Noções sobre infiltração online no processo penal brasileiro: uma análise a partir do estudo de Luís Greco

Notions about online infiltration in the brazilian criminal procedure: an analysis from the study of Luís Greco

Artigo recebido em 10/03/2024 e aprovado em 12/04/2024.

Wellington José Campos

Mestre em direito das relações econômicas e sociais, Faculdades Milton Campos.
Professor no Instituto Mineiro de Direito.

Resumo

Este estudo visa explorar as complexidades da infiltração online dentro do processo penal brasileiro, abordando suas implicações éticas e legais por meio da perspectiva do estudo de Luís Greco sobre a experiência alemã. O objetivo é avaliar a necessidade de um marco regulatório que concilie a eficácia investigativa com a salvaguarda dos direitos fundamentais no contexto da digitalização crescente. A metodologia utilizada é a dedutiva, por meio da revisão bibliográfica, com uma abordagem comparativa. O artigo analisa como a legislação alemã, especialmente o § 100b StPO, regula a infiltração online, enfatizando critérios rigorosos e medidas protetivas para garantir a justiça e a proporcionalidade das operações de investigação. A pesquisa baseia-se na análise teórica e na revisão da legislação pertinente, buscando adaptar as lições aprendidas com a experiência alemã ao cenário brasileiro. Destaca-se a importância de um marco legal específico que permita a infiltração online de forma ética e fundamentada, respeitando os direitos individuais enquanto enfrenta os desafios impostos pelo ciberespaço. O artigo conclui enfatizando a contribuição de Greco para o diálogo sobre infiltração online no Brasil, sugerindo que a abordagem legislativa da Alemanha pode oferecer diretrizes valiosas para a criação de uma legislação brasileira que equilibre a segurança e as liberdades civis. Propõe-se uma reflexão sobre as implicações da infiltração online, reiterando a necessidade de um debate aprofundado e do desenvolvimento de normas claras para a prática investigativa no ambiente digital, respeitando princípios éticos e constitucionais.

Palavras-chaves: Alemanha; Brasil; infiltração online; legislação; marco regulatório; processo penal.

Abstract

This study aims to explore the complexities of online infiltration within the Brazilian criminal process, addressing its ethical and legal implications through the perspective of Luís Greco's study of the German experience. The objective is to assess the need for a regulatory framework that reconciles investigative effectiveness with the safeguarding of fundamental rights in the context of increasing digitalization. The methodology used is deductive, through bibliographical review, with a comparative approach, the article analyzes how German legislation, especially § 100b StPO, regulates online infiltration, emphasizing strict criteria and protective measures to guarantee justice and proportionality of investigative operations. The research is based on theoretical analysis and a review of relevant legislation, seeking to adapt the lessons learned from the German experience to the Brazilian scenario. The importance of a specific legal framework that allows online infiltration in an ethical and well-founded manner is highlighted, respecting individual rights while facing the challenges posed by cyberspace. The article concludes by emphasizing Greco's contribution to the dialogue on online infiltration in Brazil, suggesting that Germany's legislative approach can offer valuable guidelines for creating Brazilian legislation that balances security and civil liberties. A reflection is proposed on the implications of online infiltration, reiterating the need for an in-depth debate and the development of clear standards for investigative practice in the digital environment, respecting ethical and constitutional principles.

Keywords: Germany; Brazil; online infiltration; legislation; regulation mark; criminal procedure.

1 Introdução

O advento da internet e das novas tecnologias digitais trouxe desafios inéditos para a investigação criminal. Crimes que antes eram praticados no mundo físico passaram a ser praticados também no mundo virtual, o que exigiu o desenvolvimento de novas ferramentas e técnicas de investigação.

A infiltração online é uma dessas técnicas. Ela consiste na participação de agentes públicos em grupos ou fóruns virtuais, com o objetivo de coletar informações sobre a prática de crimes. Essa técnica pode ser utilizada para investigar uma ampla gama de crimes, incluindo tráfico de drogas, pornografia infantil, crimes financeiros e ciberterrorismo.

No Brasil, a infiltração online é regulamentada pela Lei 12.850/2013, que dispõe sobre a investigação criminal conduzida por agentes de polícia judiciária. No entanto, a legislação brasileira ainda é incipiente, o que abre espaço para debates sobre suas implicações éticas e legais.

A evolução das tecnologias de investigação no Brasil tem sido acompanhada de uma crescente preocupação com as implicações éticas e legais dessas novas ferramentas. No contexto da infiltração online, a atenção se concentra em dois principais aspectos: a privacidade das pessoas e os seus direitos individuais, bem como os limites éticos e constitucionais da atuação dos agentes públicos.

No que diz respeito à privacidade e aos direitos individuais, a infiltração online pode representar uma violação da privacidade dos usuários da internet. Os agentes públicos que participam de grupos ou fóruns virtuais podem coletar informações pessoais dos usuários, como nomes, endereços de *e-mail*, números de telefone e até mesmo imagens ou vídeos. Essas informações podem ser utilizadas para fins investigativos, mas, também, podem ser utilizadas para fins ilícitos, como chantagem ou extorsão, o que nos impõe uma transformação e evolução nos meios investigativos, como apontado por Castells (2001), "a era digital redefiniu não apenas as interações sociais, mas, também, impôs novos desafios ao direito penal, exigindo adaptações significativas nas abordagens de investigação criminal".

Quanto aos limites éticos e constitucionais da atuação dos agentes públicos, a infiltração online pode representar um conflito entre a necessidade de investigar crimes e o direito à liberdade de expressão. Os agentes públicos que participam de grupos ou fóruns virtuais podem passar-se por pessoas que não são, o que pode ser considerado uma violação da liberdade de expressão. Além disso, os agentes públicos podem induzir os usuários a cometer crimes, o que também pode ser considerado uma violação da liberdade de expressão.

Em uma era caracterizada por avanços tecnológicos rápidos e uma crescente digitalização da sociedade, o direito penal enfrenta desafios sem precedentes. A expansão do ciberespaço abriu novos horizontes para a atividade criminosa, trazendo consigo a necessidade de métodos investigativos adaptados a esse novo ambiente.

Este artigo propõe-se a explorar as nuances da infiltração online no processo penal brasileiro, oferecendo uma análise detalhada e fundamentada no estudo de Luís Greco, intitulado "A infiltração online no processo penal – Notícia sobre a experiência alemã e inteligência artificial". Essa obra pioneira fornece uma base comparativa e teórica essencial para entender as implicações dessa prática no contexto brasileiro, como técnica de investigação, tem-se mostrado uma ferramenta indispensável ao combate a uma variedade de crimes, particularmente aqueles perpetrados no ambiente digital.

A metodologia adotada neste estudo se caracteriza por sua abordagem dedutiva e comparativa, fundamentando-se principalmente na revisão bibliográfica detalhada de textos legais, doutrinários e acadêmicos relevantes, com especial atenção ao trabalho de Luís Greco e à legislação alemã concernente à infiltração online, em particular o § 100b StPO. A pesquisa inicia-se com a formulação de hipóteses baseadas em premissas teóricas existentes sobre a infiltração online e suas implicações no processo penal, tanto no Brasil quanto na Alemanha. Seguindo uma lógica dedutiva, parte-se de teorias gerais para a análise de situações específicas, examinando como a legislação e as práticas alemãs podem ser adaptadas ao contexto brasileiro, considerando as particularidades jurídicas e sociais do país.

A investigação enfoca a comparação entre os sistemas jurídicos, buscando identificar os critérios adotados pela Alemanha para a regulamentação da infiltração online, como a exigência de rigorosos controles judiciais e

a implementação de salvaguardas para proteger os direitos dos indivíduos envolvidos. Por meio desse exame comparativo, o estudo propõe uma reflexão sobre as potenciais diretrizes para a elaboração de um marco regulatório no Brasil que contemple a eficácia necessária às investigações cibernéticas, sem prejuízo aos direitos fundamentais garantidos pela Constituição. Dessa forma, a pesquisa transcende a simples análise legal, engajando-se em um diálogo profundo com as questões éticas e constitucionais que circundam a prática da infiltração online, propondo um equilíbrio entre a segurança pública e a preservação das liberdades individuais no ambiente digital.

No Brasil, a aplicação dessa técnica tem-se tornado cada vez mais relevante, especialmente em investigações relacionadas a crimes cibernéticos, tráfico de drogas, atividades terroristas e exploração infantil , crimes que, muitas vezes caracterizados pela sua natureza transnacional e pelo anonimato proporcionado pela internet, exigem dos investigadores uma abordagem que vai além dos métodos convencionais. Dessa forma, a infiltração online permite às autoridades adentrar nas camadas mais profundas e obscuras da internet, viabilizando o acesso a informações e a coleta de evidências que, de outra forma, permaneceriam inacessíveis.

A evolução e a ampla adoção da internet e das tecnologias associadas têm transformado significativamente o panorama do direito processual penal. Por um lado, essa transformação digital tem facilitado novas formas de criminalidade, originando crimes que são exclusivamente cometidos no ambiente virtual, além de ampliar as possibilidades para a realização de atos criminosos tradicionais por meio de ferramentas digitais. Por outro lado, observa-se um interesse cada vez maior por parte das autoridades em explorar essas mesmas tecnologias digitais para aprimorar as estratégias de prevenção e combate ao crime. É nesse cenário que reflete uma dualidade na qual a tecnologia, ao mesmo tempo em que se apresenta como um vetor para novas modalidades de crime, também emerge como um recurso valioso nas mãos do Estado para efetivar a justiça e a segurança pública.

No entanto, o uso da infiltração online não está isento de desafios, questões de privacidade e direitos individuais surgem como pontos críticos nessa discussão, bem como a prática levanta inúmeros questionamentos sobre até que ponto é possível equilibrar a necessidade de eficácia da investigação criminal com o respeito aos direitos fundamentais dos indivíduos. Esse equilíbrio delicado entre eficácia investigativa e respeito aos direitos humanos torna-se ainda mais complexo quando consideramos o papel emergente da inteligência artificial nas técnicas de infiltração online.

Nesse contexto, o estudo de Luís Greco configura-se especialmente relevante ao examinar a experiência alemã. Esse doutrinador não apenas descreve como a infiltração online é regulamentada e aplicada em um contexto jurídico diferente, mas, também, aborda a integração da inteligência artificial nessas operações, possibilitando uma perspectiva valiosa, que auxilia na compreensão das potencialidades e limitações da infiltração online, além de fornecer *insights* importantes sobre como essa prática pode ser implementada de maneira responsável e ética.

O presente artigo tem como objetivo não apenas elucidar os aspectos técnicos e legais da infiltração online no Brasil, mas, também, promover uma reflexão crítica sobre as implicações mais amplas dessa experiência no cenário da justiça penal, contribuindo para o debate jurídico e acadêmico, proporcionando uma análise que vai além dos contornos puramente legais, debruçando-se sobre as ramificações éticas, sociais e tecnológicas dessa prática na era digital.

2 Experiência alemã em infiltração online: um estudo de caso

A Alemanha se destaca como um país pioneiro na regulação da infiltração online com a promulgação da Lei de Combate ao Terrorismo (*Gesetz zur Bekämpfung des Terrorismus* ou GBL), em 2006, estabelecendo um marco legal significativo na segurança cibernética. Essa legislação autoriza e regula minuciosamente o uso da infiltração online para investigar atividades terroristas e outras formas graves de criminalidade, evidenciando o compromisso alemão em adaptar as estratégias de segurança nacional ao ambiente digital e seus desafios únicos.

De acordo com a legislação alemã, a autorização da infiltração online está sujeita a critérios rigorosos para assegurar que essa medida intrusiva seja aplicada de maneira justa e proporcional. Isso inclui a necessidade de haver indícios substanciais de atividades criminosas sérias, garantindo que tais operações sejam reservadas para circunstâncias excepcionais. Além disso, é imperativo que outras abordagens investigativas tenham sido consideradas inadequadas ou ineficazes, ressaltando a natureza intrusiva dessa técnica como último recurso.

Inicialmente, tentativas de aplicar essa técnica investigativa foram baseadas em interpretações extensivas ou análogas de três disposições legais do sistema jurídico alemão: a legislação referente à apreensão de objetos para investigação (§ 94 do Código de Processo Penal Alemão – *Strafprozessordnung*, StPO), as regras sobre buscas domiciliares (§ 102 StPO) e a legislação que regula o monitoramento de comunicações (§ 100a StPO).

O *Bundesgerichtshof*, equivalente ao Superior Tribunal de Justiça no Brasil, confrontou essas questões pela primeira vez em 2007, concluindo que não existia base legal para a invasão de sistemas computacionais e que analogias com outras normas também não eram aplicáveis. Essencialmente, determinou-se que acessar dados armazenados em computadores representava uma grave violação ao direito fundamental à autodeterminação informacional, um princípio já reconhecido pelo Tribunal Constitucional Federal Alemão, desde 1983, derivado do direito ao livre desenvolvimento da personalidade e da dignidade humana, conforme estipulado na Lei Fundamental da Alemanha (*Grundgesetz* – GG).

As disposições legais sobre buscas domiciliares, que tradicionalmente contemplam intervenções físicas e não virtuais, foram consideradas inaplicáveis, pois baseiam-se no princípio da publicidade, que obriga a notificação e a permissão do investigado para acompanhar a busca em sua residência. Da mesma forma, as leis que autorizam intervenções ocultas ou o monitoramento de comunicações foram julgadas insuficientes para cobrir a amplitude das operações de infiltração online, que visam à coleta abrangente de dados armazenados em dispositivos eletrônicos, indo além da mera interceptação de comunicações.

Nesse cenário, o tribunal expressou a necessidade de uma legislação específica que autorizasse expressamente a infiltração online, atendendo a rigorosos critérios de intervenção nos direitos fundamentais. Essa demanda por uma base legal específica levou ao desenvolvimento posterior na legislação alemã. Paralelamente à decisão do BGH, o Estado alemão da Renânia do Norte-Vestfália introduziu, em sua Lei de Proteção à Constituição de 2006, uma disposição que autorizaria tal medida, embora focada no contexto de inteligência estatal e não no processo penal. Essa abordagem distinta entre a persecução penal e a coleta de inteligência reflete o princípio da separação entre as atividades de investigação criminal e as operações de inteligência, uma salvaguarda essencial contra abusos estatais.

Posteriormente, o Tribunal Constitucional Federal Alemão, ao revisar essa legislação em 2008, estabeleceu um novo direito fundamental, garantindo a confiabilidade e integridade dos sistemas informáticos, derivado do direito geral à personalidade. Isso levou à criação de uma norma autorizativa específica para a infiltração online na Lei Federal de Polícia Criminal (*Gesetz über das Bundeskriminalamt*, BKA-Gesetz) em 2008, posteriormente examinada e considerada parcialmente constitucional pelo Tribunal em 2016.

Em 2017, foi introduzida uma norma específica no Código de Processo Penal Alemão (§ 100b StPO), permitindo a infiltração online como medida de investigação no processo penal, cuja constitucionalidade está atualmente sob nova avaliação pelo Tribunal Constitucional Federal. Esse desenvolvimento legislativo reflete o cuidadoso equilíbrio que o direito alemão procura manter entre a eficácia das investigações criminais e a proteção dos direitos fundamentais, enfatizando a necessidade de uma base legal clara e específica para intervenções tão invasivas quanto à infiltração online.

A operação também deve ser direcionada para proteger a vida ou a integridade física dos cidadãos, sublinhando a priorização da segurança e do bem-estar dos indivíduos. Finalmente, deve haver uma análise cuidadosa da proporcionalidade e relevância da infiltração no contexto específico, garantindo sua diretiva pertinente à investigação.

A supervisão do Poder Judiciário sobre a infiltração online na Alemanha assegura a adesão aos princípios do Estado de direito, estabelecendo um pilar para a conformidade legal das operações. Os agentes responsáveis pela execução dessas operações estão submetidos a restrições significativas, visando prevenir abusos e proteger os direitos fundamentais.

Essas restrições englobam a proibição de criar identidades falsas, visando manter a transparência; a vedação à indução de atividades criminosas, reforçando o princípio de que o Estado não deve facilitar ou promover a criminalidade; e a exigência de manter registros detalhados das atividades, possibilitando revisões e auditorias para garantir a integridade das operações.

Dessa forma, podemos afirmar que a experiência da Alemanha com a infiltração online oferece um exemplo valioso para outras nações que buscam navegar sobre o equilíbrio entre eficácia na prevenção do crime online e a proteção dos direitos individuais. Sua legislação é louvada por sua estabilidade, permitindo investigações eficazes enquanto institui salvaguardas robustas contra excessos e abusos. Isso sublinha a necessidade de uma abordagem legislativa cuidadosamente ponderada e estruturada para enfrentar os desafios impostos pelo ciberespaço, enfatizando a importância de conciliar segurança, privacidade e direitos humanos na era digital.

A discussão em torno da infiltração online pelo Estado alemão, iniciada por volta de 2006, revela um panorama complexo de desafios éticos, legais e tecnológicos enfrentados no combate à criminalidade na era digital. A jurisprudência alemã, em especial a decisão do *Bundesgerichtshof* (BGH), de 2007, marcou um ponto de inflexão ao enfatizar a ausência de uma base legal clara para a invasão de dispositivos informáticos, destacando a necessidade de proteger o direito fundamental à autodeterminação informacional.

Essa preocupação com a privacidade digital não se limitava apenas à busca por uma autorização legal para tais intervenções, mas, também, ao reconhecimento do impacto profundo que a vigilância estatal pode exercer sobre a liberdade individual. O BGH, ao rejeitar as tentativas de justificar a infiltração online com base em leis existentes, não apenas destacou a insuficiência dessas normas para abordar a complexidade das questões envolvidas, mas, também, sublinhou a importância da transparência, da proporcionalidade e da proteção dos direitos individuais em operações de vigilância.

A subsequente decisão do Tribunal Constitucional Federal Alemão (BVerfG), que estabeleceu o direito à garantia da confiabilidade e integridade dos sistemas informáticos, reflete uma profunda compreensão dos desafios únicos impostos pela era digital ao direito à privacidade e à liberdade individual. Ao criar um novo direito fundamental, derivado do direito geral de personalidade, o BVerfG não apenas forneceu uma base jurídica para regulamentar a infiltração online, mas, também, estabeleceu um precedente importante para a proteção dos indivíduos contra intervenções estatais em seus sistemas informáticos.

Essa evolução jurídica na Alemanha ilustra um esforço significativo para equilibrar a necessidade de segurança e a eficácia na investigação de crimes com os direitos fundamentais dos indivíduos. A implementação de salvaguardas legais e procedimentais, como a exigência de uma autorização judicial e a proteção do núcleo da esfera privada, demonstra um compromisso em manter essa balança equilibrada.

A influência dessa jurisprudência estende-se além das fronteiras alemãs, servindo como um modelo para outros países que buscam atualizar suas leis e práticas de vigilância para enfrentar os desafios da criminalidade digital. Ao mesmo tempo, a decisão do BVerfG sobre a infiltração online abre caminho para debates mais amplos sobre a intersecção entre tecnologia, direito e ética, especialmente no que diz respeito ao uso de inteligência artificial e outras tecnologias emergentes na aplicação da lei.

Enquanto aguardamos novas decisões e desenvolvimentos legislativos, tanto na Alemanha quanto em outros países, o debate sobre a infiltração online e a vigilância estatal continua evoluindo. Questões sobre como garantir a segurança pública sem comprometer os direitos fundamentais, como adaptar as leis às tecnologias em rápida mudança e como proteger a privacidade em um mundo cada vez mais conectado permanecem no centro das discussões.

Ao proporcionar um quadro legislativo que regula meticulosamente a prática da infiltração online, a Alemanha não apenas facilita as investigações em um domínio complexo como o ciberespaço, mas, também, reafirma seu compromisso com a preservação dos direitos fundamentais e a privacidade, oferecendo um caminho a seguir para países em busca de atualizar suas políticas de segurança e práticas investigativas para refletir as realidades da sociedade digital moderna.

3 Implicações éticas da infiltração online

As implicações éticas da infiltração online são complexas e controversas. Por um lado, a infiltração online pode ser uma ferramenta eficaz para investigar crimes graves, que ameaçam a segurança pública. Por outro lado, a infiltração online pode representar uma violação da privacidade e dos direitos individuais dos usuários da internet.

A respeito das implicações éticas da infiltração online, Luís Greco (2022, p. 25) afirma que:

> A infiltração online é uma técnica de investigação que apresenta um elevado potencial de violação dos direitos fundamentais, em especial da privacidade e da liberdade de expressão. Por isso, deve ser utilizada com cautela e apenas em situações excepcionais, quando não houver outras alternativas para a obtenção de informações relevantes para a investigação.

A atuação dos agentes públicos no contexto da infiltração online é um campo delicado que requer uma observância rigorosa de limites éticos e constitucionais, estabelecidos para proteger os direitos individuais dos usuários da internet e assegurar a legalidade e a moralidade das operações conduzidas pelo Estado. Essa prática, embora necessária no combate a crimes virtuais, deve ser circundada por um quadro de salvaguardas que garantam o respeito aos princípios fundamentais de privacidade e direitos humanos.

Um dos pilares fundamentais dessa regulamentação é a necessidade de autorização judicial prévia para a realização de qualquer operação de infiltração online. Essa autorização deve ser embasada em justificativas concretas e aderentes aos requisitos legais, garantindo que a medida seja empregada de maneira proporcional e adequada à gravidade do crime investigado. A lei estipula que essa ferramenta investigativa não deve ser utilizada em circunstâncias leves ou para a coleta de informações irrelevantes para o caso em questão, respeitando o princípio da proporcionalidade em todas as instâncias.

Adicionalmente, enfrenta-se no Brasil desafios significativos na implementação da infiltração online, principalmente pela necessidade de atualização da legislação vigente. A Lei 12.850/2013, que trata das organizações criminosas e estabelece procedimentos para a obtenção de provas, é considerada por muitos como insuficiente para abordar a complexidade e as especificidades da infiltração online. Do mesmo modo, o papel do Poder Judiciário na supervisão e regulação dessa prática requer clarificações, para assegurar uma fiscalização efetiva que proteja os direitos dos cidadãos, que paralelamente, a influência crescente da inteligência artificial (IA) na infiltração online apresenta um potencial transformador, oferecendo eficiência e eficácia aprimoradas na identificação de atividades suspeitas e na coleta de dados relevantes.

Conforme elucida, no caso brasileiro, Luís Greco (2019)

> Seria necessário apenas esclarecer a razão específica pela qual ela precisa ser expressamente prevista, concretamente: em qual dos direitos previstos no art. 5º da CF ela intervém? Trata-se de intervenção no âmbito de proteção do art. 5º, X, que declara "invioláveis a intimidade, a vida privada ... das pessoas", ou do art. 5º, XII, que também qualifica de "inviolável o sigilo de dados"? Ou há necessidade de recorrer a um novo direito fundamental não-escrito relativo à confiabilidade e integridade dos sistemas informáticos? Tendemos para essa última posição (Greco; Gleizer, 2019, p. 1.497).

No entanto, essa mesma tecnologia traz consigo desafios consideráveis, especialmente a necessidade de manter um controle humano efetivo sobre as operações automatizadas, para prevenir violações de privacidade e assegurar a aderência aos direitos individuais, bem como recomenda-se uma série de medidas para aprimorar a prática da infiltração online no Brasil.

Primeiramente, é imperativo que a legislação seja revisada e atualizada, para definir claramente os limites, requisitos e procedimentos para a realização dessa atividade. Além disso, o Poder Judiciário deve assumir um papel ativo na supervisão dessas operações, garantindo a proteção dos direitos fundamentais dos cidadãos. A regulamentação do uso da IA em contextos de infiltração online também se faz necessária, estabelecendo diretrizes que garantam o equilíbrio entre eficácia investigativa e respeito aos direitos humanos.

Assim sendo, enquanto a infiltração online mostrar-se uma ferramenta valiosa para o combate à criminalidade no ambiente digital, sua concretização requererá uma abordagem cautelosa e responsável. A criação de um marco regulatório robusto, que contemple tanto as inovações tecnológicas quanto os imperativos éticos e legais, é essencial para promover a segurança pública sem comprometer os direitos e liberdades individuais, visto que

> [...] Se quisermos dotar as nossas instâncias persecutórias de uma faculdade de intervir nesse direito, precisaremos, assim, de lei específica que a fundamente (e não apenas a regule). Enquanto inexistir essa lei, o acesso ao conteúdo de sistemas informáticos terá de ocorrer através das medidas da busca e da apreensão do dispositivo físico em que esse conteúdo se encontra armazenado (Greco; Gleizer, 2019, p. 1.498).

4 O processo penal alemão e a infiltração online

A introdução do § 100b no Código de Processo Penal alemão (StPO) em julho de 2017 marca um avanço significativo nas metodologias de investigação penal na Alemanha, refletindo uma adaptação legislativa às complexidades emergentes trazidas pela era digital. Esse capítulo do código, projetado para regular a infiltração online por autoridades investigativas, baseia-se nas premissas estabelecidas pelo Tribunal Constitucional Federal da Alemanha (BVerfG), delineando um conjunto rigoroso de critérios e salvaguardas que buscam equilibrar a eficácia da investigação criminal com a proteção dos direitos fundamentais dos indivíduos.

A legitimação da infiltração online como técnica investigativa é criteriosamente circunscrita pelo legislador alemão, exigindo a presença de uma suspeita bem fundamentada na legislação alemã que reconhece diferentes níveis de suspeita (suspeita inicial, suspeita forte e suspeita suficiente), cada uma correspondendo a uma fase específica do processo investigativo. A infiltração online, por sua natureza invasiva, demanda uma justificativa baseada em uma suspeita que excede a mera iniciação de uma investigação, necessitando de indícios substanciais que apontem para a probabilidade significativa de que um crime tenha sido cometido, sendo que essa suspeita não deve ser fruto de conjecturas ou generalizações, mas, sim, de evidências concretas e particularizadas relacionadas ao caso em questão.

A aplicação dessa medida é restrita a um catálogo predefinido de crimes considerados especialmente graves, refletindo a intenção do legislador de reservar a infiltração online para casos de extrema importância. Esse catálogo, estipulado pelo Tribunal Constitucional, inclui crimes que ameaçam bens jurídicos de suma importância, tais como a vida, a liberdade física, a segurança do Estado. Da mesma forma, a inclusão de um delito na referida relação não apenas sinaliza sua gravidade abstrata, mas, também, impõe ao Judiciário a tarefa de avaliar sua gravidade concreta no contexto específico da investigação.

A normativa alemã estabelece a infiltração online como um recurso subsidiário, o qual só pode ser empregado quando outros métodos investigativos forem considerados inviáveis ou significativamente menos eficazes. Esse princípio da subsidiariedade é uma manifestação direta do respeito ao direito à privacidade e à integridade informacional dos indivíduos, garantindo que a medida invasiva seja vista como último recurso.

A proporcionalidade da medida, avaliada tanto pelo legislador quanto pelo aplicador da lei, exige uma minuciosa análise de sua justificação e eficácia em relação ao impacto sobre os direitos dos indivíduos envolvidos. Aspectos como a quantidade de informações não relacionadas ao caso que podem ser inadvertidamente coletadas e a temporalidade entre o ato investigado e a aplicação da medida são cruciais nessa avaliação.

5 Impacto sobre terceiros

Um aspecto notável da legislação é a consideração dos efeitos da infiltração online sobre terceiros não relacionados à investigação, reconhecendo que sistemas informáticos modernos frequentemente contêm dados sobre múltiplos usuários, a lei permite, em certas condições, a infiltração de dispositivos pertencentes a terceiros, desde que haja uma conexão direta com o investigado. Essa previsão legal busca abordar a realidade de que criminosos podem utilizar dispositivos de terceiros para ocultar suas atividades, ao mesmo tempo que estabelece salvaguardas para minimizar a intrusão em vidas de indivíduos inocentes, conforme enfatizam Greco e Gleizer (2019): "A utilização da infiltração online deve ser ponderada com cuidado, levando em consideração a gravidade do crime, a efetividade da medida e o impacto sobre os direitos fundamentais dos indivíduos envolvidos".

No arcabouço legal alemão, a inclusão do § 100b no Código de Processo Penal não apenas codificou os pressupostos para a utilização da infiltração online nas investigações penais, mas, também, estabeleceu um conjunto robusto de salvaguardas destinadas a proteger os direitos dos indivíduos durante a execução de tais medidas, o que desenvolve e reflete um esforço legislativo cuidadoso para equilibrar as necessidades investigativas do Estado com os direitos fundamentais dos cidadãos à privacidade e à proteção de dados.

> A infiltração online é uma ferramenta poderosa que pode ser utilizada para combater crimes graves, mas sua aplicação deve ser cuidadosamente regulamentada para evitar abusos e garantir a proteção dos direitos fundamentais (BVerfG, 2017).

Para mitigar os riscos inerentes à infiltração online, o legislador impôs exigências rigorosas para a execução da medida, enfatizando a minimização da intrusão e a prevenção do acesso desautorizado a dados por terceiros. Essas precauções técnicas exigem que as ferramentas utilizadas na infiltração sejam projetadas para reverter automaticamente qualquer alteração feita no sistema do investigado após a conclusão da medida. Além disso, medidas adicionais devem ser tomadas para garantir que dados coletados durante a operação sejam armazenados de maneira segura, inacessíveis a indivíduos não autorizados, sejam eles internos à força tarefa investigativa ou externos.

Assim sendo, a transparência e a responsabilidade garantem o registro meticuloso de informações pertinentes à operação. São mandatórios, incluindo, nesse rol, os detalhes sobre as ferramentas técnicas empregadas, os sistemas visados, alterações efetuadas que não sejam meramente transitórias e os dados especificamente acessados ou coletados. Esses registros não apenas possibilitam uma avaliação subsequente da proporcionalidade e da legalidade da medida, mas servem como um meio de atribuir responsabilidades pelos atos realizados durante a execução da infiltração.

O direito alemão estabelece explicitamente a inadmissibilidade da infiltração online em situações onde prevaleça a expectativa de que informações pertencentes ao núcleo da esfera privada do indivíduo sejam as únicas a serem obtidas. Essa disposição visa a proteção dos espaços mais íntimos e pessoais da vida do indivíduo, reconhecendo que tais esferas devem permanecer invioláveis, mesmo diante de investigações criminais. Ademais, há uma obrigatoriedade de que, sempre que tecnicamente possível, seja evitada a coleta de dados pertencentes a esse núcleo privado, e, na eventualidade de sua coleta inadvertida, que tais dados sejam prontamente eliminados ou submetidos a uma avaliação judicial quanto à sua admissibilidade como prova.

As disposições legais também contemplam a possibilidade de que terceiros sejam afetados pela medida de infiltração. Nesse contexto, a legislação estipula critérios específicos para quando sistemas de terceiros, que podem ser utilizados pelo investigado, tornam-se alvos legítimos da infiltração. Essa nuance legal reconhece as complexidades das redes sociais e de comunicação modernas, onde a distinção entre os dispositivos do investigado e de terceiros pode afigurar-se tênue, assim como a proteção estendida a terceiros visa minimizar o impacto da medida sobre indivíduos não relacionados à investigação, preservando assim o respeito aos direitos de todos os envolvidos.

No debate sobre os procedimentos de proteção de dados, o legislador alemão enfatiza a importância da gestão e da proteção de dados pessoais coletados durante a infiltração online, o que envolve a identificação precisa dos dados coletados, a notificação obrigatória ao indivíduo afetado sobre a medida executada e a eliminação imediata de dados que não sejam mais necessários para os fins da investigação ou para um subsequente controle judicial. Essas etapas asseguram que os dados pessoais sejam manuseados com o máximo cuidado e respeito pela privacidade individual, alinhando-se aos princípios de minimização de dados e responsabilidade.

> Em primeiro lugar, a constitucionalidade da infiltração online é questionada em razão da amplitude do catálogo de fatos. Em sua decisão de 2008, o BVerfG estabeleceu que o emprego da infiltração online só seria justificável em razão de perigos concretos para bens jurídicos extremamente importantes, que seriam o corpo, a vida, a liberdade e outros bens importantes para a coletividade, cuja ameaça colocaria em risco as bases ou a subsistência do Estado de direito ou as bases da existência dos seres humanos. Do extenso catálogo de fatos constam, no entanto, crimes que, na visão dos reclamantes, não protegem tais bens jurídicos: entre outros, a falsificação de moeda, a lavagem de dinheiro, a corrupção e a receptação (Greco; Gleizer, 2019, p. 1.510).

Portanto, a incorporação do § 100b ao Código de Processo Penal alemão representa um marco na legislação penal, trazendo à tona um equilíbrio meticuloso entre as prerrogativas investigativas do Estado e a proteção dos direitos fundamentais dos indivíduos na era digital, assim como as salvaguardas estabelecidas refletem um compromisso com a proteção da privacidade, a segurança dos dados e a integridade dos sistemas informáticos, delineando um modelo legal que poderia servir de referência para outras jurisdições enfrentando desafios semelhantes no âmbito da investigação penal online.

6 A infiltração online e as investigações no Brasil

A utilização de *softwares* maliciosos para fins de investigação está se convertendo em uma prática comum em várias partes do mundo, incluindo países como Estados Unidos, Espanha e Alemanha. No contexto brasileiro, apesar de relatos sobre o interesse das autoridades judiciais no uso de programas de espionagem, ainda não há informações concretas sobre sua efetiva utilização como ferramenta de investigação, isso porque

> [...] A Constituição Federal brasileira de 1988 contém, no rol dos direitos fundamentais, ao menos três incisos relevantes em matéria de limites da vigilância do Estado brasileiro sobre as comunicações. O inciso IV do art. 5º protege a dimensão positiva das comunicações, porquanto garante a liberdade de expressão ("IV – é livre a manifestação do pensamento, sendo vedado o anonimato"). Os incisos X e XII do mesmo artigo, por sua vez, protegem a liberdade negativa sobre as comunicações, ou seja, a faculdade de mantê-las em sigilo ou de ao menos limitar seus destinatários, ao preceituarem o direito à privacidade ("X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação") e o sigilo das comunicações ("XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal") (Antonialli; Abreu, 2022, p. 15).

A implementação de *softwares* maliciosos, ou *malwares*, e outras estratégias de busca de provas online, concede a quem os opera uma vasta gama de funcionalidades, incluindo nesses a capacidade de acessar e transferir arquivos, senhas e outras informações armazenadas em sistemas de computadores para servidores remotos, desvinculados do dispositivo alvo. Além disso, esses programas podem ser utilizados para monitorar e coletar dados sobre as atividades online dos usuários, incluindo os horários de acesso, *sites* e *e-mails* visitados, endereços IP e os tipos de navegadores usados.

A infiltração online e as buscas por meio de *softwares* não se referem a um único tipo, mas sim a um conjunto de ferramentas que variam em função e designação, dependendo de suas características e objetivos. Entre eles, podemos citar os cavalos de troia, bombas lógicas (*logic bombs*), programas espiões (*spyware*), registradores de teclas (*keyloggers*) e de tela (*screenloggers*), kits de raiz oculta (*rootkits*), vermes (*worms*), vírus, ameaças mistas (*blended threats*) e robôs (*bots*). Cada um desses tipos de *malware* tem capacidades específicas, sendo projetados para infiltrar, danificar ou realizar espionagem em sistemas informáticos, sem o conhecimento ou consentimento do usuário.

Eduardo Bolsoni Riboli (2019) caracteriza os programas maliciosos como

> [...] um conjunto de *softwares* concebidos especificamente para coletar dados de um dispositivo eletrônico ou sistema de computador sem a autorização ou o conhecimento do usuário sobre sua instalação e operação. Embora haja uma variedade de *softwares* espiões, cada um com suas funções particulares e, frequentemente, capazes de executar múltiplas tarefas, uma propriedade comum a todos é a habilidade de se ocultarem durante a instalação e o funcionamento, sendo que normalmente, esses programas são ativados por meio de outro *software* que possa parecer útil ou inócuo para o usuário, pelo menos nas fases iniciais de sua execução.

A infiltração online, engloba uma variedade de programas, cada um com funções e características específicas, conhecidos por denominações como cavalos de Tróia, bombas lógicas (*logic bombs*), programas espiões (*spyware*), registradores de teclas (*keyloggers*) e de tela (*screenloggers*), kits de raiz oculta (*rootkits*), vermes (*worms*), vírus, ameaças combinadas (*blended threats*) e robôs automatizados (*bots*). Conforme analisado por Eduardo Bolsoni Riboli, esses programas são projetados para extrair dados de dispositivos eletrônicos ou sistemas informáticos, sem a permissão ou conhecimento dos usuários, mantendo a instalação e operação dessas ferramentas ocultas. Inicialmente, eles podem ser ativados por outro *software* que aparente ser útil ou inofensivo.

Os programas têm a capacidade de serem instalados discretamente em dispositivos ou sistemas, sem alertar o usuário, afetando a funcionalidade do sistema invadido, algumas variantes de *malware*, como k*eyloggers* e *screenloggers*, capturam todas as interações com o teclado, fornecendo ao operador informações sobre as atividades realizadas pelo usuário, outros podem ativar *webcams* e microfones para coletar dados visuais e sonoros do ambiente, enquanto há aqueles capazes de acessar informações de geolocalização em tempo real e monitorar comunicações, inclusive contornando protocolos de criptografia.

É fundamental destacar que esses dispositivos ocultos podem exigir a inserção física em um sistema para sua execução, no entanto, com a evolução tecnológica, a instalação desses programas maliciosos por meios digitais, sem contato físico direto com os dispositivos visados, tornou-se mais comum, utilizando-se, por exemplo, de *e-mails* contendo *links* fraudulentos ou outros métodos de infiltração mal-intencionados.

A adoção de programas mal-intencionados, conhecidos como *malwares*, nas investigações judiciais, ressalta-se pela eficácia notável que esses apresentam em um contexto onde a interação humana com sistemas informáticos torna-se cada vez mais intrínseca no cotidiano. A tendência é fortalecida pelo avanço tecnológico e pelo crescente emprego dos meios digitais em atividades ilícitas, diversos *malwares* e outros programas, em suas diversas formas – desde cavalos de troia e bombas lógicas até programas espiões e registradores de atividade digital –, desbloqueiam um leque amplo de dados e informações que, de outra forma, permaneceriam inacessíveis pelos métodos convencionais de coleta de provas. Essas ferramentas conseguem contornar barreiras significativas, como criptografias e técnicas de anonimato online, permitindo o acesso a elementos cruciais para a investigação de crimes.

Antônio Magalhães Gomes Filho, em sua obra, delineia a utilização de *malware* no âmbito processual penal como uma metodologia investigativa emergente, definindo que tais técnicas, geralmente conduzidas por agentes externos ao Poder Judiciário, como a polícia ou o Ministério Público, caem sob a categoria de procedimentos extraprocessuais regulados pela legislação com o intuito de adquirir provas materiais. No domínio penal, a utilização dessas ferramentas tem como objetivo principal a obtenção de evidências concretas que possam confirmar ou refutar alegações sobre a perpetração de um delito penalmente relevante.

A natureza desses mecanismos de investigação de prova é predominantemente extraprocessual, com abordagens que visam descobrir elementos, dados e informações essenciais para confirmar ou negar a existência de um fato previamente estabelecido, cuja demonstração é pertinente ao processo. Muitas vezes, tais meios de obtenção de prova são singulares e, uma vez adquiridos, são prontamente integrados ao processo judicial, entretanto não é incomum que essas operações sejam executadas por autoridades responsáveis pela investigação inicial de crimes, como menciona Gomes Filho, sublinhando a autonomia investigativa atribuída a esses agentes.

Um aspecto distintivo desses métodos investigativos é a sua realização sem o conhecimento prévio do alvo, incorporando o elemento surpresa para evitar a destruição de evidências ou a continuação de condutas delituosas sob vigilância. Esse *modus operandi*, caracterizado pela ocultação e pela surpresa, é deliberado para prevenir a obstrução do processo investigativo, como observado por Paolo Tonini, que enfatiza a importância do contraditório ser postergado para um momento subsequente à coleta de provas, garantindo a eficácia da diligência.

No entanto,

> [...] nada obstante os benefícios possíveis de advir do *malware* como um novo e poderoso meio de obtenção de prova, a sua operacionalização na seara processual penal enfrenta dúvidas e questionamentos. A primeira delas relaciona-se a uma característica inerente a essa própria técnica probatória, que é o fato de o acesso ao equipamento ou sistema informático ocorrer de modo oculto, sem o prévio conhecimento do seu utilizador (Ribeiro; Cordeiro, 2022, p. 1.470).

Apesar do potencial dos *malwares* em enriquecer o arsenal de ferramentas disponíveis para a obtenção de provas, sua operacionalização no campo processual penal acarreta uma série de dilemas e desafios. A inserção secreta desses programas em sistemas informáticos, permitindo acesso irrestrito a dados e informações do usuário, levanta preocupações sérias sobre privacidade e ética. A vasta gama de funcionalidades desses *softwares*, que vão desde o monitoramento de teclas digitadas até a vigilância de movimentos físicos do usuário, amplia o escopo da investigação mas, também, intensifica as questões relativas à invasão de privacidade.

Dessa forma vemos que,

> A persecução penal pode levar a diversos perigos, como a violação dos direitos fundamentais dos indivíduos, a propagação de informações falsas e a intensificação da cultura do ódio online. Além disso, a persecução pode dificultar o trabalho das autoridades competentes na investigação e punição de crimes (Barbosa, 2020, p. 14).

Ademais, a capacidade desses programas de operar recursos dos dispositivos infectados introduz incertezas sobre a fidelidade dos dados recolhidos, questionando sua validade como evidência. Acrescenta-se a isso a

possibilidade de os esforços de vigilância atingirem sistemas e indivíduos não relacionados à investigação, implicando na coleta indevida de informações de terceiros. Assim sendo, nesse panorama, a necessidade de evoluir os métodos de coleta de provas em resposta às estratégias criminosas cada vez mais sofisticadas e digitalizadas torna-se evidente. O surgimento de tais métodos representa instrumentos potenciais para aprimorar as investigações, ainda que sua aplicação demande uma cuidadosa ponderação entre a eficácia investigativa e a proteção dos direitos fundamentais.

O desafio reside em desenvolver um marco regulatório que harmonize o uso dessas tecnologias invasivas com as garantias constitucionais, assegurando um equilíbrio entre os imperativos de justiça e os princípios de liberdade e privacidade, bem como distinguindo a persecução penal e a infiltração online, visto que

> [...] A persecução penal e a infiltração online são duas faces da mesma moeda. Ambas as práticas envolvem a utilização da internet para investigar e punir crimes. No entanto, a persecução é realizada por indivíduos ou grupos sem autorização legal, enquanto a infiltração online é realizada por agentes de investigação com a devida autorização judicial (Barbosa, 2020, p. 15).

7 Considerações finais

A legislação alemã sobre a infiltração online no processo penal representa um esforço meticuloso para conciliar a necessidade de ferramentas investigativas eficazes na era digital com a proteção dos direitos fundamentais. Ao estabelecer critérios rigorosos e mecanismos de proteção, o § 100b StPO exemplifica uma abordagem ponderada que reflete as complexidades e desafios trazidos pela tecnologia moderna. Enquanto a prática da infiltração online continua a evoluir, a legislação alemã serve como um referencial para o debate global sobre como equilibrar eficácia investigativa e direitos individuais no contexto digital.

A infiltração online é uma ferramenta valiosa para as autoridades no combate a crimes virtuais. No entanto, a infiltração online deve ser utilizada com cautela, respeitando os direitos individuais dos usuários da internet. Assim evidencia-se a crucialidade da infiltração online como ferramenta investigativa no processo penal, abordando a complexidade e as nuances dessa prática sob a lente do estudo pioneiro de Luís Greco. O trabalho desse autor, ao trazer à tona a experiência alemã e a interseção com a inteligência artificial, fornece *insights* valiosos para o contexto brasileiro, destacando-se como uma contribuição fundamental para a compreensão e o debate sobre os limites e as possibilidades da infiltração online na legislação penal.

Greco aponta para a necessidade imperativa de um marco regulatório específico que motive, de forma expressa, a infiltração online, questionando em qual direito fundamental essa intervenção se insere e se há a necessidade de um novo direito fundamental não escrito relativo à confiabilidade e à integridade dos sistemas informáticos, bem como a tendência do autor para esta última posição, a qual enfatiza a singularidade dos desafios impostos pela digitalização e a necessidade de leis específicas que permitam o acesso ao conteúdo de sistemas informáticos de maneira ética e legalmente fundamentada.

A análise de Greco sobre a legislação alemã e sua aplicação no processo penal alemão, especialmente com a introdução do § 100b StPO, ilustra um esforço legislativo para equilibrar eficácia investigativa e proteção dos direitos fundamentais, sendo esse equilíbrio meticuloso entre as prerrogativas investigativas do Estado e a proteção dos direitos individuais, refletindo uma abordagem que poderia servir de modelo para outras jurisdições, inclusive para o Brasil, onde a legislação sobre a infiltração online ainda está em desenvolvimento.

A experiência alemã, conforme elucidada por Greco, demonstra a importância de critérios rigorosos e mecanismos de proteção no empreendimento da infiltração online, garantindo que essa medida intrusiva seja justa, proporcional e reservada para circunstâncias excepcionais. As salvaguardas estabelecidas na legislação alemã, como a exigência de autorização judicial prévia, a proteção do núcleo da esfera privada e a consideração dos efeitos sobre terceiros, oferecem um caminho para a regulamentação responsável e ética da infiltração online.

Conclui-se que, embora a infiltração online represente uma ferramenta investigativa indispensável na era digital, sua práxis requer uma abordagem cuidadosa que equilibre a eficácia na investigação criminal com o respeito aos direitos fundamentais. O estudo de Luís Greco sobre a experiência alemã e a inteligência artificial contribui significativamente para o debate jurídico e acadêmico, fornecendo uma análise abrangente que transcende os

aspectos puramente legais para abordar as implicações éticas, sociais e tecnológicas dessa prática. Ao fazer isso, Greco não apenas esclarece os desafios enfrentados, mas, também, aponta para direções futuras na busca de uma harmonização entre segurança pública e proteção dos direitos individuais no processo penal brasileiro.

Assim, a reflexão trazida por Luís Greco ilumina o caminho para uma legislação brasileira mais adaptada às realidades contemporâneas do cibercrime e da investigação digital. O autor ressalta a importância de uma base legal específica e robusta para a infiltração online, que não apenas autorize, mas, também, regule meticulosamente essa prática, assegurando que os direitos fundamentais sejam preservados em meio ao avanço tecnológico.

A falta de uma legislação específica que contemple os desafios impostos pela digitalização pode resultar em uma zona cinzenta, onde a eficácia das investigações criminais é limitada pela insegurança jurídica. Portanto, suas considerações reforçam a urgência de um debate aprofundado e da elaboração de normas claras que permitam às autoridades brasileiras empregar técnicas de infiltração online de maneira efetiva e constitucional.

A experiência alemã, detalhadamente examinada por Greco, oferece um paradigma valioso para o Brasil, especialmente no que tange à necessidade de salvaguardas que protejam a privacidade e os dados pessoais dos indivíduos. A abordagem alemã, que combina rigor legal com proteções robustas, poderia inspirar o desenvolvimento de um marco jurídico brasileiro que equilibre os imperativos de segurança com a preservação das liberdades civis.

Portanto, a contribuição de Luís Greco vai além da análise jurídica; ela convoca os legisladores, juristas e a sociedade brasileira a refletirem sobre as implicações mais profundas da infiltração online, argumentando por uma legislação que reconheça e responda aos desafios éticos, sociais e tecnológicos apresentados pela vigilância digital, promovendo uma justiça penal que seja ao mesmo tempo eficaz e respeitosa dos direitos humanos.

Reafirma-se assim, a relevância da obra de Luís Greco para o debate sobre infiltração online no Brasil, enfatizando a necessidade de uma legislação inovadora que acompanhe as transformações digitais. Greco nos lembra que, enquanto navegamos pelas águas turbulentas da era digital, é imperativo que as ferramentas de investigação criminal evoluam não apenas em eficácia, mas, também, em conformidade com os princípios éticos e constitucionais que fundamentam a sociedade brasileira, o que se estabelece como um marco essencial para todos aqueles engajados na construção de um processo penal que seja justo, moderno e respeitoso dos direitos fundamentais no contexto da sociedade da informação.

8 Referências

BADARÓ, Gustavo Henrique. *Processo penal*. 2. ed. Rio de Janeiro: Elsevier, 2014.

BÄR, H. Comentário à decisão BVErfGE 120, 274. *Mmr*, p. 325-333, 2008.

BARBOSA, Samyra Santos. Persecução penal na internet: o papel do Ministério Público no combate à justiça pelas próprias mãos. *Revista Brasileira de Ciências Criminais*, v. 2, n. 102, p. 11-24, 2020.

BEUKELMANN, T. Online-Durchsuchung und Quellen-TKÜ. *NJW-Spezial*, p. 440-444, 2017.

BLECHSCHMITT, P. Quellen-TKÜ und Online-Durchsuchung. *StraFo*, p. 361-369, 2017.

BRUNS, C. *In*: HANNICH, J. (coord.). *Karlsruher Kommentar zur Strafprozessordnung*. 8. ed. München: C.H. Beck, 2019. p. 1-1000. v. 1.

CASTELLS, M. *A sociedade em rede*: do conhecimento à política. São Paulo: Paz e Terra, 2001.

CASTRO, Luiz Augusto Sartori de. Busca e apreensão mediante uso de malware. *Boletim IBCCRIM*, São Paulo, v. 21, n. 251, p. 6-8, out. 2013.

DERIN, B.; GOLLA, S. J. Der Staat als Manipulant und Saboteur der IT-Sicherheit. *NJW*, p. 1111-1117, 2019.

FERNANDES, Alice Cristina Galvão. A persecução penal na internet: uma nova forma de justiça privada? *Revista Brasileira de Ciências Sociais*, v. 29, n. 86, p. 113-134, 2014.

GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – notícia sobre a experiência alemã. *Revista Brasileira de Ciências Criminais*, v. 2, n. 101, p. 325-344, 2019.

GUARDIA, Gregório Edoardo R. S. *Meios de busca de provas e inovações tecnológicas penal*: obtenção e tratamento de dados digitais no processo penal. São Paulo: Max Limonad, 2018, p. 285.

MENDES, Laura Schertel. A infiltração online como ferramenta de investigação: desafios e perspectivas. *Revista Brasileira de Segurança Pública*, v. 7, n. 2, p. 145-164, 2013.

SILVA, Guilherme Soares da. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. *Revista Brasileira de Direito Constitucional*, v. 25, n. 102, p. 345-364, 2019.

SOUZA, José Maria de. A persecução penal na internet: um estudo sobre a justiça pelas próprias mãos no mundo virtual. *Revista Brasileira de Direito Eletrônico*, v. 10, n. 2, p. 456-478, 2012.