, a fim de obter a confiança do investigado ou utilizando de sua ingenuidade. (BRAGA, 2019). Entretanto, percebe-se que essa investigação se utiliza de perfis falsos que buscam conseguir a confiança do investigado.

Antes da inserção da infiltração virtual de agentes na legislação brasileira, em 2017, era comum o uso de perfis falsos pela polícia judiciária para a obtenção de elementos informativos no ambiente digital, principalmente na investigação de crimes de pornografia infantil. Essa técnica, após o advento da Lei nº 13.441/17, passou a estar relacionada com a infiltração virtual de policiais, devendo, portanto, ter autorização judicial para que tornasse lícita a prova colhida. Sendo assim, percebe-se que a ausência de autorização judicial prévia, torna a prova obtida ilícita e deverá ser desentranhada do processo, uma vez que violaria o direito de não autoincriminação. (SILVA, 2017)

Dessa forma, um dos métodos bastante utilizados no Brasil e no mundo para a investigação de crimes cibernéticos é a infiltração policial na internet. A infiltração virtual de agentes é um mecanismo que até mesmo antes da positivação no ordenamento jurídico brasileiro já era utilizado, amparando-se pela Lei nº 12.850/13, quando havia indícios de organização criminosa ou, não havendo, quando havia internacionalidade da conduta. Com a Lei nº 13.419/17, que alterou o ECA e a Lei nº 13.964/19, que alterou a Lei de Organizações Criminosas, a infiltração virtual passou a estar expressa no ordenamento, trazendo novos requisitos e características, os quais serão abordados no capítulo seguinte.

II - INFILTRAÇÃO POLICIAL

A infiltração policial é um método de investigação especial que consiste na inserção de um agente de polícia judiciária treinado, em um contexto criminoso, simulando estar fazendo parte desses crimes, a fim de obter provas, colher informações e identificar os suspeitos. Assim explica, Flávio Pereira (2012, p. 234):

> De inicio, con relación al agente infiltrado, deberá ser un sujeto, ordinariamente integrado en las fuerzas de seguridad del Estado, especialmente un agente de Policía, que utilizará de una "identidad supuesta" a los fines de conseguir se infiltrar y obtener la confianza de los otros miembros de la organización criminal. También deberá poseer el designio de investigar y descubrir una conducta delictiva en marcha o desarrollo, buscando pruebas, datos e informaciones que ayuden en la desarticulación de una concreta organización criminal. (PEREIRA, 2012, p. 234)

Percebe-se, portanto, que nessa técnica de investigação, o agente é inserido em uma organização criminosa, por exemplo, de maneira dissimulada, sendo criado um personagem para esse infiltrado a fim de que ele consiga ganhar a confiança dos criminosos e colher o máximo de informações possíveis.

Ocorre que, os crimes passaram a evoluir para um nível que vai além do físico, ou seja, passaram a ser praticados em ambientes virtuais, fazendo com que a infiltração física não tivesse tanta efetividade no combate à essa espécie de delito. Diante disso, essa nova roupagem da criminalidade trouxe um aspecto a mais, qual seja, a necessidade de conhecimento tecnológico. Daí surge a infiltração virtual, que nada mais é do que uma modalidade de infiltração policial que não se opera fisicamente, mas virtualmente por meio da internet.

Segundo a Delegada Federal Diana Calazans Mann (2018, págs. 18 e 19):

> [...] estar-se-á diante de uma infiltração virtual quando uma equipe de policiais especificamente designada para a tarefa, em face de indícios da prática de crimes cibernéticos – próprios ou impróprios, obtém uma autorização judicial e estabelece uma relação de confiança com um usuário da internet ainda não qualificado, mediante ocultação da condição de policial e criação de uma identidade fictícia, visando com isso, obter a qualificação do investigado e provas dos crimes praticados. Considera-se necessário inserir no conceito de infiltração digital o requisito da autorização judicial, uma vez que, presentes todos os elementos do conceito cunhado acima, haverá restrição a direitos fundamentais do investigado, restrições de tal ordem que somente se admitem com a vênia judicial, em face do princípio da reserva de juiz conforme se verá adiante. Presentes todos esses elementos, a atividade policial poderá ser considerada uma infiltração digital.

Portanto, a infiltração digital possui os mesmos objetivos daquela operada em meio físico, entretanto, será exercida por meio da internet, através de uma identidade falsa, a qual manterá contato e obterá confiança dos criminosos por meios informáticos.

Cabe ressaltar que, a figura do agente infiltrado (*underground* agente) não se confunde com o agente disfarçado, agente de inteligência, informante e colaborador. Enquanto o infiltrado deve necessariamente ter uma relação com os investigados, obtendo sua confiança, o agente disfarçado é um policial que, descaracterizado, busca investigar determinados crimes, sem, contudo, ter envolvimento com os investigados. O agente de inteligência, por sua vez, não constitui parte da polícia judiciária, portanto, não tem a função de investigar crimes. Portanto, esse agente busca investigar fatos que ameacem a soberania nacional. (SILVA, 2017)

Segundo Silva, o informante é aquele que não faz parte da polícia judiciária, porém, é depositada uma confiança nele, a fim de que entregue informações às autoridades policiais, de forma anônima, recebendo uma contraprestação material ou imaterial. (SILVA, 2017). E, por fim, o colaborador é aquele que é coautor ou partícipe do crime que está sendo investigado e, para obter benefícios legais, confessa o delito e contribui com a investigação. Há também a figura do agente provocador, que é vedada pelo ordenamento jurídico brasileiro e será abordada no próximo capítulo.

II.I - A evolução da infiltração policial no ordenamento jurídico brasileiro

A técnica especial de investigação, infiltração de agentes, é prevista em grande parte dos países democráticos, mas sua origem ocorreu na França, no ano de 1800 em que foi inserido o primeiro agente infiltrado denominado de Eugène Francois Vidocq, de forma particular, sem a intervenção do Estado. (JUNIOR, 2018, pág. 12).

> A infiltração policial é, hoje, utilizada em diversos países, sendo admitida, também, pelo Tribunal Europeu de Direito Humanos, desde que de acordo com o ordenamento jurídico interno do país, como foi declarado no caso *Bannikova contre Russie*. (SILVA, 2017, pág. 27)

A primeira vez que foi tratado a respeito da infiltração de agentes no ordenamento jurídico brasileiro foi em 2001, pela inserção no art. art. 2º, I, da Lei nº 9.034/1995, pela Lei nº 10.217/2001, como um método de investigação no combate às organizações criminosas. Essa Lei foi revogada pela Lei nº 12.850/2013, vigente nos dias atuais. O segundo diploma legal que

abordou tal técnica investigativa foi a Lei nº 10.409/2002, que tratava sobre o combate aos crimes relacionados a drogas, que foi revogada pela Lei nº 11.343/2006, vigente hoje em dia.

No ano de 2004, a Convenção das Nações Unidas contra o Crime Organizado Transnacional, foi promulgada no Brasil, por meio do decreto nº 5.015/2004. Essa convenção, também conhecida como "Convenção de Palermo" dispõe sobre as técnicas especiais de investigação em seu artigo 20.

Em 2017, foi publicada a Lei nº 13.441, a qual promoveu alterações na Lei nº 8.069/90 (Estatuto da Criança e do Adolescente), que passou a prever a infiltração de agentes no ambiente virtual, a fim de investigar, principalmente, crimes contra a dignidade sexual de crianças e adolescentes. E, por fim, em 2019, com a publicação da Lei nº 13.964 (Pacote Anticrime), a previsão da infiltração de policiais na internet foi inserida também na Lei de Organizações Criminosas (12.850/13) a qual já dispunha acerca da infiltração em meio físico. E ainda, inseriu na Lei de Lavagem de Dinheiro essa técnica especial de investigação.

Ressalta-se que, em 2016, a Lei nº 13.260/2016, que trata do terrorismo, previu que serão aplicadas as disposições da Lei nº 12.850/13 para a investigação, processo e julgamento. Sendo assim, entende-se que a infiltração de agentes também poderá ser utilizada para a investigação do terrorismo.

Insta salientar que, a infiltração de agentes no ambiente digital está prevista nas duas leis supracitadas, para investigação de crimes específicos elencados nas leis. Dessa forma, na Lei nº 12.850/13, tal investigação poderá ser realizada para investigar os crimes (não se aplica às contravenções penais) previstos na própria Lei e a eles conexos. Já o Estatuto da Criança e do Adolescente, trouxe um rol taxativo dos crimes que autorizam a infiltração de agentes na internet, são eles: crimes previstos nos arts. 240, 241 , 241-A , 241-B , 241-C e 241-D do próprio Estatuto e nos arts. 154-A, 217-A, 218, 218-A e 218-B do Código Penal Brasileiro.

Contudo, apesar dessas duas leis especificarem os crimes em que será autorizada a infiltração virtual, a maioria da doutrina entende que também se aplica à Lei de Drogas.

Portanto, atualmente é visto que tal modalidade de investigação está prevista expressamente no art. 53, I, da Lei nº 11.343/2006 (atual lei de drogas), nos arts. 10 a 14 da Lei nº 12.850/2013 (atual lei das organizações criminosas), nos arts. 190-A a 190-E, do Estatuto da Criança e do Adolescente, no art. 1º, §6º da Lei nº 9.613/1998 (Lei de Lavagem de Dinheiro), além da Convenção de Palermo, no art. 20.

II.II - Características e requisitos da infiltração policial cibernética

A infiltração policial virtual para ser realizada deve cumprir dois requisitos principais, são eles: o *fumus comissi delicti* e o *periculum in mora*. O *fumus comissi delicti* significa que deve haver pelo menos indícios da existência do crime para justificar a realização da investigação. Dessa forma, não é possível utilizar-se da infiltração para iniciar a investigação de um crime, sem que haja indícios da existência e indícios de autoria, contudo, não é exigido prova cabal do crime, somente indícios. Já o *periculum in mora* trata-se dos riscos e prejuízos que a demora para realização da medida pode causar na busca de elementos informativos. Contudo, deve-se ressaltar que tal modalidade de investigação é excepcional, ou seja, só será autorizada a sua realização caso a prova não possa ser obtida por outros meios. E o magistrado deve preferir aquelas menos invasivas, que restringem menos a esfera da liberdade individual do acusado.

a) Finalidade

A finalidade precípua da infiltração de agentes é detectar atividades ilícitas efetuadas pelos criminosos e informá-las às autoridades, recolhendo o máximo de provas possíveis. As provas, portanto, são indispensáveis e a prisão dos envolvidos é consequência dessa investigação. (MANN, 2017)

b) Subsidiariedade da infiltração

Acerca das características da infiltração na internet, é importante destacar a subsidiariedade. Tanto na Lei de Organizações Criminosas, no art. 10-A, quanto no Estatuto da Criança e do Adolescente, no art. 190-A, é visto que esse método de investigação no meio digital só poderá ser utilizado caso não seja possível produzir a prova por outros meios disponíveis. Ou seja, tal modalidade tem a característica de ser excepcional, pois só será efetivada se outros meios de produção de prova não forem eficientes e capazes.

Isso ocorre porque tal técnica é considerada de extremo risco para os agentes infiltrados, além disso, é uma investigação que demanda a relativização de direitos constitucionais

assegurados ao investigado e às vítimas (SILVA, 2017, pág. 65). Por esses motivos, destaca-se a subsidiariedade dessa medida, nas palavras de Oliveira e Kozan (2019) “para a deflagração dessa técnica especial de investigação é necessário analisar a essencialidade de cada medida, a fim de que não seja utilizada de forma indiscriminada.”. (OLIVEIRA; KOZAN. 2019, pág. 93)

Insta salientar que existem doutrinadores que criticam a subsidiariedade na infiltração realizada no ambiente virtual no que diz respeito aos riscos que o agente se submete, isso porque, diferentemente da infiltração física, essa não gera riscos à integridade física do infiltrado. Como explica Francisco Sannini Neto “[...] não vemos razão para a exigência de subsidiariedade em relação a esta técnica de investigação, constituindo, tal requisito, um embaraço desnecessário no combate aos crimes em questão.” (SANNINE NETO, 2017)

c) Necessidade de representação do delegado de polícia ou requerimento do Ministério Público e autorização judicial

Outro aspecto de extrema relevância para o assunto é a necessidade de representação do delegado de polícia ou requerimento do Ministério Público e a consequente autorização judicial para iniciar a ação de agentes de polícia infiltrados virtuais.

Assim como na infiltração mais antiga prevista no ordenamento jurídico, qual seja, a operada em meio físico, a digital também necessita de autorização judicial e oitiva do Ministério Público. As disposições que tratam dessa técnica especial de investigação dispõem que tal medida será adotada mediante requerimento do Ministério Público ou Representação do Delegado de Polícia.

Ambas as leis que tratam da infiltração no meio virtual abordam que, caso o pedido seja formulado pela autoridade policial, o juiz, antes de decidir, ouvirá o Ministério Público. Ocorre que, no caso inverso, se o pedido for feito pelo Ministério Público, o legislador se omitiu no que diz respeito a ouvir o delegado. Posto isso, alguns doutrinadores manifestam a respeito de ser necessária a oitiva da autoridade policial no caso da infiltração digital também, como explicam Cunha e Pinto (2017):

> A lei foi omissa quanto à oitiva do Delegado de Polícia quando a infiltração for requerida pelo MP. Anotamos, porém, que o art. 10, da lei 12.850/13 (Criminalidade Organizada), dispõe que, solicitada a infiltração, no curso do inquérito policial, antes deve ser tomada a "manifestação técnica do delegado

> de polícia". Cremos que, a despeito da omissão do legislador, seja salutar essa oitiva. Afinal, se apenas "agentes de polícia" podem ser infiltrados, não faz sentido que a autoridade policial deixe de ser previamente consultada sobre a medida. (CUNHA, Rogério; PINTO, Ronaldo, 2017)

Dessa forma, tendo em vista que o Delegado de Polícia é quem preside o inquérito policial, não faz sentido que a infiltração seja executada sem a sua oitiva, afinal, é ele quem pode dizer se tal operação é viável naquele momento e se existem agentes disponíveis e preparados.

d) Prazo

Em relação à duração da infiltração, o legislador especificou em cada lei o tempo máximo. E é através dessa duração que a doutrina divide a infiltração, tanto física, quanto virtual em *Ligth Cover* e *Deep Cover*. Antes de abordarmos os tempos especificamente de cada lei, conceituaremos essas duas formas de infiltração, conforme a doutrina.

Primeiramente, cabe informar que tais denominações surgiram na doutrina norte-americana, e os estudiosos brasileiros passaram a utilizá-la também no Brasil. A infiltração *Light Cover*, também conhecida como “infiltração leve” é aquela que demanda menos tempo, oferecendo menor risco para o agente. Já a *Deep Cover*, ou “infiltração profunda” é aquela que dura mais tempo, tem maior risco e é mais complexa. (PIRES, 2018, p. 21)

No que diz respeito aos prazos da infiltração na internet, no Estatuto da Criança e do Adolescente, o prazo previsto é de até 90 dias, podendo ser renovado, sem ultrapassar o prazo máximo de 720 dias, desde que seja demonstrada efetiva necessidade e o juiz autorize, analisando “a adequação, a necessidade e a razoabilidade, decidindo de forma fundamentada” (ZANELLA, 2020). Dessa forma, segundo o entendimento da doutrina, uma infiltração que demande um tempo de aproximadamente 90 dias é considerada “*Light Cover*”, já aquela que é renovada, não ultrapassando 720 dias classifica-se como “*Deep Cover*”.

Já na Lei de Organizações Criminosas, o legislador inseriu prazos máximos diferentes para a infiltração “*in loco*” (real) e a virtual, sendo que, para a primeira, o prazo limite é de 6 meses, porém, não é especificado quantas vezes e até quando é possível a renovação além desse prazo e, para a segunda, é especificado que também terá o limite de 6 meses, porém, poderá ser renovado somente até o máximo de 720 dias, devendo comprovar a efetiva

necessidade, assim como na Lei nº 8.069/90. Nessa lei, percebe-se que, em relação à infiltração digital, aquela considerada "*Light Cover*" é a que dura até 6 meses e aquela que demanda renovações, não ultrapassando o máximo de 720 dias, classifica-se como "*Deep Cover*", segundo a doutrina.

Por fim, a Lei de Drogas, a Lei de Lavagem de Dinheiro e a Convenção de Palermo, apesar de permitirem a infiltração real, não fazem qualquer menção ao prazo máximo desse procedimento investigatório.

A partir do exposto, é possível perceber que, para a infiltração física, o legislador não traz expressamente em nenhuma das leis o prazo máximo em que essa investigação poderá ser renovada, em contrapartida, nas duas leis que abordam a infiltração digital, é disposto expressamente que o total não poderá exceder o máximo de 720 dias.

Há críticas na doutrina a respeito desse prazo limitador que o legislador impôs para a infiltração digital. Isso porque, apesar de ser um obstáculo no abuso das investigações, em determinados casos mais complexos, pode ser necessário um tempo maior de operação. O professor Everton Zanella (2020) argumenta que o melhor seria se o legislador não previsse um tempo limite, mas sim fazer como nas interceptações telefônicas e na infiltração física, condicionando as renovações à comprovação de sua imprescindibilidade. (ZANELLA, 2020)

e) Agente de polícia judiciária e a voluntariedade do infiltrado

Conforme as duas leis que tratam da infiltração policial virtual, os únicos policiais que podem realizar tal investigação são a polícia civil e a federal, que são as polícias judiciárias, autorizadas a apurar infrações penais. Os policiais militares, rodoviários, ferroviários e guardas municipais não estão autorizados a realizar tal investigação. Além disso, estão vedados os membros do Ministério Público, os agentes de inteligência, detetives particulares etc.

Diferentemente do que ocorre na infiltração física na Lei nº 12.850/13, o legislador, ao prever a infiltração digital no Estatuto da Criança e do Adolescente, não abordou o direito do agente infiltrado de recusar a participação. Dessa forma, parte da doutrina entende que a infiltração operada no meio digital prescinde de anuência do agente, devendo, entretanto, ser infiltrado aquele agente que detém conhecimento de computação. (SANNINE NETO, 2017).

Contudo, alguns doutrinadores viram a possibilidade de utilizar o art. 14 da Lei de Organizações Criminosas para a infiltração digital prevista no ECA, pelos seguintes motivos.

Antes da publicação da Lei nº 13.964 de 2019, a única previsão da infiltração no ambiente virtual era no Estatuto da Criança e do Adolescente, em que o legislador não previu os direitos do agente infiltrado. A previsão desses direitos estava expressa somente na Lei 12.850/13 para a infiltração operada no meio físico. Diante disso, surgiram divergências no que diz respeito à aplicação desses direitos para o infiltrado virtual. Sendo assim, como visto acima, alguns doutrinadores afirmavam não ser aplicável no meio digital tendo em vista, por exemplo, o menor risco que o agente sofreria. Porém, outros acreditavam ser possível a aplicação desses direitos, previstos no art. 14 da Lei nº 12.850/13, para a infiltração digital. Cavalcante (2017), por exemplo, aborda dois argumentos para tal aplicação analógica:

> Penso que seja possível estender esses direitos também ao agente infiltrado de que trata o art. 190-A do ECA por duas razões: a) trata-se de analogia com a finalidade de proteger a integridade física de um agente estatal; b) a maioria dos grupos criminosos que praticam delitos contra a dignidade sexual de crianças e adolescentes na internet caracterizam-se como organizações criminosas (art. 1º, § 1º da Lei nº 12.850/2013), aplicando-se, por consequência, o art. 14 dessa Lei. (CAVALCANTE, 2017)

Ocorre que, em dezembro de 2019, com a publicação do Pacote Anticrime, foi inserida na Lei de Organizações Criminosas a modalidade virtual de infiltração de agentes, no art. 10-A a 10-D. Dessa forma, é possível inferir que os direitos previstos no art. 14 do referido dispositivo dizem respeito aos dois tipos de infiltração, tanto o inserido recentemente quanto aquele já expresso anteriormente, já que não há nada vedando a aplicação. Posto isso, acredita-se que tais direitos podem ser aplicados, por analogia, à infiltração disposta no Estatuto da Criança e do Adolescente também.

f) Riscos

Os riscos que a ação infiltrada gera ao agente são grandes, tendo em vista que o policial terá que obter a confiança do(s) investigado(s), gerando perigo não só para si, mas até para seus familiares. Entretanto, é fato que a infiltração digital acarreta menos riscos do que a real, já que não há contato físico entre o agente e o investigado. Além disso, a identidade fictícia do agente

também é criada na infiltração virtual, pois, em diversos momentos o infiltrado terá que se identificar para os investigados, a fim de que obtenha sucesso nas investigações.

Entretanto, o art. 12, §3º, da Lei nº 12.850/13, disciplina que a operação será sustada mediante requisição do Ministério Público ou pelo delegado de policial se houver indícios seguros de que o infiltrado sofre risco iminente. A despeito da investigação virtual ter menos riscos, é possível inferir que tal dispositivo, apesar de ter sido disposto à infiltração "*in loco*", também poderá ser aplicado à infiltração na internet, tendo em vista que os riscos são menores, mas existem.

Essa característica está muito ligada à voluntariedade do agente abordada anteriormente, pois, discute-se a respeito da conduta volitiva do agente de negar participação na infiltração virtual, já que os riscos são extremamente menores que a física.

g) Sigilo

A infiltração virtual de agentes, assim como a física, é medida extremamente sigilosa. O artigo 10-B, da Lei nº 12.850/13 e o artigo 190-B, do ECA, asseguram que, aos autos do procedimento, apenas o juiz, o Ministério Público e o delegado de polícia responsável pelo caso poderão ter acesso. Sendo assim, por óbvio, a defesa técnica não poderá ter conhecimento da infiltração, até a conclusão das diligências. Deve o juiz, portanto, zelar pelo sigilo da investigação, para assegurar sua eficácia.

Por esse motivo, a infiltração é executada somente na fase de inquérito policial, para subsidiar uma denúncia futura, pois, durante a fase processual, já existe contraditório e ampla defesa, perdendo o sentido da infiltração, que deve ser sigilosa.

h) Responsabilidade criminal do agente

A infiltração policial permite que o agente, a fim de colher indícios de autoria e materialidade, cometa alguns ilícitos penais, isso porque, quanto mais imerso ele estiver naquele contexto criminoso, mais chance de a investigação dar certo, contudo, para isso o agente infiltrado deve ganhar a confiança dos criminosos.

Para isso, portanto, a Lei nº 12.850/13, no art. 13, §1º, determinou que "Não é punível, no âmbito da infiltração, a prática de crime pelo agente infiltrado no curso da investigação, quando inexigível conduta diversa.". Supõe-se que tal dispositivo se refere à infiltração operada no meio físico, pois, após a inserção da infiltração digital na lei, a exclusão da responsabilidade se deu de maneira diferente, que será tratado posteriormente.

Sendo assim, a partir do supracitado artigo, alguns doutrinadores entendem que, o agente infiltrado, caso cometa algum crime durante a infiltração, terá excluída a culpabilidade por inexigibilidade conduta diversa. Como ensina Guilherme de Souza Nucci (2021):

> Trata-se de excludente de culpabilidade, demonstrando não haver censura ou reprovação social ao autor do injusto penal (fato típico e antijurídico), porque se compreende estar ele envolvido por circunstâncias especiais e raras, evidenciando não lhe ter sido possível adotar conduta diversa. (NUCCI, 2021, p. 148)

Ocorre que, existem divergências doutrinárias quanto à natureza jurídica da exclusão da responsabilidade penal do agente infiltrado. Apesar da doutrina majoritária entender pela exclusão da culpabilidade, alguns autores, como Damásio de Jesus, entendem que deve ocorrer a exclusão da ilicitude, diante do estrito cumprimento do dever legal. (ZANELLA, 2020)

Em se tratando da infiltração operada no meio digital, os dispositivos legais tanto no ECA (art. 190-C), quanto na Lei do Crime Organizado (art. 10-C), são idênticos no que diz respeito à responsabilidade criminal do agente infiltrado. Esses artigos preveem que não comete crime o policial que oculta a sua identidade para, por meio da internet, colher indícios de autoria e materialidade nos crimes que estão investigando.

Percebe-se, portanto, que nesse caso, é usado o termo "não comete crime", enquanto naquele falava-se que "não é punível". Há uma crítica à redação desse dispositivo por parte dos doutrinadores, por não explicar diretamente a causa absolutória na qual estará amparado o agente infiltrado. Cunha e Pinto (2017) entendem que tais dispositivos garantem a exclusão da tipicidade especificamente para o agente que oculta sua identidade na internet para colher indícios de autoria e materialidade, ou seja, que há a excludente somente para o crime previsto no art. 154-A do CP (invasão de dispositivo informático).

Para esses autores, os legisladores do dispositivo agiram com pouca técnica, deixando uma lacuna:

> Melhor seria se tivesse adotado forma semelhante à da lei 12.850/13, que simplesmente exclui a punição do agente infiltrado que comete crime por inexigibilidade de conduta diversa. É certo que no caso da infiltração virtual não é fácil vislumbrar hipóteses em que o agente policial pudesse ser colocado em uma situação na qual lhe seria inexigível outra conduta a não ser a criminosa, pois, pelas próprias características dessa forma de infiltração, não deve haver contato pessoal entre ele e os autores dos crimes sob investigação. Logo, a probabilidade de risco imediato à integridade pessoal é amenizada. Mas nada impediria a imposição de uma causa excludente da tipicidade tratando expressamente da exclusão do crime de invasão de dispositivo informático e de outros crimes eventualmente cometidos por meio virtual. (CUNHA; PINTO, 2017)

Dessa forma, percebe-se que há uma lacuna e, diante disso, diversas interpretações. Cunha e Pinto acreditam que a atipicidade deve ser estendida aos demais crimes que o infiltrado estará investigando. Já o Delegado de Polícia Civil Henrique Hoffmann Monteiro de Castro (2017) entende que ficará excluída a ilicitude das condutas típicas praticadas pelo agente para manter a identidade fictícia, como falsidade documental ou ideológica, por estrito cumprimento do dever legal.

II.III- A dificuldade de investigação nos ambientes profundos da internet (*deep web* e *dark web*)

Como já abordado anteriormente, o desenvolvimento da internet foi extremamente importante para a globalização, comunicação e acesso à informação pela população de todo o mundo. A parte da internet que a grande maioria dos usuários acessa com propósitos comuns, como redes sociais, buscas no google, Youtube etc., é chamada de *surface*. Essa parte da internet chamada *surface* é uma pequena parcela de toda a rede, é conhecida como a parte "amigável" da internet, aquela em que a maior parte da população acessa no dia a dia, com facilidade. Ocorre que, essa parte da rede é facilmente rastreada e a privacidade dos usuários é facilmente violada. Por esse motivo, ambientes profundos foram desenvolvidos na internet a fim de dificultar o rastreio dos dados, com objetivo de ter uma navegação mais anônima, sendo um ambiente de difícil acesso pela maioria das pessoas. (ALMEIDA, 2020).

A *Deep Web*, portanto, é essa parte profunda da internet, anônima e criptografada, a qual necessita de softwares específicos para ser acessada. Essa rede é conceituada por Shimabukuro e Silva como:

> A internet profunda, ou Deep Web nada mais é do que a parte da rede cujo conteúdo não está disponível ou indexado nos principais mecanismos de pesquisa (Google, Bing, Yahoo). Ela é formada por milhões de páginas, com dimensão inimaginável e com crescimento similar ao da Internet Visível. (SHIMABUKURO, Adriana; SILVA, Melissa Garcia Blagitz de Abreu. apoud SILVA, 2017, p. 20)

Ocorre que, essa dificuldade de acesso, ao longo dos anos, foi se tornando mais acessível aos usuários, por isso, foi desenvolvida uma rede ainda mais profunda e anônima, chamada de *Dark Web*. Essa rede somente é acessada por quem possui as credenciais completas, pois os sites são formados por números e letras sem sentido. Apesar de não ser um ambiente criado efetivamente para o cometimento de delitos, muitos criminosos utilizam do anonimato que ela proporciona para cometer crimes como tráfico de drogas, pornografia infantil, fraudes, dentre outros.

Nesse sentido, percebe-se que, por ser um ambiente criptografado, de difícil acesso e rastreio, a investigação de crimes cometidos nessa rede é um desafio para a polícia judiciária. É importante ressaltar que, apesar de a *Dark Web* ser quase impossível de ser rastreada pelas autoridades, nenhuma rede é cem por cento segura. Por esse motivo, as investigações nesse ambiente devem ser inovadoras, usando técnicas especiais.

No Brasil, existiram algumas operações de combate a crimes cometidos nas partes profundas da internet em que se utilizou a infiltração virtual de agentes. Algumas dessas investigações foram antes do advento da Lei nº 13.441/17, que previu a infiltração na internet, porém, sendo fundamentadas na Lei nº 12.850/13, que, na época, previa somente a infiltração física. Outras operações já foram realizadas depois de 2017, fundamentadas no Estatuto da Criança e do Adolescente, que teve a infiltração virtual inserida pela Lei nº 13.441/17.

Pode-se citar como exemplo as operações *Dyrtnet*, *Darknet* e Protetor, realizadas pela Polícia Federal, a fim de combater crimes sexuais infanto-juvenis, em que foram utilizadas a infiltração virtual de agentes para a investigação. Todas as operações, através da infiltração de um agente com um perfil falso, desencadearam na prisão de diversas pessoas que praticavam crimes previstos no Estatuto da Criança e do Adolescente, além da apreensão de HD's e DVD'S. (RODRIGUES; CARDOSO; MARWELL, 2021).

O policial federal Luiz Walmocyr dos Santos Junior, explicou como que a infiltração de um agente na *Dark Web* é importante para a captura dos criminosos. Como já abordado anteriormente, esse ambiente da internet é de difícil acesso, sendo quase impossível rastrear o IP. O policial, então, explica que é criada uma estrutura, dentro de um servidor, fazendo com que o usuário seja trazido para a internet tradicional para que possa ser rastreável, ou seja, o criminoso, sem saber, sai por alguns segundos do ambiente TOR (software que permite a criptografia), momento em que o IP do usuário se torna rastreável. (RODRIGUES; CARDOSO; MARWELL, 2021).

Percebe-se, portanto, que essa técnica especial de investigação é utilizada de forma subsidiária pela polícia federal do Brasil, porém, é bastante eficaz, principalmente nos crimes virtuais contra a dignidade sexual de crianças e adolescentes. O Brasil é referência internacional na utilização dessa técnica de investigação, possuindo notoriedade no combate aos crimes sexuais infanto-juvenis cometidos no ambiente virtual, assim como o FBI. ((RODRIGUES; CARDOSO; MARWELL, 2021).

III - VALIDADE DAS PROVAS COLHIDAS DURANTE A INFILTRAÇÃO POLICIAL VIRTUAL

Restando esclarecida e compreendida essa técnica de investigação especial no âmbito digital, bem como suas características e sua importância na persecução penal, passa-se a analisar a validade das provas colhidas por essa infiltração.

Muitos doutrinadores possuem o entendimento de que a validade da infiltração no ambiente virtual é a mesma daquela operada no meio físico, disposta no art. 10, da Lei nº 14.850/13 e daqueles métodos especiais de investigação dispostos na Lei de Interceptações, Lei nº 9.296/1996. (ALMEIDA, 2019).

A infiltração no ambiente virtual demanda mais dificuldade para a obtenção de provas válidas do que a infiltração real. Isso ocorre porque, no ambiente cibernético a investigação pode afetar diversos países, já que as barreiras nacionais são facilmente ultrapassadas na criminalidade virtual e, além disso, o anonimato gerado pela rede, causa obstáculos na investigação, tendo em vista a existência dos direitos à intimidade, privacidade e ao sigilo das informações inerentes a qualquer pessoa. Entretanto, vale lembrar que nenhum direito

fundamental é absoluto, ou seja, é possível que sejam restringidos em determinadas ocasiões, para o bem comum, em virtude do grau de periculosidade dos crimes que estão sendo investigados.

Assim sendo, para que a prova obtida seja válida, a infiltração digital deve seguir requisitos que serão observados tanto pelo legislador quanto pelo juiz, observando alguns princípios supraconstitucionais, dentre eles, o princípio da superioridade ética do estado, princípio da lealdade, princípio da reserva de constituição, princípio da proibição de autoincriminação e princípio da proporcionalidade.

A superioridade ética do Estado dispõe que os servidores que estão atuando na investigação, não pratiquem atos que façam com que se equiparem com os criminosos, devendo agir sempre em conformidade com o estado democrático de direitos. Por óbvio, a infiltração policial gera um choque entre a atuação do agente e o princípio mencionado e, por esse motivo, essa técnica de investigação deve ser ponderada pelo princípio da proporcionalidade, a fim de minimizar o confronto com as regras sociais. (MANN, 2018)

Dessa forma, a ponderação dos direitos restringidos para a realização dessa operação é feita através da proporcionalidade. Sendo assim, a proporcionalidade atua como um critério de valoração na atuação do Estado, devendo alcançar um equilíbrio no interesse do particular e no interesse público, pois, de um lado encontra-se a busca do *ius puniendi* do Estado, a fim de garantir a segurança coletiva e do outro encontra-se a garantia dos direitos fundamentais do investigado. (PEREIRA, 2012). Esse princípio, portanto, é essencial para que as provas obtidas possuam validade no processo penal, sendo necessário analisar o caso concreto e observar o critério trifásico de adequação, necessidade e proporcionalidade em sentido estrito da medida. (MANN, 2018).

Nesse sentido, quando se fala em adequação, o magistrado deve analisar se com a infiltração será possível alcançar o fim que pretende, ou seja, se os resultados da infiltração serão úteis para a solução do crime investigado.

Em relação à necessidade, deve-se demonstrar que aquela medida é indispensável para obter sucesso na investigação, analisando se outros meios de obtenção de prova menos invasivos não são aptos a esse fim. Essa necessidade é vista principalmente quando os crimes ocorrem em ambientes criptografados com grande restrição de acesso.

No que concerne à proporcionalidade em sentido estrito, entende-se que será analisado se as vantagens obtidas pela medida aplicada serão superiores às desvantagens causadas por ela. (SILVA, 2017). Sendo assim, no que concerne à infiltração virtual, deve-se ponderar se os direitos restringidos do investigado, em relação aos bens jurídicos em risco, justificam a aplicação dessa medida. É possível citar como exemplo os crimes contra a dignidade sexual de crianças e adolescentes cometidos na internet, em que a proteção desse bem jurídico, quando sopesado com os direitos que serão restringidos dos investigados, justificam a aplicação da infiltração, mesmo que a privacidade e intimidade dos suspeitos sejam afetados.

Nesse sentido, é visto que a técnica especial de investigação abordada sempre será realizada através da proporcionalidade, principalmente por ser uma medida invasiva, que afeta direitos constitucionais e que possui grande risco para o agente infiltrado. Assim como ensina Pereira:

> Por esto, resulta imprescindible someter los pedidos de autorización para operaciones encubiertas a un filtro rígido y marcado por el carácter de excepcionalidad, de modo que este control sirva —a través del principio de proporcionalidad— como un arma de seguridad a la sociedad, al individuo y al Estado, evitándose de este modo una flexibilización abusiva de los derechos y garantías fundamentales de aquellas personas sometidas a la persecución penal. (PEREIRA, 2012, p. 469).

Sendo assim, da mesma forma que a proporcionalidade será observada quando o magistrado for decidir pela autorização ou não da medida, terá que ser observada a todo momento pelo agente infiltrado e por todos os que estiverem participando da operação, a fim de que não prejudique a validade das provas obtidas e não gere riscos físicos para o infiltrado.

Logo, essa técnica de investigação é válida, quando é um meio imprescindível para a investigação, haja vista que nenhum direito é absoluto e, para que as provas obtidas por meio dela sejam legítimas, deve-se ater aos princípios da proporcionalidade e excepcionalidade. (OLIVEIRA; KOZAN. 2019, pág. 96/97)

III.I - Princípio do *Nemo Tenetur se Detegere*

Um dos direitos do investigado que é mitigado pela infiltração de agentes é o direito à não autoincriminação, também conhecido em latim por *nemo tenetur se detegere*. Esse princípio

é uma modalidade do direito à autodefesa e assegura que o investigado não é obrigado a produzir provas em seu desfavor, isto é, não é obrigado a ajudar na produção de provas que o incriminem.

Na Constituição Federal de 1988, esse direito está disposto no art. 5º, inciso LXXIII, através do direito ao silêncio, que é uma das garantias intrínsecas do direito à não autoincriminação. Esse direito assegura que o investigado pode calar-se perante autoridades, a fim de não colaborar para a produção de provas contra si e tal conduta não poderá ser interpretada em nenhuma hipótese em seu desfavor.

Renato Brasileiro Lima conceitua esse direito fundamental como sendo:

> [...] uma modalidade de autodefesa passiva, que é exercida por meio da inatividade do indivíduo sobre quem recai ou pode recair uma imputação. Consiste, grosso modo, na proibição de uso de qualquer medida de coerção ou intimidação ao investigado (ou acusado) em processo de caráter sancionatório para obtenção de uma confissão ou para que colabore em atos que possam ocasionar sua condenação. (LIMA, 2017, apoud SILVA, 2017, p. 73)

Nesse sentido, quando se trata de uma infiltração policial, seja ela real ou virtual, há uma limitação desse direito ao investigado. Isso porque, os investigados acabam contribuindo para a obtenção de provas contra si sem saber, pois desconhecem a condição de agente infiltrado daquele membro da organização em quem confiam. (MANN, 2019)

Por esse motivo, a necessidade de que a infiltração de agentes seja admitida somente em casos excepcionais, ou seja, naquelas situações em que o prejuízo social causado por aqueles crimes justifica a mitigação de direitos fundamentais em benefício da sociedade.

Entretanto, insta ressaltar que, por ser uma medida severa, é necessário que os agentes ajam com cautela, haja vista que a vontade do investigado não pode ser induzida pelos agentes, isto é, os infiltrados não podem interferir na conduta dos investigados, devem demonstrar que aquele resultado seria produzido ainda que o agente infiltrado não estivesse presente. (MANN, 2019)

III.II - Agente infiltrado como testemunha anônima

Um dos direitos do agente infiltrado é o anonimato, esse direito garante a segurança do agente e possibilita outras operações de infiltração. Sendo assim, o infiltrado tem o direito de

ter sua identidade preservada durante a fase extrajudicial e durante todo o processo. Todavia, há questionamentos acerca de o agente infiltrado ser ouvido em juízo como testemunha e se sua identidade permaneceria em sigilo.

É pacífico na doutrina e na jurisprudência o entendimento de que o policial infiltrado poderá ser arrolado para depor em juízo como testemunha se a defesa requerer sua oitiva ou se as provas carreadas aos autos não forem suficientes. Entretanto, quanto ao anonimato do agente e seus dados qualificativos, a doutrina diverge.

Guilherme de Souza Nucci (2021), entende que o anonimato do policial deve se manter somente para o público em geral e da imprensa. No entanto, para o réu e seu defensor deve ser identificado o policial infiltrado, sob pena de ferir o direito à ampla defesa do réu. Isso porque, a testemunha anônima, "não pode ser contraditada, nem perguntada sobre muitos pontos relevantes, visto não se saber quem é. Além disso, todos os relatórios feitos por esse agente camuflado – e nunca revelado – não podem ser contestados, tornando-se provas irrefutáveis [...]" (NUCCI, 2021, p.147)

Já Renato Brasileiro Lima, citado por Zanella (2020) entende que "o agente infiltrado deve ser uma testemunha anônima em relação aos demais acusados, porém seus dados qualificativos devem ser disponibilizados ao defensor técnico, a quem cabe a responsabilidade de preservar o sigilo". Percebe-se que Lima tem um entendimento que está no meio termo, já que acredita que o anonimato deve ser mantido em relação aos acusados, mas que a defesa técnica deve conhecer a identificação do agente infiltrado.

Por fim, um terceiro entendimento é do sigilo absoluto dos dados do agente infiltrado. Esse entendimento é seguido pelo professor Marcelo Mendroni (2020) e por Everton Zanella (2020).

Mendroni (2020), portanto, argumenta que a identificação do agente deve ser mantida em sigilo por três principais razões. O primeiro motivo é de que, se a identidade do agente for revelada, dificilmente o policial concordará em colaborar, já que os criminosos vão saber sua real identidade. A outra razão é de que, sendo revelada a identidade, esse policial não mais poderá ser infiltrado em outras operações e, portanto, faltará agentes preparados para atuar nessas operações de risco. Por fim, a razão mais evidente é a do risco à vida do agente, não só dele, como de seus familiares.

Para tanto, explica:

> [...] nos parece evidente que, quando testemunhe em Juízo, deverá ter a sua verdadeira identidade mantida em sigilo, com tratamento especial, para sua

> própria proteção e de sua família, utilizando-se, além dos dispositivos previstos na própria Lei nº 12.850/13 – específica, também, subsidiariamente, no que couber, os dispositivos da Legislação de Proteção a testemunhas – Lei nº 9.807/99. (MENDRONI, 2020, p. 212)

Logo, para ele a identidade do policial infiltrado deverá limitar-se ao conhecimento do Delegado de Polícia que coordena a operação, do Promotor e do Juiz.

Zanella (2020) concorda com o posicionamento acima, ressalvando que o depoimento do agente infiltrado não deve ser regra, ou seja, deve somente ser colhido de forma excepcional, quando for imprescindível. Para tanto, argumenta que:

> se isso ocorrer, deve o testemunho efetivamente ser anônimo, preservando-se os dados identificadores e qualificativos do agente infiltrado, até mesmo em relação aos advogados dos acusados, já que tratamos de processos-crimes que envolvem membros de organizações criminosas, de forma que, aplicando-se o princípio da proporcionalidade, é imperioso optar-se pela preservação da segurança do agente infiltrado. (ZANELLA, 2020)

O professor ainda argumenta que esse entendimento não fere o princípio da ampla defesa, como entendem alguns doutrinadores, haja vista que a defesa técnica terá acesso a todos os autos e às provas colhidas na infiltração. Assim, a fim de garantir a ampla defesa e o contraditório, a oitiva do policial infiltrado deve ser feita por sistema de videoconferência, com utilização de distorção de voz e imagem, como ocorre em Portugal e na França. (ZANELLA, 2020)

III.III - Descoberta fortuita de provas

Na infiltração virtual de agentes, é possível que ocorra a descoberta de provas relacionadas a outros crimes que sequer estão sendo investigados. Por exemplo, o agente infiltrado está investigando o crime de venda de registros que contenham cenas de sexo ou pornografia envolvendo crianças (art. 241, do ECA) e acaba descobrindo outros crimes também cometidos por aqueles investigados, como por exemplo crime de tráfico de pessoas.

Nesse caso, as provas obtidas de forma fortuita são válidas, em razão do fenômeno da serendipidade que consiste justamente em buscar algo e encontrar outra coisa. É pacífico o entendimento do STJ da validade das provas obtidas de forma fortuita nos casos de

interceptação telefônica, sendo interpretada pela doutrina da mesma forma para a infiltração policial. (CAVALCANTE, 2017).

Confira precedentes da Corte Superior de Justiça:

> RECURSO ORDINÁRIO EM HABEAS CORPUS. CABIMENTO. EXERCENTE DE MANDATO ELETIVO. MEDIDA CAUTELAR. SUSPENSÃO DO EXERCÍCIO. INDÍCIOS DE AUTORIA. REAVALIAÇÃO. EXAME APROFUNDADO. IMPOSSIBILIDADE. CONVERSA NO WHATSAPP. SIGILO. QUEBRA POR DECISÃO JUDICIAL. ENCONTRO FORTUITO DE PROVAS. POSSIBILIDADE. CORRUPÇÃO PASSIVA E ORGANIZAÇÃO CRIMINOSA. PRÁTICA NO EXERCÍCIO DO CARGO E EM RAZÃO DELE. CONTEMPORANEIDADE. INEXIGÊNCIA. EXISTÊNCIA. JUSTO RECEIO. FATOS POSTERIORES. DESNECESSIDADE. PROIBIÇÃO DE CONTATO COM OUTROS IMPUTADOS. INSUFICIÊNCIA. OFENSA À CONSTITUIÇÃO. INOCORRÊNCIA. RECURSO DESPROVIDO. [...] 3. Não é ilícito o uso de prova decorrente do seu encontro fortuito, sendo válidos os elementos obtidos casualmente, por ocasião do cumprimento autorizado de medida de obtenção de prova relativa a outro delito, ainda que inexista conexão ou continência com o crime supervenientemente encontrado e que este não cumpra os requisitos autorizadores da medida probatória, desde que não haja desvio de finalidade na execução do meio de obtenção de prova. [...] 7. Recurso desprovido. (RHC 118.641/RS, Rel. Ministro RIBEIRO DANTAS, QUINTA TURMA, julgado em 23/03/2021, DJe 26/03/2021) (grifo nosso)

> PENAL. AGRAVO REGIMENTAL NO RECURSO ESPECIAL. OFENSA AO PRINCÍPIO DA COLEGIALIDADE. NÃO OCORRÊNCIA. AUTORIA DELITIVA. MATÉRIA NÃO PREQUESTIONADA. INCIDÊNCIA DA SÚMULA 282/STF. INTERCEPTAÇÃO TELEFÔNICA. SERENDIPIDADE. POSSIBILIDADE. DOSIMETRIA. CONSEQUÊNCIAS DO DELITO. EXASPERAÇÃO DA PENA-BASE. FUNDAMENTAÇÃO IDÔNEA. QUANTUM DA REPRIMENDA. PROPORCIONALIDADE. AGRAVO REGIMENTAL DESPROVIDO.
> [...] 5. **A jurisprudência desta Corte é firme no sentido da adoção da teoria do encontro fortuito ou casual de provas (serendipidade).** Segundo essa teoria, **independentemente da ocorrência da identidade de investigados ou réus, consideram-se válidas as provas encontradas casualmente pelos agentes da persecução penal, relativas à infração penal até então desconhecida, por ocasião do cumprimento de medidas de obtenção de prova de outro delito regularmente autorizadas, ainda que inexista conexão ou continência com o crime supervenientemente encontrado e este não cumpra os requisitos autorizadores da medida probatória, desde que não haja desvio de finalidade na execução do meio de obtenção de prova.** [...] 9. Agravo regimental não provido. (AgRg no REsp 1752564/SP, Rel. Ministro RIBEIRO DANTAS, QUINTA TURMA, julgado em 17/11/2020, DJe 23/11/2020) (grifo nosso)

> [...] 1. **Não há violação ao princípio da ampla defesa** a ausência das decisões que decretaram a quebra de sigilo telefônico em investigação originária, na qual **de modo fortuito ou serendipidade se constatou a existência de indícios da prática de crime diverso do que se buscava,** servindo os documentos juntados aos autos como mera notitia criminis, em razão da total independência e autonomia das investigações por não haver conexão delitiva. 2. **O chamado fenômeno da serendipidade ou o encontro fortuito de provas - que se caracteriza pela descoberta de outros crimes ou sujeitos ativos em investigação com fim diverso - não acarreta qualquer nulidade ao inquérito que se sucede no foro competente**, desde que remetidos os autos à instância competente tão logo verificados indícios em face da autoridade. [...] (RHC 60.871/MT, Rel. Ministro NEFI CORDEIRO, SEXTA TURMA, julgado em 04/10/2016, DJe 17/10/2016) (grifo nosso)

Percebe-se, portanto, que as provas obtidas durante a infiltração virtual de agentes de forma fortuita, poderá ser considerada válida, em razão do fenômeno da serendipidade, ainda que o crime descoberto não seja autorizador da medida de infiltração policial. Ressalta-se, dessa forma, a importância desse entendimento para a investigação criminal, haja vista que, ainda que a infiltração seja autorizada para a investigação do crime A, caso descubra-se a ocorrência também de um crime B, essas provas poderão ser utilizadas no processo penal para a responsabilização do investigado pelos crimes descobertos.

III.IV - Informações compartilhadas na internet como material probatório

É evidente que informações compartilhadas na internet podem ser utilizadas como provas no processo penal. Entretanto, é preciso fazer uma análise acerca dessas informações para averiguar quais delas fere o direito à intimidade do ofendido.

Para isso, Almeida (2019) diferencia as informações públicas das informações privadas compartilhadas nas redes. As informações que são publicadas abertamente de maneira voluntária e consciente para diversas pessoas, revertem-se de caráter público. Sendo assim, não há privacidade a ser protegida pelo direito, uma vez que o autor da mensagem publicou por livre e espontânea vontade, consentindo tacitamente ou expressamente ao acesso legítimo ao seu direito de intimidade.

Nesse sentido, as provas obtidas por meio de informações compartilhadas nas redes de maneira pública, não ofendem o direito à intimidade do investigado, sendo, portanto, válidas no processo penal.

No entanto, existem também aquelas informações publicadas de maneira privada, que dificulta a sua obtenção para ser utilizada no processo penal, haja vista afrontar garantias constitucionais do investigado.

As informações consideradas privadas são aquelas em que são publicadas pelo titular para uma pessoa ou um determinado grupo de pessoas de sua escolha através da confiabilidade. Entretanto, é necessário salientar que aquelas conversas realizadas, por exemplo, em "salas de bate-papo" não estão amparadas pelo sigilo, isso porque estão sendo realizadas em um ambiente virtual, logo, tornam-se de domínio coletivo.

No entanto, as conversas realizadas entre duas pessoas, de forma restrita, somente poderão ser acessadas pelos agentes estatais, precedendo-se de ordem judicial, sob pena de violar o direito à privacidade e intimidade dos interlocutores. (ALMEIDA, 2019)

Diante disso, percebe-se que há limites na obtenção de provas por meio de informações colhidas na internet, sendo que até a autorização judicial do juiz deve ser feita através da ponderação de princípios conflitantes, sob pena de invalidar as provas documentais obtidas nas redes.

III.V - Flagrante preparado e flagrante esperado

A infiltração virtual de agentes pode ir de encontro com o princípio da lealdade. Esse primado assegura que o Estado não utilizará de meios enganosos para a obtenção de provas, ou seja, será orientado pelo princípio da impessoalidade e da presunção de inocência do investigado, pois o dever do Estado não é criminalizar as pessoas.

Por esse motivo, a infiltração jamais poderá interferir na atuação do investigado, isto é, o policial infiltrado deve ser cuidadoso a fim de que não provoque ou instigue uma conduta delituosa por parte do investigado, pois, se assim o fizer, o flagrante e as provas obtidas serão considerados ilícitos.

Nesse sentido, segundo Mariana Fioravante (2021), o agente provocador será aquele que de alguma forma induz ou instiga o investigado a praticar um delito, com a finalidade de fazer a prisão em flagrante e obter provas. Entretanto, essa ação viola o direito fundamental de não se autoincriminar e o da ampla defesa e, por isso, é proibida pela legislação, acarretando a ilicitude do flagrante e da prova obtida.

Como pode-se observar na seguinte Ementa do Tribunal Regional Federal da 3ª Região (TRF-3), referente à Operação "*Darknet*", em que o Tribunal decidiu que não restou configurado o flagrante preparado, haja vista que o investigado não foi induzido:

> RECURSO EM SENTIDO ESTRITO. PORNOGRAFIA INFANTIL. ART. 241-A e ART. 241-B DA LEI Nº 8.069/90. RECEBIMENTO DA DENÚNCIA. OPERAÇÃO DARKNET. FLAGRANTE PREPARADO. AUSÊNCIA. NÃO CONFIGURAÇÃO DE CRIME IMPOSSÍVEL. RECURSO PROVIDO. [...] Após autorização judicial para infiltração de agentes e criação do fórum "Forpedo Brasil" na "DeepWeb", o acusado foi identificado como sendo um dos usuários que compartilhou material pedófilo no referido ambiente, o que culminou com o seu rastreamento e cumprimento de mandado de busca e apreensão em sua residência. **2. Ausência do flagrante preparado ou provocado, eis que nenhum dos usuários foi induzido a praticar crimes pelos policiais infiltrados. Não houve convite ou qualquer outra forma de instigação, nem se fez nascer a intenção da prática dos delitos. Houve, sim, a criação de um fórum onde havia uma espécie de cadastro prévio, etapa que permitia a identificação dos IP's dos usuários, ante a dificuldade de rastreamento ao se utilizar a "DeepWeb" através do programa TOR. Constatada atividade suspeita pelo usuário, com a publicação de material que denotasse a prática de crimes, o IP era rastreado e a investigação prosseguia com o objetivo de averiguar elementos de autoria e materialidade. Os crimes foram efetivamente consumados, com o compartilhamento de material de cunho pedófilo, para só após se dar o rastreamento e a identificação dos IP's. Os agentes policiais não fomentaram nem impediram a prática dos crimes, daí não se pode falar em crime impossível. A hipótese amolda-se ao que se entende pelo flagrante esperado, válido e aceito em nosso ordenamento jurídico.** [...] (TRF-3 - RSE: 00131528920144036181 SP, Relator: DESEMBARGADOR FEDERAL JOSÉ LUNARDELLI, Data de Julgamento: 11/12/2018, DÉCIMA PRIMEIRA TURMA, Data de Publicação: e-DJF3 Judicial 1 DATA:07/01/2019) (grifo nosso)

Como é visto, a infiltração policial realizada na operação supracitada não restou eivada de nenhum vício, tendo em vista que os policiais não induziram o suspeito a praticar os crimes contra a dignidade sexual infanto-juvenil, pelo contrário, o acusado disponibilizou material pornográfico de forma voluntária.

Dessa forma, é entendido que quando há ausência de vontade livre e espontânea do acusado faz com que o crime praticado seja considerado crime impossível, devido à ineficácia absoluta do meio empregado, disposto no art. 17, do CP, o qual tornará a conduta atípica. (ALMEIDA, 2019). Nesse sentido, destaca-se a Súmula nº 145 do Supremo Tribunal Federal, a qual dispõe que "Não há crime, quando a preparação do flagrante pela polícia torna impossível a sua consumação.".

Entretanto, a despeito de o flagrante provocado ser considerado ilícito, o flagrante esperado é admitido e, portanto, é necessário fazer essa comparação entre os dois institutos. Analisa-se o julgado do TRF-4, quanto à diferenciação entre flagrante preparado e flagrante esperado.

> [...] 7. **Não se verifica a ocorrência do flagrante preparado e tampouco ilicitude da prova, porquanto a atuação do agente da Polícia Federal como infiltrado no programa Gigatribe foi autorizado judicialmente e atendeu todas as recomendações e limites de investigação** no sentido de apenas obter registros sobre usuários do aplicativo que compartilhavam entre si, material de pedofilia-pornográfica no ambiente virtual. 8. No caso, os crimes já estavam sendo cometidos e o aguardo e a espera do fornecimento da senha, apenas foi para confirmar a atuação delitiva. E assim que tal foi realizado, permitiu-se com maior clareza e certeza flagrar que o usuário J. M. compartilhava material nefasto envolvendo crianças e adolescentes pelo aplicativo Gigatribe. **Trata-se, pois de flagrante esperado, já que a polícia tinha notícias de que infrações penais estavam sendo cometidas por inúmeros agentes pela aludida rede social fechada e aguardava o momento da consumação das condutas para de executar as devidas medidas constritivas penais** [...] (TRF4, ACR 5068165-51.2013.4.04.7100, SÉTIMA TURMA, Relatora SALISE MONTEIRO SANCHOTENE, juntado aos autos em 20/03/2019) (grifo nosso)

Assim, diferentemente do flagrante provocado, em que o agente induz o investigado à prática do ilícito, o flagrante esperado ocorre quando a polícia espera o melhor momento para capturar o acusado, isto é, o policial toma conhecimento prévio acerca de um crime que está sendo praticado ou irá se consumar e adota providências para prendê-lo em flagrante em um melhor momento. Não há, portanto, por parte do agente policial qualquer induzimento ou instigação, mas tão somente à espera do melhor momento para efetuar a prisão em flagrante. (MARCÃO, 2021)

Na infiltração virtual, o flagrante esperado pode ser realizado, por exemplo, em uma situação em que o policial infiltrado obtém materiais do investigado, como fotos e vídeos, por

meio virtual, e descobre que ele o armazena e, após a descoberta, a equipe efetua o flagrante após tomar as devidas providências. Nesse caso, o agente infiltrado somente cumpriu com a sua função de descobrir as condutas do investigado, sem induzir o investigado. Esse flagrante é legal, segundo a jurisprudência e a doutrina. (CABETTE, 2017).

Ingrid Silva (2017), citando Renato Brasileiro de Lima, ensina que o agente provocador dispõe de algumas características.

> Em síntese, como observa a doutrina, caracteriza-se, o agente provocador, pela presença dos seguintes elementos: a) efetiva incitação por parte do agente provocador determinando a vontade delituosa do indivíduo provocado (elemento objetivo); b) vontade de determinar a prática de um crime para possibilitar a punição de seu autor (elemento subjetivo); c) adoção de medidas de precaução para evitar que o crime provocado se consume. (LIMA, 2017, apoud SILVA, 2017, p. 42).

Diante do exposto, percebe-se que o agente infiltrado deve agir com cautela durante a operação, a fim de que não induza o investigado à prática delitiva, deixando que o investigado inicie os atos preparatórios e executórios espontaneamente, para que as provas obtidas na investigação sejam válidas para o processo penal.

Vale a pena, no entanto, destacar o entendimento de José Carlos Teixeira Costa Júnior (2018), que explica que tal escusa não poderá ser utilizada quando o crime se consumar antes da instigação. Isso ocorre, por exemplo, se o policial provocar o investigado a transmitir, oferecer, divulgar materiais pornográficos envolvendo criança ou adolescente (crime do art. 241-A), ainda assim será possível o flagrante pelo crime do 241-B, que se consuma pelo simples fato de possuir esse material, pois a posse iniciou-se antes e a despeito da instigação.

Nesse sentido, a fim de valorar as provas colhidas durante a infiltração, a autoridade judicial deverá analisar o contexto em que essas provas foram adquiridas, conforme ensina Ingrid Silva: “na valoração das provas, a autoridade judicial deve analisar em quais contextos as provas foram colhidas, a fim de que os prejuízos ocasionados pela ponderação dos princípios sejam menores que os benefícios.” (SILVA, 2017, p. 74)

CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo precípuo a análise da validade das provas colhidas durante o método de investigação conhecido como infiltração policial, nos crimes cometidos no ambiente cibernético. Para tanto, buscamos inicialmente trazer um estudo do que são os crimes virtuais e sua classificação, trazendo como possível solução de investigação, a infiltração policial virtual.

A partir dessa apresentação inicial, passamos à análise da técnica de investigação em si, tratando do seu conceito, de suas características, de seu funcionamento, finalidade. A partir desse estudo, percebemos que a infiltração virtual de agentes possui características de subsidiariedade e excepcionalidade, ou seja, são utilizadas somente utilizada em *ultima ratio*, isto é, como último recurso.

Dessa forma, percebemos que essa investigação é bastante invasiva e afronta alguns direitos fundamentais do acusado, em especial os direitos à privacidade, intimidade e o direito à não autoincriminação. Entretanto, apesar de muita discussão acerca da ilegitimidade dessa técnica de investigação, foi visto que a criminalidade virtual está cada vez mais forte e evoluída, gerando a necessidade de ações efetivas por parte do Estado para o seu combate.

Diante disso, a legislação brasileira, dispôs expressamente a possibilidade de infiltração de agentes virtuais para a obtenção de provas no combate a determinados crimes, legitimando a atuação dos policiais, ainda que relativizando direitos fundamentais dos investigados.

Entretanto, concluímos esse estudo, considerando ser legítima e necessária a infiltração policial virtual para a investigação de determinados crimes, principalmente porque o ambiente cibernético além de afetar bens jurídicos deveras caros para a sociedade, como por exemplo, a dignidade sexual de crianças e adolescentes, possui mecanismos que dificultam a investigação nesses espaços, como por exemplo a utilização de criptografia, sensação de impunidade e anonimato.

Nesse sentido, entendemos que a infiltração deve ser realizada e as provas colhidas através dela serão válidas. No entanto, deve-se seguir as normas, a fim de não tornar a medida, e consequentemente as provas, ilícitas. Para tanto, a infiltração deve ser baseada na proporcionalidade, isto é, tendo em vista que os direitos do investigado serão relativizados, deve haver uma ponderação de direitos para não prejudicar a investigação.

Dessa forma, inicialmente a infiltração deve ser utilizada somente quando não houver outro meio menos invasivo para a obtenção das provas, devendo obrigatoriamente ser precedida de autorização judicial, ter indícios veementes de materialidade, individualizar os sujeitos

investigados (ainda que por um perfil ou *nickname*), ter prazo determinado, documentar tudo que for realizado durante o procedimento e, principalmente, não induzir ou instigar o investigado a praticar crimes, isto é, atuar de forma cuidadosa para não interferir na vontade do investigado, pois, se assim o fizer, o flagrante e as provas colhidas serão consideradas ilícitas.

Cabe ressaltar que a infiltração policial no ambiente digital é, de certa forma, nova no ordenamento jurídico brasileiro. Isso porque, foi introduzida expressamente pela primeira vez no ano de 2017, possibilitando a utilização dessa técnica somente para crimes específicos contra a dignidade sexual de crianças e adolescentes. Após, em 2019, passou-se a prever a infiltração virtual também na Lei de Organizações Criminosas. Dessa forma, ainda é cedo para avaliar se é uma técnica efetiva no combate aos crimes cibernéticos, porém, é um método de investigação que está sendo bastante utilizado frente à criminalidade cibernética e, como vimos pelas jurisprudências apresentadas, seguindo as regras estabelecidas pela lei, as provas serão válidas no processo penal e consequentemente, a infiltração terá sido efetiva.

REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA IBGE NOTÍCIAS. **PNAD Contínua TIC 2018: Internet chega a 79,1% dos domicílios do país.** 2020. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/27515-pnad-continua-tic-2018-internet-chega-a-79-1-dos-domicilios-do-pais. Acesso em: 12 mar. 2021.

ALMEIDA, Kesller Cristina Silva de. **Infiltração policial no âmbito virtual como meio extraordinário de investigação criminal**, 2019. Monografia (Bacharel em Direito) - Universidade Federal do Paraná. Curitiba, 2019. Disponível em: https://acervodigital.ufpr.br/bitstream/handle/1884/68068/Monografia%20-%20Kesller%20Cristina%20Silva%20de%20Almeida%20%282019%29.pdf?sequence=1&isAllowed=y. Acesso em 15 mar. 2021.

ALMEIDA, Washington Almeida. **Deep Web, Dark Web… o lado oculto da internet**. Gran Cursos Online, 2020. Disponível em: https://blog.grancursosonline.com.br/deep-web-dark-web-o-lado-oculto-da-internet/. Acesso em: 14 jun. 2021.

BRAGA, Diego Campos Salgado. **Métodos de investigações no âmbito cibernético**, 2019. Artigo. Disponível em: https://jus.com.br/artigos/71463/metodos-de-investigacoes-no-ambito-cibernetico . Acesso em: 01 jun. 2021.

BRASIL. Constituição (1988). Constituição: República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso: 16 jun. 2021.

_____. Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 20 mar. 2021.

_____. Código Penal Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 20 mar. 2021.

_____. Lei 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, DF, 13 jul. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em 12 mar. 2021.

_____. Lei nº 11.343, de 23 de agosto de 2006. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm> Acesso em: 08 maio 2017.

_____. Lei 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei 9.034, de 3 de maio de 1995; e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, DF, 2 ago. 2013. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em 15 abr. 2021.

_____. Lei 13.260, de 16 de março de 2016. Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis n º 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. Diário Oficial da República Federativa do Brasil, Brasília, DF, 16 mar. 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em 12 mar. 2021.

_____. Lei 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Diário Oficial da República Federativa do Brasil, Brasília, DF, 24 dez. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em 12 mar. 2021.

_____. (1963). Súmula nº 145. Supremo Tribunal Federal. Disponível em: http://www.stf.jus.br/portal/jurisprudencia/menuSumarioSumulas.asp?sumula=2119

_____. (2019). Acórdão. Recurso em Sentido Estrito n. 00131528920144036181 SP. 07 de janeiro de 2019. 11ª Turma do TRF da 3ª Região. Recebimento da Denúncia: não configuração de crime impossível. Diário Eletrônico nº 04 (Publicações Judiciais I – TRF). Disponível em: http://web.trf3.jus.br/diario/Consulta/PublicacoesAnteriores/2019-01-01

CABETTE, Eduardo Luiz Santos. **Infiltração Virtual: alguns breves apontamentos**, 2017. Artigo. Conteúdo Jurídico, 2017. Disponível em: http://www.conteudojuridico.com.br/coluna/2626/infiltracao-virtual-alguns-breves-apontamentos. Acesso em: 02 set 2021.

CAETANO, Aldo Maxwell Pereira de Mesquita. **Crimes virtuais: aplicação, falibilidade e impunidade,** 2015. Monografia (Bacharel em Direito) - Universidade Tiradentes - UNIT. Aracajú, 2015. Disponível em: https://openrit.grupotiradentes.com/xmlui/bitstream/handle/set/1195/TCC%20-%20Crimes%20Virtuais.pdf?sequence=1. Acesso em: 26 maio 2021.

CARDOSO, Lucas de Holanda M**. O Direito na Era Digital: O Cibercrime no Ordenamento Jurídico Brasileiro**, 2017. Artigo Científico. Disponível em: https://cepein.femanet.com.br/BDigital/arqPics/1611400792P734.pdf

CASTRO, Henrique Hoffmann Monteiro de**.** Lei 13.441/17 instituiu a infiltração policial virtual. **Consultório Jurídico**, 2017. Disponível em: https://www.conjur.com.br/2017-mai-16/academia-policia-lei-1344117-instituiu-infiltracao-policial-virtual#:~:text=2017.,t%C3%A9cnicas%20especiais%20de%20investiga%C3%A7%C3%A3o%20criminal.&text=Infiltra%C3%A7%C3%A3o%20policial%20na%20internet%20da,ser%20usada%20para%20outros%20crimes%3F. Acesso em: 27 maio 2021.

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. 2017, **Dizer o Direito**. Disponível em: https://www.dizerodireito.com.br/2017/05/comentarios-infiltracao-de-agentesde.html Acesso em: 19 maio 2021

CUNHA, Rogério Sanches; PINTO, Ronaldo Batista. Infiltração de agentes de polícia na internet. **Migalhas,** 2017. Disponível em: https://www.migalhas.com.br/depeso/258738/infiltracao-de-agentes-de-policia-na-internet Acesso em: 19 maio 2021.

Dicas de como se proteger contra crimes cibernéticos. **Kaspersky**. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 27 maio 2021.

FIORAVANTE, Mariana. Tudo o que você precisa saber sobre a infiltração de agente policial, **Gran Cursos Online**, 2021. Disponível em: https://blog.grancursosonline.com.br/tudo-o-que-voce-precisa-saber-sobre-a-infiltracao-de-agente-policial/#_ftnrefl. Acesso em: 15 jun. 2021.

FORTUNA, Deborah. Crimes de ódio: o que são, por que ocorrem e como combatê-los. **Correio Braziliense**, 2019. Disponível em: https://www.correiobraziliense.com.br/app/noticia/brasil/2019/09/21/interna-brasil,783574/crimes-de-odio-o-que-sao-por-que-ocorrem-e-como-combate-los.shtml. Acesso em: 10 jun. 2021.

Física e Matemática ajudam a Polícia Federal resolver crimes da internet. **Dom Total**, 2020. Disponível em: https://domtotal.com/noticia/1415954/2020/01/fisica-e-matematica-ajudam-a-policia-federal-resolver-crimes-da-internet/ Acesso em: 25 maio 2021.

GONDIM, Abnor. MP do DF estima que crimes cibernéticos causem danos de R$ 80 BI ao ano. **Tele Síntese**, 2019. Disponível em: https://www.telesintese.com.br/mp-do-df-estima-que-crimes-ciberneticos-causem-danos-de-r-80-bi-ao-ano/ Acesso em: 25 maio 2021.

GUERRA, Gustavo Gabriel Alves. **Infiltração Virtual dos Agentes Policiais: como meio de investigação de prova na persecução penal**, 2019. Monografia (Bacharel em Direito) - Universidade Evangélica. Anápolis, 2019. Disponível em: http://repositorio.aee.edu.br/bitstream/aee/8621/1/TCC%20VERS%C3%83O%20FINAL%20-%20Gustavo%20principal%5B1258%5D.pdf.

JUNIOR, José Carlos Teixeira Costa. **Limites da Infiltração Policial na Internet e a Invasão de Dispositivo Informático: O Advento da Lei 13.441/2017,** 2018. Monografia (Bacharel em Direito) - Faculdade de Direito, da Universidade Federal da Bahia. Salvador, 2018. Disponível em: https://repositorio.ufba.br/ri/handle/ri/26249.

JÚNIOR, Júlio César Alexandre. **Cibercrime: um estudo acerca do conceito de crimes informáticos**. Revista Eletrônica da Faculdade de Direito de Franca, 2019. ISSUE DOI: 10.21207/1983.4225.602. Disponível em: https://www.revista.direitofranca.br/index.php/refdf/article/view/602/pdf.

LUCENA, Laís Freitas Franca. **A Infiltração Policial em Organizações Criminosas: Limites de Atuação do Agente Infiltrado**, 2019. Trabalho de Conclusão de Curso (Bacharel em Direito) - Universidade Federal da Paraíba – UFPB, 2019. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/14268/1/LFFL10052019.pdf

MANN, Diana Calazans. **Infiltração Digital: a validade como meio de prova e os limites éticos do estado-investigador**. Dissertação (Mestrado). 2018. Instituto Superior de Ciências Policiais e Segurança Interna - ISCPSI, Lisboa. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/25245/1/Disserta%C3%A7%C3%A3o_Infiltra%C3%A7%C3%A3o_Digital_Diana%20Mann.pdf

MARCÃO, Renato. **Curso de processo penal**. 7. ed. – São Paulo: Saraiva Educação, 2021.

MENDRONI, Marcelo Batlouni. **Crime organizado: aspectos gerais e mecanismos legais**. 7. ed. São Paulo: Atlas, 2020.

NETO, Pedro Américo de Souza. **Crimes de Informática,** 2009. Monografia (Bacharel em Direito) - Universidade do Vale do Itajaí - UNIVALI. 2009. Disponível em: http://siaibib01.univali.br/pdf/Pedro%20Americo%20de%20Souza%20Neto.pdf Acesso em: 20 mar. 2021.

NUCCI, Guilherme de Souza. **Organização Criminosa**. 5. ed. Rio de Janeiro: Forense, 2021.

OLIVEIRA, Franco Henrique; KOZAN Mariana Batista. A figura do agente infiltrado virtual e a relativização de direitos fundamentais: dignidade sexual de crianças e adolescentes. **Revista GESTO: Revista de Gestão Estratégica de Organizações**, Santo Ângelo, v.7, n.1, p. 86-101, jan./jun. 2019 .

PEREIRA, Flávio Cardoso. Agente infiltrado virtual: primeiras impressões da Lei 13.441/2017. **Revista do Ministério Público de Goiás**. Goiânia, p. 97-117, 2017. Disponível em: http://www.mp.go.gov.br/revista/pdfs_12/8-ArtigoFlavio_Layout%201.pdf Acesso em: 10 maio 2021.

PEREIRA, Flávio Cardoso. **Agente Encubierto y Proceso Penal Garantista: Límites y Desafíos,** 2012. Facultad de Derecho. Universidad de Salamanca, Salamanca. Disponível em: https://gredos.usal.es/bitstream/handle/10366/121134/DDAFP_CardosoFlavio_Tesis.pdf;jsessionid=B937B33205CA6B887006BA0364F69A0C?sequence=1 Acesso em: 2 maio 2021.

PIRES, Luiza Matias. **A Infiltração Policial Virtual nos Crimes contra a Dignidade Sexual da Criança e do Adolescente: análise da infiltração sob a ótica da Lei 13.441/17**, 2018. Monografia (Bacharel em Direito) - Faculdade de Direito de Presidente Prudente/SP, 2018. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/Direito/article/view/7449. Acesso em: 2 mar. 2021.

RODRIGUES, Felipe José Sousa; CARDOSO, Sarah de Araújo Mendes; MARWELL, Tatiana Eulálio Dantas Guedes. **Utilização da infiltração virtual nas operações policiais para o combate aos crimes sexuais contra crianças e adolescentes**. Research, Society and Development, v. 10, n. 7, e24710414152, 2021 (CC BY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v10i4.14152, 2021. Acesso em: 18 jun. 2021.

RUSSO**,** Gerson de Souza; NEGRÃO, Armando de Souza. Organização criminosa e os crimes da era digital. In: **Boletim Jurídico**, 2020. Disponível em: http://boletimjuridico.publicacoesonline.com.br/85336/. Acesso em: 16 jun. 2021.

SANNINI NETO, Francisco. Infiltração virtual de agentes é um avanço nas técnicas especiais de investigação criminal. In: **Canal Ciências Criminais**, mai. 2017. Disponível em: https://canalcienciascriminais.com.br/infiltracao-virtual-agentes. Acesso em: 13 maio 2021.

SCHMIDT, Guilherme. **Crimes Cibernéticos**. 2015. Disponível em: http://www.schmidtadvogados.com/portfolio-view/crimes-ciberneticos/. Acesso em: 16 mar. 2021.

SILVA, Ingryd Martins. **A Infiltração Policial como Técnica Especial de Investigação no Ambiente Cibernético**, 2017. Trabalho de Conclusão de Curso (Bacharel em Direito) - Universidade Federal Fluminense, Macaé, 2017. Disponível em: https://egov.ufsc.br/portal/conteudo/infiltra%C3%A7%C3%A3o-policial-como-t%C3%A9cnica-especial-de-investiga%C3%A7%C3%A3o-no-ambiente-cibern%C3%A9tico. Acesso em: 2 mar. 2021.

SIMAS, Diana Viveiros de. **O cibercrime**. 2014. 168f. Dissertação (Mestrado em Ciências Jurídico Forenses). Universidade Lusófona de Humanidades e Tecnologias. Lisboa. 2014. Disponível em: https://egov.ufsc.br/portal/sites/default/files/tese_cibercrime.pdf. Acesso em: 14 abr. 2021.

ZANELLA, Everton Luiz. **Infiltração de agentes**. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Processo Penal. Marco Antonio Marques da Silva (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/442/edicao-1/infiltracao-de-agentes#:~:text=A%20infiltra%C3%A7%C3%A3o%20de%20agentes%20%C3%A9,provas%20acerca%20de%20sua%20estrutura%2C. Acesso em: 2 maio 2021.