A (I)LEGALIDADE DA UTILIZAÇÃO DE *SOFTWARES* PARA INFILTRAÇÃO INFORMÁTICA NAS INVESTIGAÇÕES CRIMINAIS

THE (IL)LEGALITY OF USING SOFTWARE FOR HACKING COMPUTER IN CRIMINAL INVESTIGATIONS

João Conrado Blum Júnior
Mestre em Direito Constitucional pela Universidade de Lisboa.
Promotor de Justiça no Ministério Público do Estado do Paraná.
E-mail: jcblumjr@gmail.com

Luís Gustavo de Souza Timossi
Pós-graduado em Direito Processual Penal e Prática Forense Penal pela Universidade Estadual de Ponta Grossa (UEPG).
Delegado de Polícia Civil no Estado do Paraná.
E-mail: delegadotimossi@gmail.com

Recebido em: 18/7/2024 | Aprovado em: 31/7/2024

Resumo: O presente artigo objetiva analisar a legalidade da utilização de *softwares* para infiltração informática em dispositivos eletrônicos durante investigações criminais, à luz do direito à privacidade, ao sigilo de correspondência, à inviolabilidade do domicílio, à confidencialidade, à imagem, à palavra e à integridade de sistemas de informação estabelecidos pelo artigo 5º, incisos X, XI e XII, da Constituição Federal. A utilização de *softwares* para infiltração, ainda não regulamentada no Brasil, traz questões éticas e legais pertinentes ao direito à privacidade e ao devido processo legal. Com base no estudo de jurisprudência, com análise de julgados e pesquisa bibliográfica e legislativa, o estudo debate a necessidade de regulamentação específica, que garanta equilíbrio entre a efetividade das investigações e a preservação dos direitos fundamentais.

Palavras-chave: Privacidade. Sigilo de correspondência. Infiltração informática. *Hacking*. *Malware*.

Abstract: *This paper aims to analyze the legality of using software for computer*

hacking in electronic devices during criminal investigations in light of the right to privacy, confidentiality of correspondence, inviolability of the domicile, confidentiality, image, word, and integrity of information systems established by Article 5, paragraphs X, XI, and XII, of the Federal Constitution of Brazil. The use of software for computer hacking, not yet regulated by current legislation, raises ethical and legal questions related to the right to privacy and due process of law. Based on a study of case law, with analysis of court decisions and bibliographical and legislative research, the study discusses the need for specific regulation, aiming to strike a balance between the effectiveness of criminal investigations and the preservation of the fundamental rights.

***Keywords**: Privacy. Confidentiality of correspondence. Computer infiltration. Hacking. Malware.*

INTRODUÇÃO

A rápida evolução da tecnologia digital tem transformado a forma de viver, comunicar-se e interagir na sociedade, proporcionando inúmeras facilidades, mas também suscitando desafios éticos e legais. Nesse contexto, emerge a necessidade premente de se reavaliar e compreender a fronteira entre avanços tecnológicos e direitos fundamentais, especialmente no âmbito das investigações criminais. Assim, com este trabalho propõe-se analisar profundamente a legalidade da utilização de *softwares* para infiltração informática em dispositivos eletrônicos durante investigações criminais, sob a luz dos princípios constitucionais que garantem a privacidade, o sigilo de correspondência, a inviolabilidade do domicílio, a confidencialidade, a imagem, a palavra e a integridade dos sistemas de informações, consagrados no artigo 5º, incisos X, XI e XII, da Constituição Federal.

Esta pesquisa se fundamenta na análise detalhada da norma constitucional, que estabelece requisitos rigorosos para a violação do sigilo das comunicações, exigindo não apenas uma ordem judicial específica, mas também a observância das hipóteses e formas estabelecidas pela lei, com a finalidade exclusiva de investigação criminal ou instrução processual penal. Um dos aspectos cruciais do estudo consiste na exploração meticulosa das

técnicas de infiltração informática, notadamente das práticas de *hacking* e do uso de *malware*, por meio da delimitação de suas funcionalidades e distinções. Para embasar a pesquisa, recorre-se a estudos especializados que analisam pormenorizadamente o funcionamento desses métodos de infiltração.

É imperativo observar que a utilização de *softwares* para infiltração informática, até o momento, carece de regulamentação específica na legislação vigente. Essa lacuna levanta questionamentos éticos e legais pertinentes ao direito à privacidade e ao devido processo legal, fundamentais em uma sociedade democrática. A presente abordagem crítica e analítica visa contribuir para o debate em torno da urgente necessidade de regulamentação específica para a utilização dessas tecnologias pelas autoridades encarregadas das investigações criminais.

Busca-se, assim, que se estabeleça um equilíbrio entre a efetividade das investigações e a preservação dos direitos fundamentais dos cidadãos, garantindo que os avanços tecnológicos não aconteçam às custas da proteção das liberdades individuais. Este estudo não apenas explora os desafios contemporâneos enfrentados no campo do direito digital, mas também oferece reflexões sobre como a sociedade pode se adaptar e se regulamentar diante do cenário complexo das tecnologias de infiltração informática em investigações criminais.

1. METODOLOGIA DE INFILTRAÇÃO NAS INVESTIGAÇÕES INFORMÁTICAS

Discutir a utilização de *softwares* para infiltração informática nas investigações criminais é de extrema relevância, especialmente diante das rápidas evoluções tecnológicas que têm transformado a maneira como as autoridades conduzem suas operações. O estudo das técnicas de *hacking* e uso de *malware* aprofunda a compreensão sobre a complexidade desse cenário.

A diferenciação entre *hacking* e *malware* permite que se entendam as nuances desses métodos de infiltração. Enquanto o *hacking* envolve o acesso remoto não autorizado via internet, o *malware* refere-se a programas

maliciosos, instalados clandestinamente em sistemas eletrônicos, que permitem o acesso remoto às informações contidas nesses dispositivos. A capacidade do *malware* de criar portais de acesso ocultos (*backdoors*) representa uma intrusão significativa na privacidade dos indivíduos, pois possibilita o monitoramento em tempo real de diversas funcionalidades dos dispositivos-alvo.

É importante notar que tanto o *hacking* quanto o uso de *malware* nas investigações conferem aos centros de comando um controle remoto abrangente, ao permitirem a captura de dados sensíveis, como senhas, documentos, correios eletrônicos e históricos de navegação. Além disso, esses métodos têm a capacidade de burlar mecanismos de segurança, como antivírus e criptografia de mensagens, o que representa um desafio significativo para a proteção da privacidade dos usuários.

Em didático texto de sua dissertação de mestrado — "*Malware* do Estado e processo penal: a proteção de dados informáticos face à infiltração por *software* na investigação criminal" —, o professor Carlos Hélder Carvalho Furtado Mendes ensina:

> As espécies de infiltração informática derivam de técnicas ocultas de intrusão à distância em sistemas mediante a utilização ou não de *softwares*. Embora sejam metodologias similares em suas funcionalidades investigativas, o "*Hacking*" e o uso de *Malware* pelo Estado se diferenciam justamente pelo fato de que a primeira não se procede mediante a instalação de *software* em dispositivos informáticos, se tratando de um "acesso remoto não autorizado" possível e vinculado à utilização da *internet*. Por tal aspecto é limitado ao período de conexão, o que diferencia substancialmente as duas espécies. *Malware*, em definição simples, refere-se a um programa malicioso instalado clandestinamente por terceiro em um sistema de processamento, uma ameaça destinada a quebra da confidencialidade e integralidade dos dados nele contidos**. Trata-se de um *software* previamente programado cuja função é infectar dispositivos eletrônicos (*smartphone*, *tablet* ou *PC*) para tornar possível o acesso remoto às informações, comunicações ou arquivos neles armazenados ou acessar suas funcionalidades (áudio, vídeo, *e-mail*, câmera, *web* e etc** [sic]**) independentemente de estarem ativas ou não.** Na visão de Ortiz Pradrillo [sic] e Torre quando utilizado pelo Estado se trata de instrumento sofisticado,

> um programa informático utilizado por agentes estatais que possui capacidade de interceptação e gravação em tempo real de dados transmitidos, recebidos ou armazenados em equipamentos eletrônicos. [...] cria-se um portal de acesso (*backdoor*) que possibilita uma comunicação oculta e remota entre o dispositivo monitorado e o centro de comando. *Backdoors* são formas ocultas de acessar o sistema do computador infectado de maneira remota, enviando os mecanismos de autenticação existente [sic], possibilitando assim, que o terceiro – investigador – acesse informações (como senhas e *logins*) ou monitore as atividades do usuário do sistema alvo infectado. Tanto o recurso *hacking* como a utilização de *malware* nas investigações permitem ao centro de comando um posicionamento à distância do dispositivo alvo, um controle remoto capaz de realizar de maneira oculta o monitoramento em tempo real, do áudio, vídeo, das funções de microfone e câmeras, do fluxo de dados e comunicações, da memória e armazenamento, da geolocalização do dispositivo móvel alvo dentre outras funcionalidades por vezes disponíveis. [...] Pois bem, a sistematização de todos as funcionalidades destacadas acima, em um controle ordenado somente é possível mediante o uso de um *software* pré-programado destinado a tal objetivo. Um "sistema de controle remoto" que inclusive possibilita aos investigadores o acesso a senhas de usuários do sistema informático alvo, documentos, correio eletrônico, histórico de páginas *web*, ou seja todos os acessos disponíveis a partir do dispositivo informático alvo, de modo a reduzir dificuldades na obtenção de material probatório que sirva na identificação de *fontes* provas[1, p. 34] (grifo nosso).

Conforme se verifica, embora ambas as técnicas permitam o monitoramento remoto e a coleta de informações, trata-se de técnicas distintas.

2. DISTINÇÃO ENTRE A INTERCEPTAÇÃO TELEFÔNICA PREVISTA NA LEI 9.296/96 E A UTILIZAÇÃO DE *MALWARE*

Caracterizados os métodos de "infiltração" em computadores, é essencial distinguir entre a utilização de *malware* na investigação criminal e a interceptação de comunicação na forma prevista na Lei 9.296/96, a Lei de Interceptação Telefônica.

A interceptação de comunicações, tanto telefônicas quanto telemáticas, envolve a captação do conteúdo de uma conversação ou comunicação em curso entre duas ou mais pessoas, com o propósito de obter informações relevantes para a investigação de um fato ilícito. Nesse contexto, as atividades de interceptação regulamentadas pela legislação são realizadas externamente aos sistemas informáticos, mantendo uma distância razoável da fonte emissora/receptora das informações. Em tal modalidade, de forma simplória, é possível dizer que há a captação em tempo real de dados, que são fornecidos e decifrados pelas operadoras, sem que haja interação do investigador. Para Mendes:

> O que ocorre é a restrição da comunicabilidade, da intimidade e vida privada, da pessoa alvo da interceptação, cujo terceiro autorizado pelo Estado – como fantasma – passa a acompanhar os passos do sujeito que se investiga[1].

Por outro lado, a infiltração por *malware* representa uma forma mais invasiva de investigação, pois ocorre diretamente nos dispositivos informáticos alvo. Ao infiltrar-se no sistema, o *malware* permite a captura de dados internamente após sua decodificação nos dispositivos, aos quais possibilita acesso amplo e irrestrito. Isso transforma uma interceptação passiva em uma captura ativa de dados. Mendes explica que:

> O *malware* a serviço da investigação não incide no fluxo comunicacional que se encontra por vezes protegido pela técnica criptográfica, mas transforma aquela interceptação passiva em "ativa" (*intercettazioni attive*), na medida em que permite a interceptação da informação após sua decodificação internamente nos dispositivos informáticos. Em suma, a utilização do *malware* transforma a interceptação do fluxo da informação em uma captura dos dados receptados pelo dispositivo alvo[1, p. 140].

A comparação entre as definições apresentadas delineia claramente as diferenças fundamentais entre as duas modalidades de interceptação, destacando o caráter intrusivo e desafiador das infiltrações por *malware*, que representam uma ameaça direta à integridade do sistema informático e, por consequência, ao direito fundamental à privacidade dos usuários.

3. (IN)ADMISSIBILIDADE DO USO DE *MALWARE* PARA FINS DE INVESTIGAÇÃO CRIMINAL

O cerne da discussão reside na ausência de legislação específica que regule e autorize de maneira inequívoca o uso de *malware* para investigação criminal. A legislação existente, como a Lei 9.296/96, não abrange essas práticas intrusivas, o que levanta questões sobre a conformidade com as garantias constitucionais de privacidade. Da mesma forma, a ausência de uma legislação específica que discipline esse procedimento levanta indagações sobre a admissibilidade em juízo das provas geradas. Diante desse cenário, é crucial analisar as implicações jurídicas e constitucionais envolvidas nesse tipo de investigação.

Em primeiro lugar, é necessário destacar que a obtenção de provas por meio de *malware* sem a devida autorização judicial configura uma violação clara aos direitos fundamentais estabelecidos na Constituição Federal. Direitos como a livre comunicação, a intimidade, a privacidade, a autodeterminação informativa e a integridade e confiabilidade dos sistemas informáticos são essenciais e devem ser preservados mesmo no contexto de investigações criminais. A Constituição Federal, no artigo 5º, incisos X, XI e XII, garante tais direitos aos cidadãos, e qualquer violação a essas garantias consiste em uma afronta direta ao texto constitucional.

É notório que a ausência de legislação específica que regule a utilização dessas tecnologias em investigações criminais cria um vácuo legal, deixando espaço para interpretações divergentes. A maioria dos especialistas concorda que, diante dessa lacuna normativa, a obtenção de provas por meio de infiltração informática pode representar uma ameaça direta aos direitos fundamentais dos cidadãos, conforme estabelecido na Constituição Federal.

A utilização de *softwares* para acesso à máquina de investigados permite ao operador:

> […] decifrar tudo o que se digita no teclado, acompanhar o que aparece na tela; monitorar a navegação na internet; acessar os dados e arquivos contidos no disco rígido ou guardados na nuvem e deles extrair cópias; acessar aplicativos de mensagens e e-mails; captar os SMS já recebidos e enviados e interceptá-los em tempo

> real; interceptar conversas telefônicas e/ou fluxos de comunicações em aplicativos de chamadas de voz e vídeo; ativar o microfone e a câmera do dispositivo e, com isso, realizar interceptações ambientais e captar imagens[2].

Isso claramente demanda uma regulamentação diante do confronto com diversos dispositivos constitucionais.

No entanto, existe uma corrente doutrinária a favor da aplicação analógica de normas existentes, como as previstas na já mencionada Lei de Interceptação Telefônica, para os casos envolvendo infiltração informática. Segundo essa perspectiva, alega-se que, mesmo na ausência de legislação específica, algumas normas existentes poderiam ser extrapoladas para cobrir essas situações particulares.

A Lei 9.296/96 estabelece a necessidade de autorização judicial para a obtenção de provas por meio de interceptações telefônicas. Além disso, a Lei 12.965/14, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, reforça a necessidade de ordem judicial para violação do sigilo das comunicações pela internet, preservando assim a inviolabilidade e o sigilo do fluxo de comunicações e das comunicações privadas armazenadas. Assim, independentemente do enfoque legal adotado, a primeira premissa é que a obtenção de provas por meio de *malware* sem autorização judicial é inquestionavelmente ilícita.

O questionamento que permanece é: mesmo com autorização judicial, tal meio de prova poderia ser considerado lícito?

Inobstante não tenham sido encontrados julgados específicos sobre a utilização desse meio de prova nos tribunais pátrios, o tema já foi objeto de debate em diversos países, como Estados Unidos da América, Alemanha, Itália, Finlândia, Espanha e Estônia. Em todas as experiências consultadas, verificou-se a necessidade de autorização judicial, mas merecem ser exploradas as experiências norte-americana e alemã.

3.1. Experiência Norte-Americana

Na experiência dos Estados Unidos, mencionada por Batista, Mendes e Pinho Filho, o uso de *malware* como meio de obtenção de provas em processos criminais ganhou atenção no final da década de 1990 e,

desde então, tem sido objeto de interpretação com base na Constituição Americana[1, 2, 3].

O primeiro registro de uso de *malware* como meio de prova naquele país foi no caso contra Nicodemo S. Scarfo e Frank Paolercio, em janeiro de 1999, em que agentes do *Federal Bureau of Investigation* (FBI) investigavam um caso de jogo ilegal e agiotagem. No curso de uma medida de busca e apreensão, examinaram o computador dos suspeitos e o disco rígido, quando encontraram um arquivo criptografado, indecifrável sem a obtenção da senha. Acreditando que o arquivo tinha informações relevantes para as investigações, os agentes solicitaram autorização judicial para a emissão de dois mandados: um para acessar o local e outro para instalar um *malware* entre o teclado e o computador — um *keylogger* — com a função de registrar as teclas digitadas. Catorze dias após a instalação, o programa registrou a senha, e os agentes obtiveram acesso ao arquivo criptografado.

Embora no caso Scarfo o FBI tenha utilizado um *hardware* para a instalação do *malware*, as barreiras práticas para a colocação física de *keyloggers* em máquinas de suspeitos, combinadas com o grande aumento da utilização de computadores para práticas criminosas, tornou necessária a criação de mecanismos para instalação remota de *malwares*.

O primeiro registro público do método foi em 2011, com a criação da tecnologia na Operação Torpedo, citada por Batista, em que a polícia holandesa identificou uma grande rede de pornografia infantil vinculada a vários endereços de Protocolo de Internet (IP, da sigla em inglês) com sede nos Estados Unidos e operada pela rede Tor[3].

A rede Tor, também conhecida por *Tor Onion Router*, foi originalmente desenhada, implementada e desenvolvida pela Marinha dos Estados Unidos (*US Naval Research Laboratory*), com o intuito de proteger as comunicações governamentais, e está atualmente disponível na internet para *download*. O *software* Tor protege a privacidade dos usuários, reenviando, aleatoriamente, as comunicações por uma série de retransmissores para tornar sua origem e destinatário anônimos e não identificáveis. Assim, permite mascarar, em camadas, o endereço IP real do utilizador que, de outro modo, poderia ser identificado, tornando praticamente impossível traçar a comunicação até o IP real.

Na Operação Torpedo, diante da localização dos IPs, os policiais holandeses requisitaram colaboração do FBI na investigação, que, após identificar um suspeito, solicitou ao Tribunal de Nebraska um mandado. A agência pedia autorização para modificar o código dos servidores utilizados para propagação de pornografia infantil, com a instalação de uma *Network Investigative Technique* (NIT), que nada mais é que uma forma de *malware*, em cada computador que acessasse o *website* com conteúdo ilícito.

A base do pedido era o *website* funcionar na rede Tor, o que tornava impossível, com as técnicas tradicionais, rastrear a comunicação e identificar os criminosos. Pela NIT, os agentes teriam um período de 30 dias para procurar e investigar os usuários, que, ao acessarem o *site*, tinham o *malware* automaticamente instalado em suas máquinas.

O *software* captava: (1) o endereço IP real do computador, bem como a data e a hora de seu reconhecimento; (2) a identificação da sessão ativa; e (3) o tipo de sistema operacional em execução, nomeadamente, a versão e a arquitetura (por exemplo: Windows 7, X86). Com base nas informações coletadas, os agentes identificaram pelo menos 25 visitantes do *site*. A operação resultou na detenção e condenação de 19 pessoas nos Estados Unidos.

Todavia, apesar de o uso de *malware* ser um meio de prova admitido nos Estados Unidos, a divisão de Houston do Tribunal do Distrito do Texas, em 2013, negou a expedição de mandado judicial com esse fim na investigação de uma fraude bancária perpetrada contra um cidadão residente no Texas. Na ocasião, o FBI solicitou que fosse autorizada a instalação de um *malware* no computador do suspeito, que registrava um IP localizado fora dos Estados Unidos da América. O pedido explicitava que, após a instalação do programa, o FBI poderia ter acesso ao disco rígido do computador, à memória RAM (*Random Access Memory*) e a outros meios de armazenamento, podendo ainda ativar a *webcam* e gerar coordenadas de localização do computador. Batista aponta que:

> O único objetivo era obter informações tais como: registos dos endereços IP utilizados; registos da atividade na *internet*, incluindo *logs*, *caches*, *browser*, histórico, *cookies*, páginas marcadas como favoritas, termos de pesquisa e sites pesquisados; registos que comprovassem a utilização daquele endereço IP para aceder ao *e-mail* de John Doe;

> provas como no momento dos factos descritos o 'atacante' usou, apropriou ou controlou o computador de John Doe a fim de criar, editar ou apagar, nomeadamente, provas como *logins*, usuários e palavras-passe, documentos, histórico de navegação, perfis, conteúdos e contactos de *e-mails*, *chat*, entre outros; provas que o *software* utilizado permitia que terceiros pudessem também controlar o computador da vítima e prova do número de vezes que o mesmo foi acedido[3, p. 38].

O pedido do FBI foi analisado pelo tribunal e negado com base na incompetência territorial, diante do fato de a localização do sistema visado — e, consequentemente, do alvo — ser desconhecida. O tribunal apontou ainda que o pedido do FBI não esclarecia o método de introdução do *software* no computador do suspeito, de modo que o procedimento não assegurava que somente o computador dele seria atingido. Outro ponto de preocupação levantado foi a utilização do *software* para a técnica descrita na solicitação de mandado como *photo monitoring*. Para o tribunal, isso era prova de que os agentes teriam acesso em tempo real à *webcam* do suspeito, sem garantia de não lesar terceiros desvinculados da prática criminosa, o que colidiria com as regras de monitoramento por vídeo sustentadas pela Quarta Emenda à Constituição daquele país.

3.2. Experiência Alemã

Ossian Bezerra Pinho Filho, professor e membro do Ministério Público brasileiro, relata que, na Alemanha:

> Em 2006, como parte de uma investigação criminal sobre fatos supostamente relacionados ao terrorismo, um promotor público solicitou a concessão de um mandado judicial, autorizando uma busca remota no computador de um suspeito por meio da instalação de um cavalo de Troia. O pedido foi rejeitado em 25 de novembro de 2006, e o promotor recorreu para o Tribunal Federal de Justiça da Alemanha (*Bundesgerichtshof*), argumentando que as disposições legais incluídas no *Strafprozeßordnung* (CPP alemão), relativas à busca (física) serviria como analogia para permitir o uso de tais meios de obtenção de provas. **O Tribunal Federal concluiu que essa analogia não poderia ser feita e que a utilização dessa medida carecia**

> **de fundamento legal, tornando-a inadmissível no processo penal** […][2] (grifo nosso).

Pouco tempo após a decisão do tribunal, em 20 de dezembro de 2006, foi introduzida na Lei de Proteção da Constituição da Renânia do Norte-Vestfália — lei que descreve os direitos e estabelece uma base legal para as operações da Agência de Proteção da Constituição (principal serviço secreto alemão) — a possibilidade de utilização de *malware*, com permissão, entre outras medidas, para coleta de informações de monitoramento, acesso a *webmail*, espionagem e controle dos sistemas informáticos afetados.

Pinho Filho cita ainda em sua obra que:

> Um recurso foi apresentado perante o Tribunal Constitucional Federal Alemão. **Em 27 de fevereiro de 2008, o tribunal chegou a uma decisão. Em primeiro lugar, considerou a questão à luz de três direitos fundamentais: (i) o direito ao sigilo da correspondência, correio e telecomunicações, (ii) o direito à inviolabilidade do domicílio e (iii) o direito à autodeterminação informativa. No entanto, considerando-se** [sic] **o método pelo qual as provas foram obtidas estava em questão, argumentou-se que a proteção constitucional não se limitava ao objeto de cada um desses direitos fundamentais. Assim, tendo em vista a necessidade de oferecer, de forma mais abrangente, a proteção constitucional em relação à integridade dos sistemas informáticos, bem como aos dados por eles armazenados e transmitidos, o tribunal consagrou o direito fundamental à garantia da confidencialidade e integridade dos sistemas de tecnologia da informação (*Grundrecht aug Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*). O direito fundamental baseia-se na dignidade humana e, sobretudo, no direito geral da personalidade (MENDES, 2013).** Depois de submeter o dispositivo em análise ao escrutínio constitucional, em particular ao recém-denominado direito fundamental, **o tribunal concluiu que violava os princípios da transparência, segurança jurídica e proporcionalidade, sendo, portanto, inconstitucional**. No entanto, o tribunal sugeriu uma futura formulação jurídica da utilização de tais meios de obtenção de provas de acordo com os requisitos constitucionais […][2] (grifo nosso).

Posteriormente, em alterações promovidas na Lei para a Defesa Face aos Perigos do Terrorismo Internacional em dezembro de 2008, foi autorizado naquele país, sob a epígrafe de "vigilância secreta em sistemas de informação", que a polícia federal, sem o conhecimento da pessoa visada, pudesse acessar seu sistema informático, com o intuito de recolher dados.

De acordo com Lydie Jorge Batista, em sua dissertação de mestrado — "O *malware* como meio de obtenção de prova em processo penal" — defendida na Universidade de Lisboa, o método foi

> […] permitido nos casos em que se verifique perigo para a vida, para a integridade física ou para a liberdade de determinada pessoa e para a liberdade ou segurança nacional, assim como, em casos de prevenção de terrorismo a nível internacional ou relacionados com as infrações previstas no § 129a do StGB (§ 4a). Mas, apenas se for muito difícil ou impossível alcançar o mesmo resultado, através de outro meio de obtenção de prova menos gravoso[3, p. 53].

Ocorre que, tamanha a possibilidade de invasão de privacidade e violação de preceitos constitucionais, foram impostos diversos limites para sua utilização. No mesmo trabalho, Batista assevera que foi necessário o estabelecimento de balizas para sua autorização:

> No que se refere à competência, o recurso ao *malware* só poderá ser autorizado pelo presidente do Tribunal Federal ou por seu representante. O despacho de autorização deverá: (1) indicar a pessoa que será atingida, se possível, identificando-a com o nome e morada; (2) descrever, o mais detalhadamente possível, o sistema informático onde serão recolhidos os dados; (3) indicar a natureza e a duração do meio; e (4) fundamentar o uso de *malware*. Não obstante, o recurso a este meio não será autorizado, se houver indícios concretos de que serão recolhidos apenas dados referentes à vida privada do indivíduo ou se for impossível garantir que a técnica utilizada não irá recolher esse tipo de dados. [...] Quanto ao procedimento, só são admitidas técnicas que realizem o mínimo de alterações no sistema informático e que permitam a sua reversão. As técnicas utilizadas devem proteger o sistema informático visado de eventuais acessos não autorizados, através de meios semelhantes. Finda a investigação, é redigido um relatório detalhado, a fim de assegurar o exercício do contraditório, onde constem: (1) os meios técnicos utilizados; (2) a duração da investigação; (3) as características do sistema informático; (4) o estado em

> que se encontrava antes da investigação; (5) as alterações sofridas após o acesso; (6) os dados recolhidos; e (7) a unidade policial que executou a técnica[3, p. 53-54].

Como se vê, embora se trate de experiência estrangeira, os limites constitucionais impostos às violações de garantias fundamentais são os mesmos que os brasileiros, podendo ser citados neste último aqueles previstos no artigo 5º, incisos X, XI e XII, da Constituição Federal. Inobstante a ausência no Brasil de previsão legal para o uso de *malware* na obtenção e admissibilidade de provas, verifica-se, na experiência estrangeira, que, para a autorização de uso da prova, os tribunais exigem, no mínimo, a observância das seguintes informações:

a) os meios técnicos utilizados;

b) a duração da investigação;

c) as características do sistema informático;

d) o estado em que se encontrava antes da investigação;

e) as alterações sofridas após o acesso;

f) os dados recolhidos;

g) o responsável que executou a técnica.

4. CASOS ENVOLVENDO O APLICATIVO WHATSAPP WEB NO BRASIL

O WhatsApp é um sistema de comunicação instantânea multiplataforma que permite aos usuários trocar mensagens e fazer chamadas de voz e de vídeo pela internet. Está disponível para dispositivos como *smartphones* e computadores. O WhatsApp Web é a extensão do WhatsApp utilizada em computadores e permite aos usuários acessar suas conversas, enviar mensagens, imagens e vídeos diretamente pelo navegador da *web*. Para usar o WhatsApp Web, os usuários precisam escanear um código de resposta rápida (*QR Code*) exibido na página *web* utilizando o aplicativo móvel do WhatsApp instalado em seus *smartphones*, sincronizando assim as mensagens entre os dispositivos.

Embora haja uma diferença conceitual entre a utilização de *malware* para fins de investigação criminal e o espelhamento do WhatsApp com a ferramenta WhatsApp Web, ambas as técnicas, em diferentes graus e sem que haja regulamentação, permitem acesso amplo e irrestrito do operador a toda e qualquer comunicação realizada, inclusive em período anterior à determinação de quebra de sigilo, o que, nesse ponto, aproxima a medida do instituto de busca e apreensão. Todavia, o ponto nevrálgico da discussão é a possibilidade de o agente responsável pela investigação inserir ou excluir informações do dispositivo, fato que demanda maior atenção, com a criação de protocolos específicos para o emprego desse método.

No caso de espelhamento de WhatsApp, o Superior Tribunal de Justiça tem adotado posições divergentes.

No julgamento do Recurso em *Habeas Corpus* nº 99.735 2018.01.53349-8, a corte declarou nulas as provas produzidas com espelhamento do WhatsApp Web, por entender ser impossível a analogia com o instituto da interceptação telefônica, nos seguintes termos:

> EMEN: RECURSO ORDINÁRIO EM *HABEAS CORPUS*. PENAL E PROCESSO PENAL. TRÁFICO DE DROGAS E ASSOCIAÇÃO AO TRÁFICO. AUTORIZAÇÃO JUDICIAL DE ESPELHAMENTO, VIA WHATSAPP WEB, DAS CONVERSAS REALIZADAS PELO INVESTIGADO COM TERCEIROS. ANALOGIA COM O INSTITUTO DA INTERCEPTAÇÃO TELEFÔNICA. IMPOSSIBILIDADE. PRESENÇA DE DISPARIDADES RELEVANTES. ILEGALIDADE DA MEDIDA. RECONHECIMENTO DA NULIDADE DA DECISÃO JUDICIAL E DOS ATOS E PROVAS DEPENDENTES. PRESENÇA DE OUTRAS ILEGALIDADES. LIMITAÇÃO AO DIREITO DE PRIVACIDADE DETERMINADA SEM INDÍCIOS RAZOÁVEIS DE AUTORIA E MATERIALIDADE. DETERMINAÇÃO ANTERIOR DE ARQUIVAMENTO DO INQUÉRITO POLICIAL. FIXAÇÃO DIRETA DE PRAZO DE 60 (SESSENTA) DIAS, COM PRORROGAÇÃO POR IGUAL PERÍODO. CONSTRANGIMENTO ILEGAL EVIDENCIADO. RECURSO PROVIDO. […] 2. O espelhamento das mensagens do *WhatsApp* ocorre em sítio eletrônico disponibilizado pela própria empresa, denominado *WhatsApp Web*. Na referida plataforma, é gerado um tipo específico de código de barras, conhecido como Código QR (*Quick Response*), o qual só pode ser lido pelo celular do usuário que pretende usufruir do serviço. Daí a necessidade de apreensão, ainda que por breve período de tempo, do aparelho telefônico

que se pretende monitorar. 3. Para além de permitir o acesso ilimitado a todas as conversas passadas, presentes e futuras, a ferramenta *WhatsApp Web* foi desenvolvida com o objetivo de possibilitar ao usuário a realização de todos os atos de comunicação a que teria acesso no próprio celular. O emparelhamento entre celular e computador autoriza o usuário, se por algum motivo assim desejar, a conversar dentro do aplicativo do celular e, simultaneamente, no navegador da *internet*, ocasião em que as conversas são automaticamente atualizadas na plataforma que não esteja sendo utilizada. 4. Tanto no aplicativo, quanto no navegador, é possível, com total liberdade, o envio de novas mensagens e a exclusão de mensagens antigas (registradas antes do emparelhamento) ou recentes (registradas após), tenham elas sido enviadas pelo usuário, tenham elas sido recebidas de algum contato. Eventual exclusão de mensagem enviada (na opção "Apagar somente para Mim") ou de mensagem recebida (em qualquer caso) não deixa absolutamente nenhum vestígio, seja no aplicativo, seja no computador emparelhado, e, por conseguinte, não pode jamais ser recuperada para efeitos de prova em processo penal, tendo em vista que a própria empresa disponibilizadora do serviço, em razão da tecnologia de encriptação ponta-a-ponta, não armazena em nenhum servidor o conteúdo das conversas dos usuários. 5. Cumpre assinalar, portanto, que o caso dos autos difere da situação, com legalidade amplamente reconhecida pelo Superior Tribunal de Justiça, em que, a exemplo de conversas mantidas por *e-mail*, ocorre autorização judicial para a obtenção, sem espelhamento, de conversas já registradas no aplicativo *WhatsApp*, com o propósito de periciar seu conteúdo. 6. É impossível, tal como sugerido no acórdão impugnado, proceder a uma analogia entre o instituto da interceptação telefônica (art. 1.º, da Lei n.º 9.296/1996) e a medida que foi tomada no presente caso. 7. Primeiro: ao contrário da interceptação telefônica, no âmbito da qual o investigador de polícia atua como mero observador de conversas empreendidas por terceiros, no espelhamento via *WhatsApp Web* o investigador de polícia tem a concreta possibilidade de atuar como participante tanto das conversas que vêm a ser realizadas quanto das conversas que já estão registradas no aparelho celular, haja vista ter o poder, conferido pela própria plataforma *online*, de interagir nos diálogos mediante envio de novas mensagens a qualquer contato presente no celular e exclusão, com total liberdade, e sem

deixar vestígios, de qualquer mensagem passada, presente ou, se for o caso, futura. **8. O fato de eventual exclusão de mensagens enviadas (na modalidade "Apagar para mim") ou recebidas (em qualquer caso) não deixar absolutamente nenhum vestígio nem para o usuário nem para o destinatário, e o fato de tais mensagens excluídas, em razão da criptografia *end-to-end*, não ficarem armazenadas em nenhum servidor, constituem fundamentos suficientes para a conclusão de que a admissão de tal meio de obtenção de prova implicaria indevida presunção absoluta da legitimidade dos atos dos investigadores, dado que exigir contraposição idônea por parte do investigado seria equivalente a demandar-lhe produção de prova diabólica.** 9. Segundo: ao contrário da interceptação telefônica, que tem como objeto a escuta de conversas realizadas apenas depois da autorização judicial (*ex nunc*), o espelhamento via Código QR viabiliza ao investigador de polícia acesso amplo e irrestrito a toda e qualquer comunicação realizada antes da mencionada autorização, operando efeitos retroativos (*ex tunc*). 10. Terceiro: ao contrário da interceptação telefônica, que é operacionalizada sem a necessidade simultânea de busca pessoal ou domiciliar para apreensão de aparelho telefônico, o espelhamento via Código QR depende da abordagem do indíviduo ou do vasculhamento de sua residência, com apreensão de seu aparelho telefônico por breve período de tempo e posterior devolução desacompanhada de qualquer menção, por parte da Autoridade Policial, à realização da medida constritiva, ou mesmo, porventura - embora não haja nos autos notícia de que isso tenha ocorrido no caso concreto -, acompanhada de afirmação falsa de que nada foi feito. 11. Hipótese concreta dos autos que revela, ainda, outras três ilegalidades: (a) sem que se apontasse nenhum fato novo na decisão, a medida foi autorizada quatro meses após ter sido determinado o arquivamento dos autos; (b) ausência de indícios razoáveis da autoria ou participação em infração penal a respaldar a limitação do direito de privacidade; e (c) ilegalidade na fixação direta do prazo de 60 (sessenta) dias, com prorrogação por igual período. 12. Recurso provido, a fim de declarar a nulidade da decisão judicial que autorizou o espelhamento do *WhatsApp* via Código QR, bem como das provas e dos atos que dela diretamente dependam ou sejam consequência, ressalvadas eventuais fontes independentes, revogando, por conseguinte, a

> prisão preventiva dos Recorrentes, se por outro motivo não estiverem presos[4] (grifo nosso).

Mais recentemente, divergindo da interpretação, em decisão monocrática no Agravo em Recurso Especial 2257960/MG, o ministro Reynaldo Soares da Fonseca, analisando a questão à luz dos artigos 53, incisos I e II, da Lei 11.343/06; 31, incisos III e VII, da Lei 12.850/13; 70, incisos II e III, da Lei 12.965/14, bem como do artigo 489, §11, inciso VI, do Código de Processo Civil, entendeu pela licitude das provas obtidas por meio de espelhamento do aplicativo de comunicação via WhatsApp Web.

Nos fundamentos da decisão, o Ministro destacou que:

> […] a questão posta em juízo traz a baila a aferição da possibilidade de utilização, no ordenamento jurídico pátrio, de ações encobertas, controladas virtuais ou de agentes infiltrados no plano cibernético. A questão que se põe é: pode-se revestir a mencionada manobra policial de legalidade, gerando o subsequente aproveitamento das provas?
>
> A resposta se denota positiva, desde que o uso da ação controlada na investigação criminal esteja amparado por autorização judicial. A chancela jurídica, portanto, possibilita o monitoramento legítimo, inclusive via espelhamento do *software WhatsApp Web*, outorgando funcionalidade à persecução virtual, de inestimável valia no mundo atual. A prova assim obtida, via controle judicial, não se denota viciada, não inquinando as provas derivadas, afastando-se a teoria do *fruits of the poisounous* [sic] *tree* na hipótese[5].

Após fazer breve digressão sobre as previsões da Lei de Organizações Criminosas, da Lei de Drogas e da Lei de Interceptação Telefônica, o magistrado entendeu que:

> A lei de interceptação, em combinação com a Lei das Organizações Criminosas, na hipótese, outorga legitimidade (legalidade) e dita o rito (regra procedimental), a mencionado espelhamento, em interpretação progressiva, em conformidade com a realidade atual, para adequar a norma à evolução tecnológica[5].

Para o magistrado:

> Concebe-se plausível, portanto, que o espelhamento autorizado via *software WhatsApp Web*, pelos órgãos de persecução, se denote equivalente à modalidade de

> infiltração do agente, que consiste, como já asseverado, em meio extraordinário, mas válido, de obtenção de prova[5].

No bojo da decisão, apontou-se ainda que

> […] a objeção de que a facilidade de manipulação da prova obtida pela via do espelhamento do *Whatsapp Web*, pelo agente infiltrado, tornaria invalida [sic] a evidência por tal meio obtida não merece guarida, na medida em que esta Corte Superior tem adotado entendimento pacífico no sentido de que "é despicienda a realização de perícia a fim de com*provar a fidedignidade das gravações, que são presumidamente autênticas, possuindo fé pública os agentes policiais envolvidos na operação. Tal entendimento independe da forma de transmissão das interceptações, se oriundos de gravações de áudio ou captação de mensagens de texto*" (AgRg no RHC n. 129.003/MT, Relator Ministro RIBEIRO DANTAS, Quinta Turma, julgado em 13/10/2020, DJe 20/10/2020)[5] (grifo no original).

Todavia, há de se apontar que o Agravo Regimental no Recurso em *Habeas Corpus* 129.003/MT citado pelo ministro para fundamentar sua decisão é referente à desnecessidade de realização de perícia para comprovar a fidedignidade de mensagens. Tratava-se de prova produzida por interceptação telefônica, que, como já observado, é técnica distinta, que não permite acesso amplo e irrestrito ao aplicativo ou ainda a possibilidade de inserção ou exclusão de informações no dispositivo pelo agente responsável pela investigação.

CONCLUSÃO

A míngua de legislação própria que estabeleça regras claras e específicas para a obtenção de provas por meio de novas tecnologias é objeto de celeuma no âmbito do ordenamento jurídico brasileiro. Os avanços tecnológicos experimentados pelo mundo moderno têm proporcionado a existência de intensos debates sobre os limites do direito à privacidade em contraponto ao direito à segurança pública, ambos direitos fundamentais aos cidadãos.

Nesse vácuo legal, a não implementação de métodos informáticos de investigação colabora para a expansão do uso de sistemas informáticos na prática e no planejamento de crimes das mais diversas naturezas.

Atualmente, no Brasil, ainda que encarcerados, membros de organizações criminosas têm se utilizado de aplicações criptografadas para planejar execuções e coordenar esquemas de tráfico de drogas, armas, pessoas e outros crimes.

A regulamentação das investigações com introdução de *malware* em dispositivos eletrônicos pode representar um passo importante no combate à criminalidade organizada, possibilitando ao Estado investigador um meio de produzir provas vedadas aos métodos tradicionais, regulados antes da era da tecnologia da informação. O direito à segurança pública eficaz é pautado no princípio fundamental da dignidade da pessoa humana insculpido na Constituição Federal, sendo dever do Estado atuar em prol de um ambiente mais seguro e justo para todos os cidadãos, o que inclui reprimir a criminalidade, em especial a organizada.

Nesse contexto, é imperativa a regulamentação de tal meio de prova que considere não apenas os requisitos e procedimentos para a autorização judicial, mas também as peculiaridades tecnológicas e éticas envolvidas. De um lado, a definição de limites claros com cautelas rigorosas para garantir a proteção dos direitos individuais é essencial para evitar abusos e preservar a integridade da privacidade em um mundo cada vez mais digitalizado. Lado outro, é preciso garantir o direito fundamental à segurança pública.

Dessa forma, mostra-se necessária a implementação de uma legislação que estabeleça a observância de protocolos mínimos para garantir a auditabilidade e a integridade dos dados obtidos por introdução de *malware*, evitando-se qualquer possibilidade de interação dos agentes responsáveis pela investigação. A criação de tais protocolos impõe-se para impedir que o operador proceda à inclusão de registros, programas, documentos etc. no equipamento eletrônico monitorado, inclusive com a criação e a utilização de programas e métodos específicos, tal qual ocorre com as interceptações telefônicas, sem que a manipulação seja rastreável, de forma a promover fiel tutela do Poder Judiciário.

Inobstante os argumentos apresentados na decisão do ministro Reynaldo Soares da Fonseca no Agravo em Recurso Especial 2257960, entende-se que é problemática a presunção de autenticidade da prova em razão da fé pública atribuída aos agentes policiais sem que haja

um protocolo específico de espelhamento que garanta efetivamente a autenticidade. Isso porque, conforme apontado no Recurso em *Habeas Corpus* 99735, ao cidadão submetido a julgamento pelo Estado-juiz é nítida a impossibilidade de contraposição à prova produzida. Por não ficar esta armazenada em servidor algum, implicaria indevida presunção absoluta da legitimidade dos atos dos investigadores, dado que exigir contraposição idônea por parte do investigado seria equivalente a demandar-lhe produção de prova diabólica.

A regulamentação e a criação de protocolos para o uso de técnicas de infiltração informática são necessárias para extirpar a ameaça de uso arbitrário ou abusivo por autoridades ou indivíduos mal-intencionados na incriminação indevida de pessoas e para assegurar que a investigação criminal seja conduzida de maneira ética e legal, protegendo, assim, os direitos e liberdades individuais dos cidadãos. A ausência de regulamentação específica traz insegurança aos atores envolvidos na persecução penal e não submete a prova a mecanismos de controle adequados, criando um ambiente propício para a alegação/efetivação de manipulação de provas e para a violação dos direitos dos cidadãos.

No caso específico do *malware* em computadores — ou mesmo em *smartphones* —, é ainda maior a preocupação com o uso indiscriminado e desregrado da tecnologia, que permite acionamento de *webcam*, microfone etc. Deve ser anotado que tal fato, discutido ainda em 2006 por tribunais internacionais, resultou no reconhecimento de inutilidade das provas, pelo entendimento de que é necessário estabelecer limites claros e garantir a transparência e a supervisão adequada para proteger os indivíduos de abusos e violações de seus direitos fundamentais.

É primordial que a sociedade como um todo esteja ciente das questões envolvidas na utilização de *malware* em investigações criminais e que participe ativamente do debate sobre a necessidade de se certificar da segurança pública e sobre os limites e as garantias desse processo. A defesa dos direitos individuais e da privacidade é uma responsabilidade de todos os cidadãos, assim como o direito à segurança pública, de modo que a regulamentação adequada das práticas em discussão é essencial

para proteger os valores democráticos brasileiros e garantir um sistema de justiça mais eficaz, justo e equitativo.

Portanto, a matéria necessita ser cuidadosamente disciplinada, levando em consideração os desafios éticos e tecnológicos que as infiltrações por *malware* apresentam, ao mesmo tempo em que se assegura a eficácia das investigações criminais.

Ao longo desta análise, ficou nítido que a falta de uma regulamentação clara abre margem para interpretações diversas e controversas. A maioria dos estudiosos e especialistas defende veementemente a necessidade de uma legislação específica que contemple a infiltração informática, garantindo, ao mesmo tempo, a salvaguarda dos princípios constitucionais que regem a privacidade, a livre comunicação, a intimidade, a autodeterminação informativa e a integridade dos sistemas informáticos.

É o que defendem Ribeiro *et al.*, ao apontarem que:

> No Brasil, não é possível sustentar a existência de uma previsão para a utilização do *malware* a partir dos marcos normativos das Leis nº 9.296/1996, 12.850/2013 e 8.069/1990. Por ser um meio de obtenção de prova atípico e com amplas repercussões sobre o domínio privado dos investigados, somente uma previsão legal expressa poderia permitir o emprego dessa técnica[6, p. 1495].

Por outro lado, a existência de correntes doutrinárias que, à míngua de regulamentação, defendem a aplicação analógica de normas existentes, como as previstas na Lei de Interceptação Telefônica, levanta questionamentos importantes sobre como o ordenamento jurídico deve se adaptar aos avanços tecnológicos.

A linha argumentativa é baseada na previsão expressa do artigo 3º do Código de Processo Penal, que prevê que "[a] lei processual penal admitirá interpretação extensiva e aplicação analógica, bem como o suplemento dos princípios gerais de direito"[7].

Gustavo Soares Torres advoga que inovação investigativa criminal, que ainda não tenha sido regulada como meio de obtenção de prova, deve ser tolerada de forma excepcional, "decorrente de interpretação extensiva ou aplicação analógica e inserida em contexto de evolução legislativa progressiva"[8, p. 266]. Em arremate, Torres aponta que "além desses

requisitos, apenas pode ser tolerada à medida que puder ser juridicamente controlada"[8, p. 266].

Embora seja recomendável que o Poder Legislativo atue prontamente para preencher essa lacuna normativa, com a criação de uma legislação específica baseada em princípios sólidos de proporcionalidade, necessidade e respeito aos direitos fundamentais, que estabeleça limites claros e garanta a transparência no uso de técnicas de infiltração informática, a atual legislação já permite, sob a tutela jurisdicional, o emprego de métodos intrusivos de investigação.

Como bem observado pelo ministro Reynaldo Soares da Fonseca, no julgamento do Agravo em Recurso Especial 2257960/MG, a aplicação analógica dos institutos previstos na Lei de Interceptação Telefônica (Lei 9.296/1996), com a Lei de Organização Criminosa (Lei 12.850/13) e/ou a Lei de Drogas (Lei 11.343/06), autoriza, sob chancela judicial, diversas medidas intrusivas, como a infiltração de agentes e a captação ambiental, que podem ser realizadas com programas de intrusão virtual remota e ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal.

E, diante da ausência de balizas legais específicas, a salvaguarda aos direitos fundamentais pode ser obtida com imposição judicial de protocolos mínimos para garantir a auditabilidade e a integridade dos dados obtidos por introdução de *malware*, com a adoção das mesmas cautelas identificadas nas experiências estrangeiras, como a descrição dos meios técnicos utilizados, a duração da investigação, as características do sistema informático afetado, o estado em que se encontrava antes da investigação, as alterações sofridas após o acesso, os dados recolhidos e o responsável que executou a técnica.

Em arremate, limites, balizas e controle são fundamentais para garantir a integridade da prova e a legitimidade de sua produção, permitindo, ainda, a responsabilização de autoridades ou indivíduos mal-intencionados por eventuais abusos ou excessos de poder praticados com a utilização indevida das ferramentas de intrusão (*accountability*).

REFERÊNCIAS

BATISTA, Lydie Jorge. **O *malware* como meio de obtenção de prova**. Dissertação (Mestrado em Ciências Jurídico-Forenses) – Universidade de Lisboa, Lisboa, 2018.

BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro: Presidência da República. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 16 ago. 2024.

BRASIL. Superior Tribunal de Justiça. **Agravo no Recurso Especial no 2.257.960 MG**. Relator: Ministro Reynaldo Soares da Fonseca. Brasília, 19 maio 2023. Migalhas. Disponível em: <https://www.migalhas.com.br/arquivos/2023/7/1DF97F3601A0B1_stj_dje_20230519_0_36752079....pdf>. Acesso em: 12 dez. 2023.

BRASIL. Superior Tribunal de Justiça. **Recurso Ordinário em Habeas Corpus no 99.735 SC**. Relatora: Ministra Laurita Vaz. Brasília, 12 dez. 2018. Revista Eletrônica da Jurisprudência. Disponível em: <https://processo.stj.jus.br/processo/revista/inteiroteor/?num_registro=201801533498&dt_publicacao=12/12/2018>. Acesso em: 12 dez. 2023.

MENDES, Carlos Hélder Carvalho Furtado. ***Malware* do Estado e processo penal**: a proteção de dados informáticos face à infiltração por *software* na investigação criminal. 2018. Dissertação (Mestrado em Ciências Criminais) – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2018.

PINHO FILHO, Ossian Bezerra. **Investigação criminal tecnológica**: infiltração por *malware* nas investigações informáticas. Curitiba: Juruá, 2022.

RIBEIRO, Gustavo Alves Magalhães *et al*. O *malware* como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 8, n. 3, p. 1463-1500, set./dez. 2022. Disponível em: <https://www.scielo.br/j/rbdpp/a/rhHb6tynNX5rNH74mNGHSrj/?format=pdf&lang=pt>. Acesso em: 16 ago. 2024.

SOARES, Gustavo Torres. **Investigação criminal e inovações tecnológicas**: perspectivas e limites. 2014. Tese (Doutorado em Direito) – Universidade de São Paulo, São Paulo, 2014.