BIANCA LORENA SILVA

INFILTRAÇÃO VIRTUAL DOS AGENTES POLICIAIS COMO MEIO DE OBTENÇÃO DE PROVAS A PERSECUÇÃO PENAL.

CURSO DE DIREITO- UniEVANGÉLICA

2023

BIANCA LORENA SILVA

INFILTRAÇÃO VIRTUAL DOS AGENTES POLICIAIS COMO MEIO DE OBTENÇÃO DE PROVAS A PERSECUÇÃO PENAL.

Monografia apresentada ao Núcleo de Trabalho Cientifico do curso de Direito da UniEVANGÉLICA, como exigência parcial para a obtenção de grau de bacharel em Direito, sob orientação do professor (a) Me. José Rodrigues Ferreira Junior.

ANÁPOLIS-2023

BIANCA LORENA SILVA

INFILTRAÇÃO VIRTUAL DOS AGENTES POLICIAIS COMO MEIO DE OBTENÇÃO DE PROVAS A PERSECUÇÃO PENAL.

Anápolis, ...de.....2023.

BANCA EXAMINADORA

_____

_____

AGRADECIMENTOS

Aos queridos orientadores da minha monografia, minha gratidão é imensa. Vocês foram fundamentais nessa jornada acadêmica, guiando-me com paciência, conhecimento e dedicação. Agradeço pela orientação precisa, pelos valiosos insights e pela confiança depositada em meu trabalho. Sem o apoio de vocês, não teria alcançado esse importante marco em minha vida.

Gostaria de estender meus agradecimentos à minha mãe, que sempre esteve ao meu lado, apoiando-me incondicionalmente. Seu amor, carinho e incentivo foram o alicerce que me impulsionou nos momentos de desafio. Sua presença constante e suas palavras de encorajamento foram a motivação necessária para não desistir. Sou grata por ter você como minha maior fã e exemplo de perseverança.

Também gostaria de expressar minha gratidão ao meu pai, que infelizmente não está mais entre nós. Sua memória e ensinamentos permanecem vivos em meu coração. Sei que ele teria se orgulhado dos meus esforços acadêmicos e teria sido um grande apoiador nesta jornada. Seu legado continua a me inspirar a buscar o melhor de mim em cada desafio que enfrento.

Aos coordenadores e supervisores do NTC da UniEVANGÉLICA de Goiás, minha gratidão por proporcionarem um ambiente acadêmico rico em conhecimento e aprendizado. Agradeço por investirem em minha formação, pela estrutura oferecida e pelo apoio constante ao longo do curso. Cada um de vocês desempenhou um papel significativo na minha jornada, moldando-me como estudante e profissional em formação.

Sei que palavras não são suficientes para expressar toda a gratidão que sinto por cada um de vocês. Vocês foram mais do que orientadores, coordenadores e supervisores, tornaram-se verdadeiros mentores em minha vida. Acreditem que cada conselho, cada correção e cada incentivo foram eternizados em minha jornada acadêmica e profissional.

Que o reconhecimento e a gratidão aqui expressos sejam um reflexo do meu compromisso em honrar tudo o que aprendi com vocês. Espero poder compartilhar meus conhecimentos e experiências com outros, assim como vocês fizeram comigo.

Mais uma vez, meu sincero obrigado a todos que contribuíram de alguma forma para o meu crescimento e sucesso na minha monografia e na minha formação como um todo. Sou grata por ter vocês em minha vida.

RESUMO

A monografia aborda o tema da infiltração virtual dos agentes policiais como um meio de obtenção de provas na persecução penal. O trabalho está dividido em três capítulos, cada um tratando de diferentes aspectos relacionados ao tema. No Capítulo I, é discutido o surgimento dos crimes cibernéticos, destacando o aumento da criminalidade virtual e os desafios enfrentados pelas autoridades policiais nesse contexto. Além disso, é analisada a legislação pertinente, especialmente aquela relacionada aos crimes cibernéticos e às formas de investigação virtual. Também são abordadas as provas obtidas por meio da infiltração do agente policial, considerando sua relevância e admissibilidade no processo penal. No Capítulo II, é apresentada a teoria dos despenalizadoras e a proteção penal. São discutidos os conceitos relacionados a esse tema e o panorama jurídico que envolve a despenalização de certos crimes. É examinado o papel do Estado como parte no processo penal e como isso se relaciona com a infiltração virtual dos agentes policiais. No Capítulo III, é discutida a posição jurídica e o tratamento legal penal da infiltração virtual dos agentes policiais. São apresentados aspectos gerais sobre o tema, incluindo os requisitos necessários para a realização da infiltração e o posicionamento doutrinário a respeito. Além disso, é analisada a posição do Tribunal Superior, especialmente o Superior Tribunal de Justiça (STJ), sobre a matéria. A monografia oferece uma análise completa e abrangente sobre a infiltração virtual dos agentes policiais como meio de obtenção de provas na persecução penal. Os diferentes capítulos exploram o surgimento dos crimes cibernéticos, a legislação aplicável, a admissibilidade das provas obtidas, a teoria dos despenalizadoras, o papel do Estado e os aspectos jurídicos relacionados à infiltração virtual. O trabalho contribui para o entendimento e a discussão desse tema relevante no contexto da segurança digital e da justiça criminal.

Palavras-chave: infiltração virtual, agentes policiais, obtenção de provas, persecução penal, crimes.

SUMÁRIO

INTRODUÇÃO

A crescente utilização da internet e o avanço da tecnologia resultaram em uma nova categoria de crimes conhecidos como crimes cibernéticos. Diante desse cenário, a investigação e a persecução penal enfrentam desafios inéditos, exigindo adaptações e abordagens eficazes para combater essa modalidade criminosa. Nesse contexto, a infiltração virtual dos agentes policiais emerge como uma ferramenta essencial para obtenção de provas e efetiva persecução penal.

A monografia se divide em três capítulos que abordam distintos aspectos relacionados à infiltração virtual dos agentes policiais. O Capítulo I explora o surgimento dessa técnica investigativa no contexto dos crimes cibernéticos, analisando a evolução desses delitos, seu impacto na sociedade e a necessidade de atualização legislativa.

No Capítulo II, é apresentada a teoria dos despenalizadoras e a proteção penal. O conceito desses termos é analisado, com destaque para o panorama jurídico em relação aos crimes na condição jurídica despenalizada. O papel do Estado no processo penal é explorado, abordando-se a necessidade de adoção de medidas eficazes para garantir a proteção dos direitos fundamentais dos cidadãos sem comprometer a persecução penal.

Já o Capítulo III concentra-se na posição jurídica e no tratamento legal penal da infiltração virtual dos agentes policiais. Aspectos gerais desse método de investigação são discutidos, assim como os requisitos necessários para sua utilização. Além disso, são apresentadas diferentes visões doutrinárias acerca dessa prática, explorando sua legalidade e eficácia na obtenção de provas. O posicionamento do

Tribunal Superior, com ênfase nas decisões proferidas pelo Superior Tribunal de Justiça (STJ) em relação à infiltração virtual dos agentes policiais, também é abordado.

A partir desses três capítulos, a monografia busca realizar uma análise aprofundada da infiltração virtual dos agentes policiais como meio de obtenção de provas na persecução penal. O objetivo é contribuir para o debate acerca da eficácia dessa técnica investigativa, levando em consideração a proteção dos direitos individuais e os desafios enfrentados pelas autoridades policiais na era digital.

CAPÍTULO I – INFILTRAÇÃO VIRTUAL DOS AGENTES POLICIAIS

O presente capítulo trata detalhadamente da aplicação da Infiltração virtual dos agentes policiais, ela que é uma modalidade que visa na proteção de dados pessoais e também auxilia na obtenção de provas de crimes cinéticos contra o estupro de vulnerável, corrupção de menores, satisfação de lascívia mediante presença de crianças e adolescentes.

No contexto é apresentado o conceito, o surgimento dos crimes cibernéticos, legislações, meio de obtenção de provas e a infiltração do agente, assim levando ao entendimento desde projeto a aplicabilidade na vida real.

1.1 Surgimento dos crimes cibernéticos

A partir de 1980, as ações criminosas intensificaram-se, envolvendo principalmente manipulação de dados bancários, pirataria de programas de computador, abusos nas telecomunicações e pornografia infantil.

Essa modalidade de delito começou a ganhar destaque no ordenamento jurídico brasileiro a partir da lei 12.737 de 2012, popularmente denominada lei Carolina Dieckmann

O crescimento acelerado das tecnologias de informação, com novas plataformas sendo lançadas diariamente, traz com sigo uma abertura muito grande para que a criminalidade se encontra e toma forças nestes ambientes fardo para as práticas delitivas. Há que se ressaltar que a internet se tornou um espaço onde seu usuário expõe sua vida, se tornando cada vez mais exposto (ROSSINI, 2002).

A internet surgiu no contexto da Guerra Fria, sendo consequência de um projeto ambicioso norte-americano, com o objetivo de proteger e dar celeridade às trocas de informações, visto que, em caso de ataques nucleares, uma efetiva comunicação seria imprescindível para o sucesso americano. A evolução no campo da informática fez com que as distâncias diminuíssem, facilitando e acelerando a troca de informações. (ROSSINI, 2002).

Em contrapartida, a criminalidade encontrou neste fato um ambiente propício para o seu crescimento, haja vista que, encobertos pelo possível anonimato e pela velocidade das comunicações, seus atos seriam dificilmente reprimidos. (SILVA,2017).

Em 2017, aconteceu uma convenção sobre o cibe crime, sendo o único tratado internacional acerca dos crimes cibernéticos, com cinquenta e quatro países que o ratificaram e quatro que apenas o assinaram, o Brasil ainda não aderiu à Convenção, sob o argumento da necessidade de convite para aderi-la, na forma do seu artigo 37, e, também, que os termos da Convenção ainda se encontram em análise à luz do ordenamento jurídico brasileiro. (BOITEUX,2013)

Os principais objetivos da Convenção de Budapeste sobre cibe crimes estão expostos em seu preâmbulo:

> Convictos de que a presente Convenção é necessária para impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adopção de poderes suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável.(BOITEUX, 2013, p.102)

Assim é importante ressaltar que a internet foi criada com intuito de facilitar e expandir a comunicação, suprindo assim a necessidade das pessoas na rapidez e na praticidade. O mundo virtual serve também como meio de entretenimento, ultrapassando os limites do computador e chegando ao celular incentivando o comercio virtual. (SILVA, 2017)

1.2 Legislação, Infiltração Virtual

A lei nº 12.737/12, de 30 de novembro de 2012, intitulada Carolina Dickman, trouxe alterações no Código Penal vigente, acrescentando os artigos 154-A e 154-B, assim, originou-se o tipo penal “Invasão de dispositivo informático” É possível destacar como crimes cibernéticos aqueles que compreendem o envio de vírus, programas e também códigos que sejam maliciosos ao destinatário. Fora isso, também é crime o furto de dados bancários e de comércios eletrônicos, ou seja, informações sigilosas, em nítida invasão de privacidade. (NERY,2016)

A figura do agente infiltrado virtual, introduzida ao ordenamento brasileiro por força da Lei n. 13.441/17, veio suprir lacuna no tocante ao enfrentamento da criminalidade cibernética, especialmente em se tratando de crimes contra a dignidade sexual de pessoas menores de idade. Referido meio de obtenção de prova, se empregado com fulcro e obediência aos princípios de legalidade, proporcionalidade e última ratio, por certo apresentará resultados eficazes na luta contra essa espécie grave de delinquência. (NERY,2016)

Lei nº 13.441/2017 consiste em técnica especial e subsidiária de investigação, qualificada pela atuação dissimulada (com ocultação da real identidade) e sigilosa de agente policial, seja presencial ou virtualmente, em face de um criminoso ou grupo de criminosos, com o fim de localizar fontes de prova, identificar criminosos e obter elementos de convicção para elucidar o delito e desarticular associação ou organização criminosa, auxiliando também na prevenção de ilícitos penais. A infiltração policial é gênero do qual são espécies a presencial (física) e a virtual (cibernética ou eletrônica). (HOFFMANN, 2017, p.1)

Importante ressaltar que o procedimento mais detalhado de infiltração de agentes previsto na Lei n. 12.850/13 pode e deve ser utilizado para complementar a previsão legal da infiltração virtual de agentes.

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

> de conexão ou cadastrais que permitam a identificação dessas pessoas. (BRASIL, 2022. Online)

Assim a infiltração virtual prevista na Lei n. 13.441/17 poderá ser operacionalizada para o enfrentamento a crimes graves, a exemplo dos crimes de invasão de dispositivo informático, estupro de vulnerável, corrupção de menores, satisfação de lascívia, mediante presença de criança ou adolescente e favorecimento da prostituição ou de outra forma de exploração sexual de criança ou adolescente ou de vulnerável. (BRASIL, 2022)

Portanto, Carlos e Friede (2014), diz que para o agente ter acesso sem está fora dos parâmetros legais, ao representar, o delegado de polícia terá de demonstrar a viabilidade da infiltração policial, já na hipótese de requerimento do Ministério Público no curso do inquérito, haverá de ter prévia manifestação da autoridade policial, tendo em vista que é ele quem irá conduzir a infiltração de agentes.

1.3 Provas

Os crimes cibernéticos no Brasil se difundiram e avançaram de maneira meteórica, e são feitos de diversas maneiras, desde um “simples” Cyberbullying, até um roubo de dados e identidade, conforme a tecnologia avançou e se difundiu o acesso à rede mundial de computadores, de igual modo se difundiu os cybers crimes. Uma prova documental importante que tem sido admitida é a ata notarial, com registro em cartório pelo qual esse instrumento público serve para pré-constituir prova de fatos como o conteúdo divulgado em páginas da Internet ou do conteúdo de mensagem, bem como o IP de origem. (NERY,2016)

Os meios de obtenção de provas para se dá a persecução penal são de diversas maneiras no âmbito da infiltração do agente virtual. Uma das formas mais usadas hoje no ordenamento jurídico para deslumbrar e comprovar os crimes cibernéticos é a intercepção telefônica. A lei 9.296 de 24 de julho de 1996, regulamento qual é a forma que se deve ser usada este mecanismo, assim se deve fazer conforme a lei determina, podendo haver o risco de se torna provas ilegais no processo e sendo retida do processo caso não seja seguido ela corretamente. (BRASIL, 2022).

> Lei 9.996/1996, parágrafo 01° A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal

> e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática. (BRASIL,1996, Online).

O outro meio é a perícia técnica, sua atuação é para a descoberta da origem dos fatos, como por exemplo qual foi a máquina (computador) ou telefone que praticou o fato delituoso, bem como a identificação do endereço de IP. De acordo com o autor (PECK, em um artigo de sua autoria em 2016, p. 16), diz que este meio de obtenção de prova para os crimes cibernéticos é muito eficaz e solida, pois, a maioria dos computadores são conectados em locais e redes públicas, assim conseguindo identificar o autor com mais precisão e rapidez (NERY,2016)

Assim, ainda que estejam tecnologicamente atualizados, segundo Corrêa os operadores devem sempre se lembrar que:

> Os operadores jurídicos deverão utilizar o bom senso para dirimir questões jurídicas relacionadas à Internet, procurando sempre relacionar a parte técnica com o ordenamento jurídico em exercício. São as análises simples e lógicas que possibilitarão um eficaz entendimento das questões cotidianas de nossos tribunais, sendo, principalmente, os bancos acadêmicos os futuros responsáveis pela construção deste, já que é neles que existe uma verdadeira interdisciplinaridade, essencial para a resolução dessas novas questões. (CORRÊA, 2000, p.107)

As redes sócias pode ser outro meio de obtenção de provas para os agentes infiltrados virtualmente, por ser uma vertente que constantemente está crescendo. Hoje em dia vem se tornando um meio onde os criminosos utilizam da sua vulnerabilidade para cometer atos antijurídicos por ser um objeto onde os usuários trocam constantemente informações; dados; assim se expondo, e favorecendo para que os criminosos cometam atos ilegítimos. (CORRÊA, 2000, p.108)

Os mais atingidos são crianças por terem menor entendimento e maior abertura para contatos virtuais, facilitando eventuais crimes que possam ocorrer.

Portanto, o autor PACELLI 2017 em seu artigo fala que a prova judiciária tem o objetivo claramente definido: a reconstrução dos fatos investigados no processo, buscando a maior coincidência possível com a realidade histórica, isto é,

com a verdade dos fatos, tal como efetivamente ocorrido no espaço e no tempo. A tarefa, portanto, é das mais difíceis, quando não impossível: a reconstrução da verdade. (2017, p.174)

1.4 Infiltração do agente

A infiltração poderá ocorrer física ou virtualmente, partindo da representação do delegado de polícia como diligência da fase investigatória, ou da fase judicial conforme; também podendo ser requerida pelo juiz, ouvido o Ministério Público, ou a pedido do próprio como instituição. A infiltração cibernética. Segundo as lições de NUCCI (2016), pode-se afirmar que a infiltração de agentes: representa uma penetração, em algum lugar ou coisa, de maneira lenta, pouco a pouco, correndo pelos seus meandros.

A infiltração consiste em introduzir um agente devidamente autorizado judicialmente e treinado na organização criminosa com intuído de colher provas e desvendar a estrutura e seus participantes. Assim, são regulamentados pela Lei n°12.850 de 2013, que dispõe sobre os direitos, no art. 14, diz que:

> Art. 14. São direitos do agente:
> I - Recusar ou fazer cessar a atuação infiltrada;
> II - Ter sua identidade alterada, aplicando-se, no que couber, o disposto no art. 9º da Lei nº 9.807, de 13 de julho de 1999, bem como usufruir das medidas de proteção a testemunhas;
> III - ter seu nome, sua qualificação, sua imagem, sua voz e demais informações pessoais preservadas durante a investigação e o processo criminal, salvo se houver decisão judicial em contrário;
> IV - Não ter sua identidade revelada, nem ser fotografado ou filmado pelos meios de comunicação, sem sua prévia autorização por escrito. (BRASIL, 2022, *online*).

Com base nessas disposições podemos ver como é a forma de atuação dos agentes infiltrados, o inciso I trata-se de uma natureza administrativo, onde dá a oportunidade do agente aceitar ou não a ordem do seu superior sem que tenha nem um tipo de punição caso ele não aceite.

Nos incisos II e III, refere-se que o agente infiltrado terá sua identidade alterada em circunstância da infiltração, o que preservara todas suas informações pessoais, isso também se estende ao seu cônjuge, ascendentes e descendes que dependam do infiltrado.

> A falsa identidade a ser fornecida ao agente infiltrado, neste aspecto, envolve, num primeiro momento, a elaboração de documentos falsos

> (carteira de identidade, passaporte, CNH, CPF, etc.). A necessária inserção de dados falsos nos respectivos sistemas de banco de dados da administração pública, sob pena de se comprometer a operação de infiltração policial. (NUCCI, 2016)

O infiltrado deverá se manter em extrema dissimulação para garantir sua segurança e até mesmo sua sobrevivência, pois estará convivendo com pessoas de extrema periculosidade, mas uma das vantagens da infiltração é justamente o contato direto do agente com a organização para a sua desarticulação. (NUCCI 2016)

Nesse sentido, Carlos e Friede corrobora ao elucidar que:

> A infiltração policial, enquanto meio de prova (art. 3°, VII, da Lei n° 12.850/13), caracteriza-se por sua própria complexidade jurídico operacional, considerando, ainda, tratar-se de uma técnica especial de 38 investigação através da qual um agente policial, devidamente selecionado e treinado para a tarefa, ocultando a verdadeira identidade, e utilizando outra a ser fornecida pelo estado, é introduzido no âmbito de uma organização criminosa e, conquistada a confiança dos verdadeiros membros, passa a atuar com o fim de obter provas a respeito das atividades delituosas praticadas, objetivando, com isso, desmantelá-la.(NUCCI, 2016, p.265)

Carlos e Friede (2014) falam também que após desmantelá-la deve acontecer a Identificação e prisão dos criminosos, inclusive de eventuais agentes públicos participantes do esquema delituoso, Identificação das fontes de renda da máquina criminosa, identificação de eventuais pessoas jurídicas utilizadas para encobrir atividades delituosas perpetradas pela organização, Identificação da estrutura estabelecida para proceder à lavagem de capital, Identificação (posterior apreensão) dos bens provenientes, direta ou indiretamente, da prática dos delitos cometidos pela organização. Recuperação de eventuais bens públicos desviados pela organização criminosa, dentre outros aspectos.

Assim entendemos que para um agente ser configurado como infiltrado ele deverá obter ou realizar estas atividades acima descritas e como também já observado até o momento, a infiltração de agentes é uma técnica de obtenção de provas.

Para a professora Luciana Boiteux:

> A infiltração é, procedimentalmente, um conjunto de atos probatórios ou, em outras palavras, um procedimento probatório... se quisermos buscar a categoria jurídica mais ampla a que pertence no direito

> processual penal, a infiltração é ato ou conjunto de atos jurídicos processuais penais (no sentido de atos jurídicos do direito processual penal, e não de ato processual no processo penal jurisdicional). (2010, p.60)

Portanto, em defesa de seu entendimento e contra-atacando a argumentação do professor Marcos Aurélio, explica que “tendo em vista sua ‘natureza jurídica’ de prova, não vemos por que considerar a infiltração como medida cautelar, que é categoria jurídica diversa”. (LIMA,2013, p.15)

O tempo de duração dessa infiltração virtual será de até seis meses, sem prejuízo de eventuais renovações, mediante ordem judicial fundamentada e desde que o total não exceda a 720 (setecentos e vinte) dias e seja comprovada sua necessidade e será admitida a infiltração se houver indícios de infração penal de que trata o art. 1º e se a prova não puder ser produzida por outros meios disponíveis. § 3º A infiltração será autorizada pelo prazo de até 6 seis meses, sem prejuízo de eventuais renovações, desde que comprovada sua necessidade. (LIMA,2013, p.22)

CAPÍTULO II – TEORIA DOS DESPENALIZADORES E PROTEÇÃO PENAL

O presente capítulo trata detalhadamente da aplicação da teoria dos despenalizadores e a proteção penal, ela que é uma modalidade que visa a garantia da constituição federal, que estabelece a celeridade, economia processual, oralidade, infomalidade e simplicidade.

No contexto é apresentado o conceito, a panoramica juridico, crimes nas condições jurídicas despenalizada e o estado como parte, assim levando oa entendimento desde projeto a aplicabilidade na vida real.

2.1 Conceito

Devido à evolução que vem ocorrendo com o decorrer dos anos no direito penal, percebeu-se a necessidade de serem criadas novas medidas para um melhor andamento dos processos judiciais. Para que estes tivessem mais agilidade e mais celeridade, buscando-se assim novas ferramentas que trouxessem estes meios ao ordenamento jurídico pátrio.

As medidas despenalizadoras na verdade não descriminalizam nenhuma conduta, nenhuma conduta foi modificada no nosso ordenamento, nem tão pouco deixou de ser típica ou proibida. O processualista e professor Nestor Távora (2017, p. 3075) esclarece que “a lei, na realidade, não propiciou despenalização, antes tornando o sancionamento mais eficaz e, de certa forma, aceitável em virtude da manipulação discursiva da linguagem escolhida pelo legislador.

Este procedimento penal está previsto legalmente na lei regulamentadora

dos Juizados Especiais Criminais de número 9.099, de 26 de setembro de 1995. E objetiva primordialmente a aplicação de penas restritivas de direito e penas de multa no lugar da imposição de penas privas de liberdade. Ou seja, busca-se uma penalização mais branda (BRASIL, 2023).

A fim de se afastar a instauração do processo penal ou interromper o seu andamento, a Lei 9.099/95 criou as medidas despenalizadoras: composição dos 26 danos; transação penal; representação nos crimes de lesões corporais leves e lesões culposas; e suspenção condicional do processo (QUEIROGA, 2018).

Vale ressaltar que a competência dos Juizados Especiais se limita ao julgamento e execução das infrações de menor potencial ofensivo. Entendendo-se inicialmente, conforme art. 61, como infração de menor potencial ofensivo as "contravenções penais e os crimes a que a lei comine pena máxima não superior a um ano, excetuados os casos em que a lei preveja procedimento especial" (CAPEZ, 2022, p. 472 - 483).

No entanto, em 2001, a Lei 10.259 dispondo sobre os Juizados Especiais na esfera federal trouxe o seguinte conceito: "consideram-se infrações de menor potencial ofensivo, para os efeitos desta Lei, os crimes a que a lei comine pena máxima não superior a dois anos, ou multa" (BRASIL, 2023, *online*)

2.2 Panorama Jurídico

Em umas das obras do autor Guilherme Nucci, no manual de processo penal e execução penal fala que "Os Juizados Especiais Criminais são abraçados por princípios que norteiam a sua criação e a sua aplicação, pilares que auxiliam na solução de conflitos, vão onde a racionalidade do texto legal não conseguiu ir" (NUCCI, 2022, p.461).

Em um Estado Democrático de Direito, os princípios devem ser analisados, ainda que implicitamente expressos pela norma. Conforme Guilherme Nucci (2022) por surgirem da 30 observação de um padrão social, eles objetivam determinar padrões que permitam a pacífica convivência humana e uma célere resposta aos

conflitos. Assim, alguns principios se destacam como o da oralidade, da celeridade, por exemplo.

A Oralidade está expressa no art. 62 da Lei 9.099, contrastando com o procedimento comum onde prevalece a forma escrita. Por ter a celeridade na prestação jurisdicional um dos seus principais objetivos é de inteira coerência que a oralidade seja empregada o máximo de vezes possível. (NUCCI, 2022)

Para o renomado jurista Chiovenda (2008, p. 174), a oralidade é apresentada como uma junção de outros princípios que formam uma rede principiológica fundamental. É um conjunto que viabiliza a validade do principio da oralidade: o imediatismo, a concentração, a imutabilidade do juiz e a irrecorribilidade das decisões.

> [...] O princípio da oralidade traz em seu bojo outros norteamentos [...] complementares ou desmembramentos [...] Poderíamos dizer que esses princípios representam ‘um todo incindível’, no sentido de que a atuação de qualquer um deles é necessária a fim de que se torne possível realizar um processo verdadeiramente oral [...]

De acordo com o jurista Guilherme Marinone, é essencial que as causas submetidas aos Juizados Especiais de menor complexidade exijam uma solução célere, de modo que o legislador seja obrigado a instituir um procedimento que confira ao cidadão uma resposta tempestiva. Essa necessidade decorre do direito de acesso à justiça, que é respaldado pelo princípio de que todos têm direito a uma resposta tempestiva ao direito de buscar a realização de seus direitos perante o juiz. Além disso, o novo inciso LXXVIII do art. 5º da Constituição Federal estabelece expressamente o direito à tempestividade da prestação jurisdicional (MARINONE, 2007).

O processo penal no Brasil segue uma lista extensa de requisitos formais e na maioria das vezes inflexíveis. Isso acontece porque o direito penal protege os mais valiosos dos bens, a vida, a integridade física e liberdade de locomoção das pessoas. Assim, demonstrando clara excepcionalidade a regra, os Juizados Especiais adotaram a informalidade como princípio que sabiamente só será aplicado mediante o não comprometimento do interesse público e o não prejuízo de terceiros (LOPES JUNIOR, 2018).

2.3 Crimes na condição jurídica despenalizada

O processo penal no Brasil segue uma lista extensa de requisitos formais e na maioria das vezes inflexíveis. Isso acontece porque o direito penal protege os mais valiosos dos bens, a vida, a integridade física e liberdade de locomoção das pessoas. Assim, demonstrando clara excepcionalidade a regra, os Juizados Especiais adotaram a informalidade como princípio que sabiamente só será aplicado mediante o não comprometimento do interesse público e o não prejuízo de terceiros.

Sendo assim, deve-se mostrar as condutas elencadas como sendo de pequeno potencial ofensivo que estão dispostas pelo artigo 61 da lei 9.099/95, **"**Art. 61. Consideram-se infrações penais de menor potencial ofensivo, para os efeitos desta Lei, as contravenções penais e os crimes a que a lei comine pena máxima não superior a 2 (dois) anos, cumulada ou não com multa (BRASIL, 2023).

De acordo com o supracitado artigo neste rol, estão dispostos tanto os crimes, quanto as contravenções penais, cujas penalidades cabíveis sejam iguais ou mesmo inferiores a dois anos, cumuladas ou não com multa.

O interessante para o ordenamento jurídico é justamente a realização da reparação do dano. Fazendo assim com que as condutas, os fatos puníveis de menor potencial lesivo, ofensivo, sejam reparadas de forma ressocializadora, através da lei 9.099/95. Assim, temos que observar também que defrontam o princípio penal como por exemplo: Subsidiariedade, fragmentariedade e ofensividade (BOEIRA, 2018).

O crime cibernético, injuria, calunia, difamação, desacato e dentre outros estão dentro do rol de crimes de menor potencial ofensivo, assim sendo alancado pela medida despenalizadoras (BOEIRA, 2018).

Nesse sentido o artigo 154-A do código penal apresenta o delito de invasão de desportivo informado inserido na legislação citada por meio da Lei nº 12.737 de 30 de novembro de 2012. A tipificação do delito se apresenta como

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita" (BOEIRA, 2018).

O crime citado possui pena de detenção de três meses a um ano e a aplicação de multa, caso a invasão gera um prejuízo econômico a pena deverá ser aumentada de um sexto a um terço. A invasão de dispositivo pertencentes a algumas figuras políticas como o Presidente da República, Presidente do Supremo Tribunal Federal, governadores e prefeitos também gera o aumento da pena, só que nesse caso deverá ser aumentada de um terço até a metade da pena apresentada no caput (art. 154 – A, § 5º, I, II, III e IV) (HIRATA,2016).

Portanto em análise e mesmo sendo cabível uma medida despenalizadoras para o cibe crimes, devemos seguir os principais princípios do devido processo legal, afim de repara o dano causado a vítima e assim tendo um processo mais célere (SILVA, 2016).

O entendimento dos magistrados sobre a teoria despenalizadoras nos crimes cibernéticos pode variar bastante, dependendo de diversos fatores, como a legislação aplicável, a jurisprudência, as circunstâncias do caso concreto e a formação e orientação jurídica do próprio magistrado (SILVA, 2016).

No contexto dos crimes cibernéticos, a teoria despenalizadoras pode ser aplicada de diversas formas, considerando que nem todos os crimes cibernéticos são igualmente graves e que, muitas vezes, há outras formas de proteger os bens jurídicos envolvidos sem a necessidade de intervenção penal (SILVA, 2016).

Por exemplo, em casos de crimes cibernéticos menos graves, como a violação de direitos autorais na internet, alguns magistrados podem entender que a intervenção penal é desnecessária, sendo mais adequada a aplicação de sanções administrativas ou civis. Por outro lado, em casos de crimes cibernéticos mais graves, como a disseminação de pornografia infantil na internet, a teoria despenalizadoras pode não ser aplicável, uma vez que a proteção dos direitos fundamentais das crianças exige uma resposta penal mais incisiva (SILVA, 2016).

Em geral, os magistrados tendem a seguir a legislação aplicável e a jurisprudência, mas também levam em conta as particularidades do caso concreto e os princípios jurídicos que orientam a aplicação do direito penal. Assim, o

entendimento sobre a teoria despenalizadoras nos crimes cibernéticos pode variar bastante entre os magistrados, dependendo das circunstâncias específicas de cada caso (SILVA, 2016).

2.4 Estado como parte responsável pelos crimes cibernéticos

A responsabilidade pelo crime cibernético geralmente é atribuída a indivíduos ou grupos que executam o crime.

No entanto, os estados têm um papel importante em prevenir e combater o crime cibernético, seja através da implementação de leis e regulamentações que proíbam e punam o comportamento criminoso, ou através da alocação de recursos para agências e departamentos que trabalham para prevenir e investigar os crimes cibernéticos (BRODT; IASI, 2014).

No Brasil, a Lei regulamentadora dos crimes cibernéticos é a Lei nº 12.737/2012, também conhecida como Lei Carolina Dieckmann, em referência ao caso em que a atriz teve fotos íntimas divulgadas na internet sem autorização. A lei ficou conhecida por estabelecer punições para crimes como invasão de dispositivos eletrônicos, interceptação de dados, falsificação de documentos digitais, entre outros (BRODT; MANCINI, 2014).

Além disso, outras leis e normas regulamentam a segurança e privacidade na internet, como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que estabelecem regras sobre o uso de dados pessoais na internet e a responsabilidade das empresas em relação à segurança das informações de seus usuários (BRASIL, 2018).

O Marco Civil da Internet é uma lei brasileira, sancionada em abril de 2014, com o objetivo de estabelecer princípios, garantias, direitos e deveres para o uso da internet no país. A lei foi criada com o intuito de regulamentar a atuação do Estado, dos provedores de internet e dos usuários na rede mundial de computadores (MENDES, 2014).

Entre os principais pontos estabelecidos pelo Marco Civil da Internet,

destacam-se:

> Neutralidade da rede: todos os dados que trafegam na internet devem ser tratados de forma igualitária, sem discriminação de conteúdo, origem, destino ou serviço.
> Proteção da privacidade: a lei estabelece que os dados pessoais dos usuários só podem ser coletados e usados com seu consentimento, e que eles têm o direito de saber quais informações estão sendo coletadas e para que finalidade.
> Responsabilidade dos provedores: os provedores de internet não podem ser responsabilizados pelo conteúdo publicado pelos usuários em suas plataformas, a menos que descumpram ordem judicial para remoção do conteúdo.
> Liberdade de expressão: o Marco Civil da Internet protege a liberdade de expressão na internet, desde que não seja utilizado para a prática de crimes ou ofensas (LEMOS, 2014, *online*).

O Marco Civil da Internet foi criado em um contexto de debates sobre a regulação da internet no Brasil e é considerado uma importante referência para a legislação de outros países no tema (LEMOS, 2014).

Há diversos autores que abordam a Lei nº 12.965/2014, o Marco Civil da Internet, em suas obras, apresentando análises, interpretações e críticas à legislação. Alguns exemplos de autores e obras relevantes são: Carlos Affonso Souza (2018), professor de direito da FGV e diretor do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio) é coautor do livro "Marco Civil da Internet Comentado" e tem diversos artigos e obras sobre direito e tecnologia, incluindo "Direito, Internet e Liberdade de Expressão".

O Marco Civil é a legislação responsável por normatizar direitos, deveres e responsabilidades para todos aqueles que usufruem da internet no Brasil, sem que haja nesse processo um desrespeito aos direitos humanos e aos valores democráticos estabelecidos pela Constituição Federal da República Federativa do Brasil (SOUZA, 2018, Online).

O marco civil é um importante momento para a história do Brasil e dos avanços ligados ao usado da internet, uma vez que é responsável por apresentar princípios e garantias fundamentais que visam proteger de maneira efetiva os direitos dos mais diversos usuários do ambiente digital (SOUZA, 2018, Online).

Diante disso, se pode dizer que um dos pontos mais importantes apresentados no Marco Civil da Internet, pois trouxe para os usuários a garantia de maior controle sobre os dados pessoais dos usuários por empresas e pelo Estado bem como a proteção desses dados. (SOUZA, 2018)

Essas são apenas algumas das citações presentes no livro, que oferece uma análise detalhada e aprofundada do Marco Civil da Internet e de seus impactos na sociedade brasileira.

Dentro do direito digital no Brasil podemos destacar que esta área do direito surgiu como forma de solucionar os desafios que o crescimento da tecnologia digital que o direito tradicional já existente não era capaz de solucionar. Como exemplo desses problemas de difícil resolução temos como tema o direito à privacidade dos usuários das novas tecnológicas, a propriedade intelectual, bem como os limites da liberdade de expressão nesses ambientes e o acesso a informação que muitas vezes pode apresentar dados deturpados. (LEMOS, 2023)

Ainda que a internet se apresente como um espaço que trouxe inúmero avanços para a sociedade em geral e também para o meio jurídico, o seu rápido avanço acabou gerando desafios que o direito não estava preparado para lidar. (LEMES, 2014)

Esses são apenas alguns exemplos de autores que abordam o Marco Civil da Internet em suas obras, existem muitos outros autores que contribuem para o debate sobre a lei e suas implicações. Nesse contexto, a participação do Estado como parte em processos judiciais assume uma importância ainda maior (SOUZA, 2014).

De acordo com a teoria dos despenalizados, a intervenção penal só deve ocorrer em casos de ofensas graves aos bens jurídicos fundamentais, como a vida, a integridade física, a liberdade, a propriedade, entre outros. Isso significa que o Estado deve atuar como autor em casos de crimes que envolvam esses bens jurídicos fundamentais, visando garantir a proteção desses direitos. (ZAFFARONI; PIERANGELI, 1988.)

Por outro lado, a participação do Estado como réu em processos judiciais também é importante para a proteção dos direitos dos cidadãos. Em casos em que o Estado comete excessos ou violações de direitos fundamentais, a possibilidade de responsabilização penal pode servir como um incentivo para que ele atue de forma justa e adequada, garantindo a proteção dos direitos dos cidadãos (GOMES,2016).

Assim, a participação do Estado como parte em processos judiciais é fundamental para a proteção penal, tanto na perspectiva do autor, quando o Estado busca garantir a proteção dos direitos fundamentais, quanto na perspectiva do réu, quando o Estado é alvo de ações judiciais por excessos ou violações de direitos fundamentais (GOMES,2016).

CAPÍTULO III – POSIÇÃO JURÍDICA E O TRATAMENTO LEGAL

O presente capítulo trata detalhadamente da posição jurídica e o tratamento legal para os crimes cibernéticos e podem variar de acordo com o sistema legal de cada país. No entanto, em geral, muitos países têm leis específicas para lidar com crimes cibernéticos e reconhecem a importância de combater as atividades ilegais realizadas através da internet e de outros meios eletrônicos.

As leis relacionadas aos crimes cibernéticos geralmente estabelecem punições específicas para esses tipos de delitos. As penalidades podem variar desde multas monetárias até penas de prisão, dependendo da gravidade do crime e do dano causado.

No contexto é apresentado aspectos gerais, requisitos, posicionamento doutrinário e o posicionamento dos tribunais Superiores (STJ), assim levando oa entendimento desde projeto a aplicabilidade na vida real.

3.1 Aspectos Gerais

Os crimes cibernéticos são uma realidade cada vez mais presente na sociedade moderna, trazendo desafios complexos para o sistema jurídico. Neste contexto, é fundamental compreender os aspectos gerais desses crimes, incluindo sua definição, características e impactos.

Os aspectos gerais dos crimes cibernéticos, podemos dividir as situações em duas categorias: direta e indireta. Além disso, a noção de referias é importante para compreender a relação entre o mundo virtual e o mundo físico no contexto

desses crimes.

As situações diretas referem-se a crimes cibernéticos em que o próprio meio digital é utilizado como instrumento para a prática da conduta ilegal. O autor Marc Goodman (2015) esclarece que exitem varias formas como o Hacking: Acesso não autorizado a sistemas, computadores ou redes com o objetivo de obter informações confidenciais, danificar ou manipular dados, bem como, distribuição de malware: Disseminação de vírus, worms, trojans e outros programas maliciosos para comprometer a segurança de sistemas ou obter informações confidenciais.

As fraudes eletrônicas é o uso de informações falsas ou enganosas para obter benefícios financeiros ilícitos, como phishing (obtenção de informações pessoais por meio de mensagens eletrônicas fraudulentas) e clonagem de cartões de crédito, assim como também exitem a difamação online: Publicação de informações falsas ou prejudiciais sobre uma pessoa ou empresa na internet (MARCN GOODMA, 2015).

Em outro momento de sua obra Future Crimes: Inside the Digital Underground and the Battle for Our Connected World" (Crimes Futuros: Por Dentro do Submundo Digital e a Batalha por Nosso Mundo Conectado, em tradução livre), Goodma (2015) explica também sobre as seguintes formas indiretas que existem e que envolvem crimes em que a internet ou meios eletrônicos são utilizados como ferramentas facilitadoras para a prática de outros delitos.

Algums formas indiretas são: Lavagem de dinheiro: Utilização de sistemas eletrônicos para ocultar a origem de fundos obtidos por meio de atividades criminosas, Tráfico de drogas ou armas: Utilização da internet e das redes de computadores para coordenar transações e contatos relacionados ao tráfico de drogas ou armas, bem como, Exploração sexual de crianças: Uso da internet para compartilhar e distribuir conteúdo pornográfico envolvendo crianças (GOODMA, 2015).

No entanto a noção de referias, refere-se à ligação entre o mundo virtual e o mundo físico nos crimes cibernéticos. Embora muitos desses crimes ocorram no ambiente digital, eles podem ter consequências reais no mundo físico, como roubo

de identidade, danos financeiros e emocionais, violação da privacidade e até mesmo impactos na segurança nacional (GOODMA, 2015).

Para Goodma (2015), é importante que as leis e os sistemas jurídicos considerem esses aspectos gerais das situações diretas e indiretas dos crimes cibernéticos, a fim de desenvolver mecanismos legais e de segurança eficazes para prevenção, investigação e punição desses delitos.

É essencial destacar que os crimes cibernéticos não conhecem fronteiras geográficas, o que amplia ainda mais os desafios enfrentados pelas autoridades. Com a globalização e a interconectividade, os criminosos podem atuar de qualquer parte do mundo, comprometendo a segurança digital em diferentes países simultaneamente. Isso requer uma abordagem colaborativa e uma cooperação internacional efetiva para combater essas ameaças, incluindo o intercâmbio de informações e a adoção de padrões de segurança comuns (SUFFERT, 2021).

3.2 – Requisitos para o Posicionamento Jurídico e o Tratamento Legal

O tratamento legal dos crimes cibernéticos pode variar em diferentes jurisdições. Em geral, os crimes cibernéticos são abordados por meio de leis específicas que criminalizam atividades como Hawking, phishing, fraude eletrônica, roubo de dados e invasões de sistemas (SANTOS, 2013).

Essas leis segundo o autor Coriolano Aurélio de Almeida Camargo Santos (p.65) são projetadas para proteger a integridade e a confidencialidade dos dados, bem como para garantir a segurança das infraestruturas críticas. Em muitos países, os crimes cibernéticos são punidos com penas de prisão, multas e outras medidas corretivas, dependendo da gravidade da infração (SANTOS, 2013).

A investigação e a punição dos crimes cibernéticos exigem a cooperação de várias entidades, incluindo autoridades policiais, agências de segurança cibernética e unidades especializadas em crimes tecnológicos. A obtenção de provas digitais e a identificação dos responsáveis podem ser desafiadoras, pois os criminosos muitas vezes usam técnicas sofisticadas para encobrir suas atividades e

esconder sua identidade (BLUM, 2020).

Renato Opice Blum (2020), destaca em sua obra ´´Direito Digital", que a cooperação internacional desempenha um papel fundamental no combate aos crimes cibernéticos, uma vez que essas atividades podem atravessar fronteiras e envolver indivíduos de diferentes países. Acordos de cooperação e tratados internacionais são estabelecidos para facilitar o intercâmbio de informações, a extradição de suspeitos e a colaboração entre as autoridades competentes.

Essas iniciativas visam fortalecer a capacidade de resposta global aos crimes cibernéticos e garantir que os criminosos não possam se esconder ou escapar da justiça (BLUM, 2020).

A autora Laura Schertel Mendes (2018), destaca que é importante a evolução contínua da tecnologia e as ameaças cibernéticas requer uma constante atualização das leis e dos métodos de investigação. Os profissionais jurídicos e as autoridades responsáveis devem estar atentos às mudanças no cenário da segurança cibernética e trabalhar em conjunto com especialistas em tecnologia para aprimorar as estratégias de prevenção, detecção e repressão aos crimes cibernéticos

Somente com um esforço conjunto e uma abordagem multidisciplinar será possível enfrentar os desafios cada vez mais complexos e proteger a sociedade no mundo digital (MENDES,2014)

O combate aos crimes cibernéticos exige uma abordagem multidisciplinar e colaboração entre entidades e especialistas. A evolução da tecnologia e a sofisticação das ameaças cibernéticas demandam a constante atualização das leis e métodos de investigação. A cooperação internacional é essencial para enfrentar crimes que ultrapassam fronteiras. Profissionais jurídicos devem trabalhar em conjunto com especialistas em tecnologia para desenvolver estratégias eficazes de prevenção, detecção e repressão (BLUM, 2020).

3.3 Posicionamento Doutrinário

A infiltração virtual dos agentes policiais como meio de obtenção de provas na persecução penal é um tema complexo e polêmico que suscita diferentes posicionamentos doutrinários. Algumas correntes doutrinárias defendem sua utilização como uma ferramenta necessária para combater efetivamente crimes praticados no ambiente virtual (LIMA, 2016).

Argumenta-se que o avanço tecnológico criou novas modalidades delitivas, exigindo uma resposta adequada por parte das autoridades. A infiltração virtual permitiria a coleta de provas indispensáveis, especialmente em casos de organizações criminosas que atuam na internet (LIMA, 2016).

Guilherme Nucci (2022), jurista e professor de Direito Penal, tem defendido a infiltração virtual como uma importante ferramenta para a investigação e repressão de crimes cometidos no ambiente virtual. Ele argumenta que a infiltração é essencial para acompanhar as mudanças no cenário criminal e proteger a sociedade.

O Professor e autor brasileiro na área de Direito Penal, André Estefam (2016), tem se manifestado a favor da infiltração virtual como um meio necessário para a investigação e repressão de crimes cibernéticos. Ele destaca a importância de utilizar meios modernos para enfrentar as novas formas de criminalidade.

Por outro lado, há doutrinadores que adotam um posicionamento restritivo à infiltração virtual. Eles argumentam que ela representa uma invasão da privacidade e um risco para os direitos fundamentais dos indivíduos. Defendem que o Estado deve respeitar os limites impostos pela Constituição, evitando a utilização abusiva de técnicas invasivas. Para essa corrente, é preciso encontrar um equilíbrio entre a necessidade de investigação e a proteção dos direitos individuais (ESTEFAM, 2016).

O Professor e autor renomado na área do Direito Processual Penal, Aury Lopes Junior. (2021), tem uma visão crítica em relação à infiltração virtual. Ele argumenta que essa técnica viola a privacidade dos indivíduos e pode resultar em abusos, defendendo a necessidade de limites claros e rigorosos para sua utilização.

Embora Guilherme Nucci (2022), também seja mencionado anteriormente como um jurista favorável à infiltração virtual, é importante destacar que ele também apresenta uma visão restritiva. Nucci argumenta que a infiltração virtual deve ser utilizada com parcimônia e respeitando os direitos fundamentais, buscando um equilíbrio entre a efetividade da investigação e a proteção dos indivíduos.

Alguns especialistas sustentam que, independentemente do posicionamento adotado em relação à infiltração virtual, é crucial estabelecer uma regulamentação rigorosa para sua utilização. Essa regulamentação deve definir os requisitos e limites para a infiltração virtual, estabelecendo salvaguardas para evitar abusos e proteger os direitos fundamentais dos investigados. É necessário estabelecer critérios objetivos que garantam a legalidade e a legitimidade da infiltração virtual, além de assegurar a transparência e o controle sobre sua aplicação (GOMES, 2017).

Outra perspectiva argumenta que cada caso de infiltração virtual deve ser analisado individualmente, considerando os interesses envolvidos, a gravidade do delito e a proporcionalidade da medida. Defende-se uma avaliação criteriosa, baseada em critérios objetivos, para decidir sobre a legalidade e a legitimidade da infiltração virtual em cada situação. Essa abordagem busca evitar generalizações e garantir que a infiltração virtual seja aplicada de forma justa e equilibrada, respeitando os direitos e garantias dos envolvidos (GOMES, 2017).

O Jurista e professor de Direito Penal, Antônio Scarance Fernandes (2019) enfatiza a necessidade de uma análise individualizada e criteriosa na aplicação da infiltração virtual. Ele argumenta que critérios objetivos devem ser estabelecidos para avaliar a legalidade e a legitimidade da técnica, garantindo a proteção dos direitos fundamentais dos envolvidos.

Em suma, a discussão sobre a infiltração virtual dos agentes policiais como meio de obtenção de provas na persecução penal envolve uma ampla gama de posicionamentos doutrinários. Enquanto alguns defendem sua utilização como uma ferramenta necessária para o combate aos crimes virtuais, outros adotam uma postura restritiva em nome da proteção dos direitos fundamentais (FERNANDES, 2019).

Independentemente do posicionamento adotado, existe acordo sobre a necessidade de uma regulamentação rigorosa e uma avaliação criteriosa para garantir o equilíbrio entre a investigação e a proteção dos direitos individuais, conforme estabelecido pela legislação brasileira, Lei 12.965/2014, conhecida como Marco Civil da Internet (BRASIL, 2022).

Enquanto alguns defendem sua utilização para combater crimes virtuais, outros são restritivos em nome dos direitos fundamentais. No entanto, há acordo sobre a necessidade de uma regulamentação rigorosa e avaliação criteriosa. Critérios objetivos devem ser estabelecidos para garantir a legalidade e legitimidade da técnica, equilibrando investigação e proteção dos direitos individuais. É preciso analisar cada caso individualmente, considerando os interesses, gravidade do delito e proporcionalidade da medida. O Marco Civil da Internet estabelece diretrizes para a infiltração virtual no Brasil (SCHERTEL, 2018).

3.4 Posicionamento do tribunal Superior (STJ)

O posicionamento do Superior Tribunal de Justiça (STJ) em relação à infiltração virtual dos agentes policiais como meio de obtenção de provas na persecução penal tem sido objeto de discussões e debates no âmbito jurídico. Esse tema envolve a utilização de recursos tecnológicos e virtuais pelos agentes para adentrar em grupos ou redes sociais com o intuito de investigar e coletar provas de crimes (NUCCI, 2022).

Resp.2.257.960/STJ - Nesse caso, o Superior Tribunal de Justiça confirmou a validade das provas obtidas por meio da infiltração virtual. Foi estabelecido que, desde que respeitados os critérios legais e constitucionais, como a autorização judicial prévia e a proporcionalidade na utilização da técnica, as provas obtidas por agentes infiltrados em redes sociais podem ser consideradas lícitas e admissíveis no processo penal. Essa jurisprudência reforça a importância do controle judicial e da observância dos direitos fundamentais durante a infiltração virtual (STJ, 2023).

Inicialmente, é importante ressaltar que o STJ reconhece a infiltração virtual como um importante instrumento no combate ao crime organizado e à criminalidade digital. O tribunal entende que a evolução tecnológica e a utilização intensa da internet como meio de comunicação exigem que as técnicas de investigação sejam atualizadas para acompanhar essas mudanças e garantir a eficácia da persecução penal (NUCCI, 2022).

Entretanto, o STJ também enfatiza a necessidade de balizar a infiltração virtual com os princípios constitucionais, em especial o direito à privacidade e à intimidade dos indivíduos. O tribunal entende que o uso dessa técnica deve ser pautado por critérios rigorosos, como a existência de indícios razoáveis da prática de crime e a autorização judicial prévia, a fim de preservar os direitos fundamentais dos cidadãos (GOMES, 2017).

RHC 176.936/STJ - Nesse caso, o Superior Tribunal de Justiça anulou as provas obtidas por meio da infiltração virtual de agentes policiais. Foi constatado que a infiltração ocorreu de forma abusiva e desproporcional, violando a privacidade e os direitos fundamentais dos indivíduos investigados. A jurisprudência estabeleceu que, mesmo que haja autorização judicial, é fundamental que a infiltração virtual seja realizada de maneira cautelosa, respeitando os limites legais e garantindo a observância dos direitos constitucionais dos envolvidos (STJ, 2023).

Além disso, o STJ ressalta que a infiltração virtual não pode servir como um meio de incitação ou provocação de crimes. Os agentes infiltrados devem atuar de forma passiva, apenas coletando provas e informações para subsidiar a investigação. O tribunal também enfatiza a importância da proporcionalidade e da necessidade da medida, ou seja, a infiltração virtual deve ser o último recurso utilizado quando outras formas de obtenção de provas se mostrarem insuficientes (PEREIRA, 2017).

No que se refere à validade das provas obtidas por meio da infiltração virtual, o STJ entende que elas são admissíveis, desde que respeitados os critérios estabelecidos pela jurisprudência. As provas devem ser obtidas de forma lícita, sem violar direitos fundamentais, e sua apresentação deve ser acompanhada de todas as

informações e documentos necessários para que sua autenticidade seja comprovada (PEREIRA, 2017).

Por fim, o STJ destaca a importância da transparência e do controle judicial na utilização da infiltração virtual. O tribunal ressalta que é necessário haver um acompanhamento rigoroso do poder judiciário sobre a atuação dos agentes infiltrados, a fim de evitar abusos e garantir que a técnica seja utilizada dentro dos limites legais e constitucionais (PEREIRA, 2017)

Em suma, o posicionamento do STJ sobre a infiltração virtual dos agentes policiais como meio de obtenção de provas na persecução penal é favorável, desde que sejam observados critérios rigorosos e respeitados os direitos fundamentais dos cidadãos. A utilização dessa técnica deve ser feita de forma proporcional, com autorização judicial prévia, e as provas obtidas devem ser lícitas e passíveis de comprovação. O controle judicial e a transparência são essenciais para garantir a legalidade e a legitimidade desse meio de investigação (PEREIRA, 2017).

CONCLUSÃO

Diante da análise minuciosa do tema "Infiltração Virtual dos Agentes Policiais" abordado no Capítulo I, bem como da compreensão da Teoria dos Despenalizadoras e Proteção Penal discutida no Capítulo II, e finalmente da posição jurídica e o tratamento legal penal explorados no Capítulo III, é possível concluir que a questão dos crimes cibernéticos apresenta desafios significativos para o sistema de justiça.

No Capítulo I, foi apresentado o surgimento dos crimes cibernéticos, evidenciando a necessidade de uma legislação adequada para lidar com tais delitos. Além disso, abordou-se a importância das provas na investigação desses crimes, ressaltando a relevância da infiltração do agente policial como uma ferramenta eficaz para o combate a essas práticas ilícitas.

No Capítulo II, a Teoria dos Despenalizadoras e Proteção Penal trouxe reflexões acerca da necessidade de uma abordagem diferenciada no tratamento dos crimes cibernéticos. Destacou-se o panorama jurídico atual e os crimes que são despenalizados, ressaltando-se a responsabilidade do Estado como parte nesse contexto.

Já no Capítulo III, discutiu-se os aspectos gerais da posição jurídica e o tratamento legal penal dos crimes cibernéticos. Foram apresentados os requisitos necessários para o posicionamento jurídico adequado e o tratamento legal eficiente

dessas condutas. Além disso, foram abordados o posicionamento doutrinário e a posição do Tribunal Superior (STJ), fornecendo uma visão abrangente das perspectivas jurídicas nesse campo.

Diante desses elementos, fica evidente que a infiltração virtual dos agentes policiais é uma ferramenta indispensável para a investigação e o combate aos crimes cibernéticos. No entanto, é necessário um equilíbrio entre a proteção dos direitos individuais e a eficiência do Estado na repressão dessas condutas.

Nesse sentido, é fundamental que a legislação se mantenha atualizada e acompanhe o avanço tecnológico, fornecendo as bases jurídicas necessárias para uma atuação eficaz das autoridades policiais. Além disso, é essencial que haja uma contínua reflexão sobre a adequação dos crimes cibernéticos à Teoria dos Despenalizadoras, visando encontrar um equilíbrio entre a repressão penal e outras formas de sanção.

Por fim, é fundamental que o posicionamento jurídico e o tratamento legal penal dos crimes cibernéticos sejam embasados em sólidos fundamentos doutrinários e respaldados por decisões do Tribunal Superior (STJ), proporcionando segurança jurídica e efetividade nas ações de combate a essas práticas delitivas.

Portanto, conclui-se que a infiltração virtual dos agentes policiais, dentro de um quadro jurídico adequado, aliada à compreensão da Teoria dos Despenalizadoras e Proteção Penal, bem como ao estabelecimento de uma posição jurídica clara e um tratamento legal penal adequado, constitui uma estratégia indispensável para o enfrentamento eficaz dos crimes cibernéticos e a proteção da sociedade como um todo.

REFERÊNCIAS

AGÊNCIA SENADO. Reprodução autorizada mediante citação da Agência Senado, Fonte: **Agência Senado** Disponível em: https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada- adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico. Acesso em:29 nov. 2022.

BOEIRA, Mariana de Mello. **REVISTA DE DIREITO DA UNIVERSIDADE DE SÃO PAULO (USP).** VL.20, N°121. Disponível em:https://www.revistas.usp.br/rfdusp/issue/view/9816/showTo, publicado em 2018. Acesso em: 08 abr. 2023.

BLUM, Renato Opice. **Direito digital.** São Paulo: Editora IASP, 2020.

BOITEUX, Luciana. Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual. **Doutrinas Essenciais de Direito Penal**. São Paulo vol. 8, 2010

BRASIL**. Lei 13.441 infiltrações de agentes da polícia** Disponível em: https://www.gov.br/planalto/pt-br. Acesso em: 29 nov. 2022

BRASIL. **Lei 10.259/2001 lei dos juizados cíveis e criminais no âmbito federal**. Disponível em:https://www.planalto.gov.br/ccivil_03/Leis/LEIS_2001/L10259.htm. Acesso em: 12 abr. 2023.

BRASIL. **Lei 13.709/2018 lei geral de proteção de dados (LGPD)**. Disponível em:https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

BRASIL. **Código penal**, artigo 154-A. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 10 abr. 2023.

BRASIL**. Lei 13.441 infiltrações de agentes da polícia** Disponível em: https://www.gov.br/planalto/pt-br. Acesso em: 29 nov. 2022.

BRASIL. **Lei nº 12.965/2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 31 mai. 2023.

BRASIL. Supremo Tribunal de Justiça. **Agravo em Recurso Especial, Nº 2257960** - MG, Julgado em 19/05/2023, Min. REYNALDO SOARES DA FONSECA. Disponível em: https://scon.stj.jus.br. Acesso em: 31 mai. 2023.
BRASIL. Supremo Tribunal de Justiça. **Recurso em habeas corpus, Nº 176939** – DF, Julgado em 24/04/2023, Min. JOEL ILAN PACIORNIK. Disponível em: https://scon.stj.jus.br. Acesso em: 31 mai. 2023.

BRODT, Luiz Augusto Sanzo, IASI, Mariana Mancini. " O crime virtual e o papel do magistrado na aplicação da lei". **Revista de Direito Eletrônico e Tecnologia da Informação**, edição 3, de 2014. Disponível em: https://juslaboris.tst.jus.br/busca-avancada. Acesso em: 10 abr. 2023.

CAPEZ, Fernando. **Curso de processo penal** / Fernando Capez. – 23. ed. – São Paulo: Saraiva, 2016.

CORREIA, Virato. **Operadores Jurídicos**. 13. p,107 ed. São Paulo: Atlas, 2000.

ESTEFAM, André**. Direito penal**: Parte Geral. – São Paulo: Saraiva, 2016.

FERNANDES, Antônio Scarance. **"Processo Penal Constitucional**´ ´Editora Saraiva, 2019.

GOMES, Luiz Flávio. "**Direito Penal- Parte Geral**". Editora Saraiva, 2016.

GOMES, Luiz Flávio. **"Crimes Cibernéticos**: Desafios e estratégias no combate à criminalidade digital **"**. Editora Saraiva, 2017.

GOODMAN. M. "***Future Crimes****: Inside the Digital Underground and the Battle for Our Connected World"* (Crimes Futuros: Por Dentro do Submundo Digital e a Batalha por Nosso Mundo Conectado, em tradução livre). Saraiva Educação S.A., 2015.

HIRATA, Alessandro. "O direito à privacidade na era digital", **Revista Brasileira de Direito Civil,** edição 16, de 2018**.**

HOFFMANN, Jussara**. Avaliação**: Mito e Desafio: uma perspectiva Construtivista. 45. ed. Porto Alegre: Mediação, 2017.

LEMOS, Ronaldo. " O marco civil da Internet", **III Jornada de Iniciação Científica e de Extensão Universitário,** edição 3, N° 3. 2014. Disponível em: https://unisantacruz.edu.br/revistas-old/index.php/JICEX/article/view. Acesso em: 08 abr 2023

LEMOS, Ronaldo. " **O que é Direito Digital?** ´´ ITS Rio (Instituto de Tecnologia e Sociedade do Rio de Janeiro), 2016. Disponível em: https://itsrio.org/wp-content/uploads/2016/04/O-que-%C3%A9-Direito-Digital.pdf.Acesso em: 17 abr. 2023.

LIMA, Marco Aurélio Costa de. **Infiltração policial:** pensando em um modelo. Monografia (graduação em Estudos de Política e Estratégia). Rio de Janeiro. ESG. 2013

LIMA, Renato Brasileiro de. **"Manual de Processo Penal"**, Volume Único. Editora Saraiva, 2016.

LIMA, Renato Brasileiro de. **"Manual de Processo Penal"**. Editora Saraiva, 2017.

LOPES.A.J**. Direito processual penal.** Saraiva Educação S.A., 2018.

LOPES JUNIOR, Aury. **Direito Processual Penal**, edição 17. Editora Saraiva, 2021.

MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**, p. 37-69, 2018.

MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet. **Revista Jurídica** p. 37 a 69. 2018.

NERY, Paula Antunes **REVISTA MP-GO 11ª edição,2016** Disponível em: http:/www. mpgo.mp.br/portal/noticia/revista-mpgo-nova-edição. Acesso em: 29 nov. 2022.

NUCCI, Guilherme de Souza. **Código penal comentado**. 2. ed. rev., atual. e ampl. São Paulo. Revista dos Tribunais. 2016

NUCCI, Guilherme. **Manual de processo penal e Execução Penal**. 2022. P.461 a 467.

PEREIRA, Flávio Cardoso. Agente Infiltrado Virtual (LEI N.13.441/17): Primeiras Impressões. **Revista do Ministério Público de Goiás**. P 110 a 115. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/Rev-MP-GO_n.33.pdf#page=97. Acesso em: 31 mai. 2023.

QUEIROGA, Tâmita Marjori Magalhães de. **Análise do instituto da transação penal como medida despenalizadoras.** São Paulo. Saraiva Educação S.A., 2018.

ROSSINI, G.; PARRINI, S.; CASTROFLORIO, T.; **Guerra Fria**. P.133, 2015.

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

SILVA, Rafael Moreira. "O papel dos magistrados na aplicação das leis de crimes cibernéticos no Brasil". **Revista Brasileira de Ciências Criminais,** edição 121, de julho/agosto de 2016.Disponíve em: https://www.editoraforum.com.br/revista-dos-tribunais. Acesso em: 10 abr.2023.

SOUZA. Carlos Affonso. Direito e Liberdade de Expressão. **Revista da Faculdade de Direito da Universidade Federal de Minas Gerais**. 2018. Disponível em:https://periodicos.ufmg.br/index.php/revista/article/view/11026/9 485. Acesso em 10 abr.2023.

SOUZA, Carlos Affonso. LEMOS, Ronaldo. "Internet e direitos humanos: proteção e limites jurídicos´´, **Revista de Direito da FGV, 2012**. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/article/view/50650. Aceso em: 12 abr. 2023.

SOUZA. Carlos Affonso. " **Marco Civil da Internet comentado´´,** Editora Revista dos Tribunais. 2014. P.13, 23, 33, 66 e 91.

SUFFERT, Sandro. **Crimes Digitais**: Prevenção e Investigação. Saraiva, 2021.
ZAFFARONI e PIERANGELI. ´´**Direito Penal Brasileiro** - Parte Geral´ ´Editora Revista dos Tribunais,1988