O *malware* como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro

Malware as a means of obtaining evidence and its implementation in the Brazilian legal system

Gustavo Alves Magalhães Ribeiro[1]
Universidade de São Paulo, São Paulo/SP, Brasil
gustavo_alvesribeiro@hotmail.com
http://lattes.cnpq.br/2412046702757861
https://orcid.org/0000-0002-3677-2710

Pedro Ivo Rodrigues Velloso Cordeiro[2]
Universidade de São Paulo, São Paulo/SP, Brasil
pedroivo.cordeiro@gmail.com
http://lattes.cnpq.br/7389277522042037
http://orcid.org/0000-0002-3854-9651

Débora Moretti Fumach[3]
Universidade de São Paulo, São Paulo/SP, Brasil
debmoretti@hotmail.com
http://lattes.cnpq.br/63853545190701
http://orcid.org/0000-0003-1552-5400

[1] Mestrando em Direito Penal pela Faculdade de Direito da USP. Bacharel em Direito pela Faculdade de Direito da USP. Advogado.

[2] Doutorando em Direito Processual Penal pela Faculdade de Direito da USP. Mestre em Direito e Estado pela Faculdade de Direito da Universidade de Brasília. Advogado.

[3] Doutoranda em Direito Processual Civil pela Faculdade de Direito da USP. Mestre em Direito Público - Administration et Politiques Publiques pela Université Paris 2 Panthéon-Assas (Título revalidado pela UNB). Promotora de Justiça.

Resumo: O *malware* constitui um novo meio de obtenção de prova em matéria criminal. A sua operacionalização ocorre a partir da instalação, de forma oculta, de um *software* malicioso no equipamento ou sistema informático de um terceiro, a partir do qual será possível o acesso aos dados e informações nele contidos. Dado o seu elevado grau de invasividade, essa técnica enseja um impacto sobre diversos direitos fundamentais e garantias processuais dos cidadãos. O presente artigo faz uma análise dos principais aspectos problemáticos envolvendo o emprego do *malware* na esfera investigativa e averigua se é possível a sua utilização no Brasil no ordenamento jurídico vigente e, em quais termos, a sua utilização seria lícita. Ao final, o artigo conclui pela impossibilidade de seu emprego com base na legislação vigente e fornece parâmetros que devem orientar uma norma que vise futuramente regular essa medida no Brasil.

Palavras-chave: *malware*; meio de obtenção de prova; direitos fundamentais; garantias processuais.

Abstract: *Malware is a new means of obtaining evidence in criminal matters. Its operation takes place from the installation, in a hidden way, of malicious software on the equipment or computer system of a third party, from which it will be possible to access the data and information contained therein. Given its high degree of invasiveness, this technique has an impact on several fundamental rights and procedural guarantees of citizens. This article analyzes the main problematic aspects involving the use of malware in the investigative sphere and investigates whether its use in Brazil is possible in the current legal system and, in what terms, its use would be lawful. In the end, the article concludes by the impossibility of its use based on the current legislation and provides parameters that should guide a norm that aims to regulate this measure in Brazil in the future.*

Keywords: *malware; means of obtaining evidence; fundamental rights; procedural guarantees.*

1. Introdução.

A vertiginosa evolução das tecnologias de informação nas últimas décadas, com destaque para o desenvolvimento da internet, revolucionou o modo como as pessoas se comunicam e organizam as suas tarefas cotidianas, bem como obtém e armazenam dados e informações. Atualmente, os equipamentos informáticos estão presentes desde as atividades afetas à vida privada dos indivíduos, até aquelas de natureza profissional.

Os efeitos dessa realidade, naturalmente, alcançaram a seara processual-penal. De um lado, o desenvolvimento e a popularização da internet e dos meios informáticos impactou a prática delitiva, permitindo o surgimento de ilícitos tipicamente virtuais, além da expansão do uso de meios digitais para a consecução de crimes não exclusivamente virtuais. De outro, é crescente o interesse do Estado no uso de meios digitais para otimizar atividades relacionadas à prevenção e repressão de delitos. É sob este contexto que se situa o presente artigo, que trata da análise da possibilidade de utilização dos chamados *malwares* na esfera processual-penal brasileira, sobretudo na apuração da autoria e materialidade de práticas criminosas.

O termo *malware* se refere a um conjunto específico de *softwares* que, instalados de modo oculto em um equipamento ou sistema informático, permitem a um terceiro não usuário o acesso às informações e dados neles contidos, além de um controle contínuo e secreto sobre uma pluralidade de suas funcionalidades. Comumente referidos como *softwares* espiões, os *malwares* permitem o recolhimento de uma diversidade de informações e dados contidos nesses equipamentos e sistemas informáticos, estejam eles em processamento ou simplesmente armazenados, além de possibilitarem a captação de sinais audiovisuais emitidos no raio de alcance dos seus componentes.

Esse grau de invasividade faz que diversas críticas sejam feitas à utilização do *malware*, qualificando-o como uma forma de *hacking* estatal. Isso porque ao tempo que tais *softwares* podem gerar um ganho de eficiência extraordinário na seara investigativa, as suas especiais características podem ensejar questionáveis restrições a direitos fundamentais e a garantias processuais constitucionalmente consagradas.

O emprego de *malwares* em investigações está cada vez mais difundido ao redor do mundo, existindo experiências nesse sentido em países como os Estados Unidos, a Espanha e a Alemanha. No Brasil, particularmente, embora o interesse pela utilização de *softwares* espiões por autoridades de polícia judiciária já tenha sido noticiado[4], não se tem conhecimento da sua efetiva aplicação como meio investigativo.

Diante dessas circunstâncias, o presente artigo tem por objetivo refletir sobre as seguintes questões: em nosso ordenamento jurídico é admissível a utilização dos chamados *malwares* na esfera processual-penal, sobretudo na apuração da autoria e materialidade de práticas criminosas? A disciplina legal vigente relativa aos meios de obtenção de prova é suficiente ou o emprego de *malwares* na esfera processual-penal depende do estabelecimento de um regramento jurídico próprio?

Para enfrentar tais questionamentos, buscou-se inicialmente caracterizar os *malwares*, bem como identificar o seu impacto sobre os direitos fundamentais e garantias processuais de um indivíduo investigado. Em seguida, faz-se uma análise da disciplina dos meios de obtenção de prova já legislados e que guardam relação com o objeto de estudo, os quais estão previstos no Código de Processo Penal e nas Leis n. 9.296/1996, 12.850/2013 e 8.069/1990. Ao final, são indicados possíveis caminhos para a conformação de um regramento seguro para a operacionalização do *malware* no Brasil.

2. *Malware*: conceituação e funcionalidades.

2.1. Natureza, atributos e espécies.

A palavra *malware* nasce da conjugação do adjetivo *malicius* e do substantivo *software*[5], referindo-se àqueles programas simples ou

---

[4] ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. Vigilância das comunicações pelo Estado brasileiro. Disponível em: <https://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf>. Acesso em: 22 mai. 2022.

[5] BATISTA, Lydie Jorge Batista. *O malware como meio de obtenção de prova em processo penal*. 2018. Dissertação (Mestrado em Direito) Faculdade de Direito da Universidade de Lisboa, Lisboa, 2018, p. 25-26.

autorreplicativos que, sem o conhecimento do seu utilizador, são inseridos de forma sub-reptícia em um sistema informático de modo a permitir que o seu controlador tenha acesso a dados já armazenados ou ainda em processamento, bem como faça o controle sobre diversas de suas funcionalidades. Uma vez secretamente instalados, tais instrumentos aproveitam-se de falhas ou aberturas do sistema informático para criar um portal de acesso remoto e invisível ao utilizador, a denominada *backdoor*, por meio da qual se obtém, à distância, acesso aos dados e funcionalidades do dispositivo[6].

A utilização de *malwares* permite ao controlador do *software* uma ampla gama de funcionalidades, tais como acessar arquivos, senhas e informações armazenadas no sistema informático, bem como transferi-los e armazená-los em servidor remoto e independente do meio invadido. Além disso, essas funcionalidades ainda podem ser instrumentalizadas de maneira a possibilitar o monitoramento e recolhimento de dados sobre atividades e hábitos do usuário na internet, como data/hora de acessos, páginas *web* ou de e-mail acessados, endereço IP e tipo de navegador utilizado.

O *malware* não constitui um *software* único, tratando-se de uma série de dispositivos que, a depender da sua natureza e funções, assumem variados nomes, como cavalos de Tróia, *logic bombs*, *spyware*, *keylogger* e *screenlogger*, *rootkits*, *worms*, vírus, *blended threats* e *bots*[7]. Todos têm

---

[6] Ao fazer o estudo dos *malwares*, Eduardo Bolsoni Riboli, define-os como "a categoria de programas informáticos desenvolvidos com a finalidade de extração de informações contidas em um dispositivo eletrônico ou sistema informático sem o consentimento e o conhecimento do utilizador quanto à sua instalação e execução. Embora existam diferentes espécies de softwares de espionagem — cada qual com sua(s) função(ões) própria(s), por vezes desempenhando mais de uma função —, todos os softwares de espionagem compartilham a característica de ocultação de sua instalação e funcionamento, sendo normalmente — ao menos em um momento inicial — executados a partir de outro programa que seja útil ou inofensivo ao usuário". RIBOLI, Eduardo Bolsoni. "Eu sei o que vocês fizeram no verão passado": o uso de software de espionagem como meio de obtenção de prova penal. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 27, n. 156, p. 91-139, jun.. 2019, p. 101-103.

[7] Para uma exposição sobre cada uma das funcionalidades dessas categorias de *malware*, ver: BATISTA, Lydie Jorge Batista. *O malware como meio de obtenção de prova*... Op. cit., p. 25-30.

em comum o fato de poderem ser instalados de forma dissimulada em um equipamento ou sistema informático, sem o conhecimento do seu utilizador, comprometendo as funções do meio invadido[8].

Alguns programas espiões, como os *keylogger* e *screenlogger*, registram toda a informação digitada no teclado pelo indivíduo, permitindo ao seu controlador ter conhecimento das atividades desenvolvidas por meio das teclas[9]. Outros *softwares* viabilizam o acionamento de *webcam* e microfone, com a consequente captação de sinais ópticos e acústicos do ambiente em que está localizado o equipamento informático invadido. Além disso, há aqueles que possibilitam a captura de dados de geolocalização do indivíduo, que pode ser realizada em tempo real e com o indivíduo em deslocamento, e até mesmo o monitoramento do fluxo das comunicações em tempo real de áudio ou texto, eludindo-se tecnologias de criptografia.

Por fim, importante ressaltar que os dispositivos ocultos podem necessitar de acoplamento físico a um sistema informático para serem executados. Ou, como tem sido mais comum nos dias atuais, podem ser instalados pela via exclusivamente digital, sem nenhum contato físico com os alvos e equipamentos os eletrônicos visados, por meio de e-mails com links falsos ou outros meios maliciosos.

2.2. *Malware* e a persecução penal.

A utilização de *malwares* em atividades investigativas é reivindicada sobretudo pelo elevado grau de eficiência que eles podem oferecer, ainda mais por se valer de um cenário de crescente integração de mecanismos informáticos ao cotidiano dos indivíduos e da utilização

---

[8] Apesar de determinados *malwares* terem ficado célebres por sua origem e utilização para fins ilícitos, algumas de suas aplicações podem ter uso comercial e estão legitimamente integradas ao dia a dia, podendo-se destacar a utilização de programas *spyware* nos processos de sondagem de hábitos de usuários de internet e de oferta de anúncios publicitários via *pop-ups*.

[9] Essa técnica, por exemplo, pode ser utilizada para a obtenção de senhas, inclusive para fins de decodificação de arquivos criptografados, permitindo também que mesmo aqueles textos digitados que venham a ser apagados ou armazenados sem o conhecimento de terceiros sejam conhecidos.

dos meios digitais para a prática de delitos. A diversidade e extensão dos dados e informações possíveis de serem acessados permite a eles alcançar resultados superiores àqueles que seriam obtidos pelos meios tradicionais de obtenção de prova. De fato, tais *softwares* viabilizam o acesso a elementos que dificilmente poderiam ser acessados por outras vias, permitindo inclusive o drible de mecanismos que elidem o acesso a informações contidas em sistemas informáticos, tais como a criptografia ou a dissimulação do IP do computador de onde a comunicação é realizada.

Entende a doutrina que a utilização do *malware* na seara processual-penal funcionará como um novo meio de investigação ou obtenção de prova, técnica que diz respeito, nas palavras de Antônio Magalhães Gomes Filho, "a certos procedimentos (em geral, extraprocessuais) regulados pela lei, com o objetivo de conseguir provas materiais, e que podem ser realizados por outros funcionários (policiais, por exemplo)"[10]. No âmbito do processo penal, esse artifício tem por finalidade o encontro de informações e elementos concretos que corroborem ou infirmem uma assertiva acerca da consumação de um fato penalmente típico.

Os meios de investigação de prova são, como regra, mecanismos extraprocessuais. Consistem em iniciativas que buscam localizar elementos, informações e dados pertinentes à verificação ou não de um fato determinado, que preexiste ao processo e cuja demonstração interessa a este. Diante disso, eventualmente, os meios de obtenção de prova são irrepetíveis e, após obtidos, são oportunamente juntados ao processo. Não raras vezes, ademais, eles são realizados por autoridades outras que não o juiz, mas os responsáveis pela fase investigativa da persecução penal, como policiais e membros do Ministério Público, a quem também é conferido um poder de investigação.

Os meios de investigação de prova são frequentemente operacionalizados sem o prévio conhecimento do sujeito contra o qual ele se

[10] GOMES FILHO, Antônio Magalhães. Notas sobre a terminologia da prova (reflexos sobre o processo penal brasileiro). In: YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide de (Orgs.). *Estudos em homenagem à professora Ada Pellegrini Grinover*. São Paulo: DPJ Editora, 2005, p. 309.

dirige, caracterizando-se pelo elemento surpresa[11], o que visa impedir a frustração do seu uso. Isso porque a prévia ciência do investigado poderia motivá-lo a destruir evidências ou interromper condutas delitivas ainda em prática e que estão sendo monitoradas. Nessas hipóteses, o contraditório não é realizado previamente à realização do meio de investigação de prova, mas diferido para momento posterior, desenvolvendo-se a diligência de forma oculta.

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. Isso significa que o controlador do *software* espião utiliza-se de um meio ardiloso para acessa o sistema informático-alvo e, de forma secreta, ter acesso aos dados e informações armazenadas e em processamento nesse sistema, além de operar diversas de suas funcionalidades, ocorrendo tudo isso em um cenário no qual diversas informações afetas à intimidade e privacidade do indivíduo poderão ser profundamente acessadas.

A segunda delas diz respeito à diversidade de *malwares* existentes, que dispõem de funcionalidades plurais e permitem o acesso a variados elementos dos sistemas informáticos invadidos. A possibilidade de utilização combinada desses *softwares* oferece um controle extenso sobre o conteúdo acessado, os hábitos *online* do usuário, as informações em processamento e comunicações realizadas e, inclusive, as ações, atividades, diálogos e deslocamentos geográficos realizados pelo indivíduo.

A terceira delas trata da operacionalização das funcionalidades inerentes ao sistema informático atingido. Após o invasor ter obtido acesso ao meio desejado, ele poderá operar diversos dos seus programas e funcionalidades, gerando dúvidas quanto à integridade dos dados e informações recolhidas.

---

[11] TONINI, Paolo. *A prova no processo penal italiano*. São Paulo: Revista dos Tribunais, 2002, p. 242-243.

A quarta delas guarda relação com a possibilidade de a vigilância recair sobre sistemas informáticos não visados, bem como indivíduos diversos aos desejados, fazendo com que dados e informações de terceiros estranhos sejam acessados e escrutinados.

A evolução das práticas criminosas, cada vez mais complexas, vertiginosas na utilização de meios digitais para sua consecução e, não raras vezes, desrespeitando barreiras territoriais, evidenciam ser incontornável e necessária a paralela evolução dos meios de obtenção de prova[12]: nesse cenário se inserem os *malwares* como meios de obtenção de prova que, embora mais invasivos da intimidade e vida privada, apresentam-se como veículos para conferir maior eficiência às investigações. O desafio que se apresenta é justamente o de se estabelecer um equilíbrio, dentro da ordem constitucional, entre emprego de *malwares* e a restrição a direitos fundamentais e garantias processuais que dele decorre[13]. Necessário, de

---

[12] Nesse sentido: "Así, el derecho de la prueba y a la prueba debe responder dinamicamente a los momentos evolutivos de la sociedade, y el sesarrollo tecnológico es uno de estos contextos de mayor evolución em las últimas décadas, com incidência plena en el comportamiento humano, por su recurrente trânsito a la interacción virtual" BUSTAMANTE RÚA, Mónica María; TORO GARZÓN, Luis Orlando. La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal,* v. 7, n. 2, p. 1347-1384, mai./ago. 2021, p. 1352.

[13] Manuel M. G. Valente, referindo-se a meios de obtenção de prova que ele denomina de "especializados, especiais e excecionais", exemplificando com a "ampliação do âmbito das interceções telefónicas, registo de voz off e imagem, gravações ambientais, gravações e fotografias por meio de câmaras de videovigilância, agentes infiltrados física e digitalmente, rastreios e persecuções digitais, localizações celulares, controlo e monitoramento concreto de IP, IMEI e GPS, recurso a IMSI-Carther(IMEI), buscas e apreensões preventivas no sistema digital a nível nacional, regional e internacional sem qualquer conhecimento do visado, e a admissibilidade e utilização como meios de prova os relatórios elaborados pelos serviços secretos", afirma que "Os textos assentam numa tónica central que devemos ter sempre no nosso pensamento jurídico-científico: as investigações preliminares, os meios ocultos de obtenção de prova e as novas tecnologias de comunicação representam uma restrição aos direitos, liberdades e garantias fundamentais pessoais, mas que se impõe como necessária e excecional na persecução de uma criminalidade organizada e estruturada nacional, regional e internacionalmente, e, por essa razão, as restrições inatas e inerentes a tais ações e meios devem, a par de uma rigorosa legislação, ser conformes ao quadro

início, breve incursão sobre os possíveis riscos a que sujeitos direitos fundamentais e garantias processuais em razão da utilização de *malwares* na seara investigativa criminal.

3. Reflexos do *malware* sobre o ordenamento jurídico.

3.1. O impacto sobre os direitos fundamentais dos indivíduos.

O uso de *malwares* em investigações criminais tem o potencial de comprometer direitos fundamentais constitucionalmente afirmados. No Brasil, por exemplo, os seus reflexos sobre a Constituição de 1988 podem ser identificados na afetação à intimidade, vida privada, honra e imagem do cidadão (art. 5º, X), à inviolabilidade do domicílio (art. 5º, XI) e ao sigilo das comunicações telemáticas (art. 5º, XII).

Isso se dá porque tais *softwares* permitem o acesso a uma grande variedade de dados e informações contidos no sistema informático alcançado (fotos, vídeos, informações bancárias, senhas, dados financeiros, arquivos e comunicações escritas etc), efeitos que podem ainda ser potencializados caso eles provoquem um acionamento da *webcam* e do microfone dos equipamentos eletrônicos, permitindo a capitação de imagens e sons de locais íntimos, bem como se associe a tecnologias de geolocalização[14], possibilitando um monitoramento contínuo do sujeito

jurídico-constitucional legitimo, válido, vigente e efetivo sob pena de negarmos o Estado constitucional democrático" VALENTE, Manuel M. G. Editorial dossiê "Investigação preliminar, meios ocultos e novas tecnologias". *Revista Brasileira de Direito Processual Penal,* vol. 3, n. 2, p. 473-482, mai./ago. 2017, p. 474 e 481.

[14] Como adverte Carlos Hélder C. Furtado Mendes: "A modalidade de investigação por geolocalização não corresponde a qualquer forma de interceptação. Primeiro, pelo fato de que monitorar as coordenadas espaço-temporais do sujeito não corresponde a interceptação de fluxo de dados entre pessoas. De um lado se tem como objeto de aquisição o conteúdo de uma comunicação entre duas ou mais pessoas, de outro a posição e o movimento de uma pessoa ou coisa." MENDES, Carlos Hélder C. Furtado. *Tecnoinvestigação criminal*: entre a proteção de dados e a infiltração por *software*. Salvador: Juspodivm, 2019, p. 206.

investigado, com mapeamento de todos os seus deslocamentos e o acesso à multiplicidade de suas comunicações.

Há vasta jurisprudência estrangeira que versa sobre o emprego de *malwares* em atividades investigativas na seara processual-penal. No âmbito norte-americano, por exemplo, as primeiras experiências remontam à década de 1990, quando da utilização pelo FBI de um *malware* chamado *Carnivore*[15]. Naquele país, o emprego de *malware* situa-se no âmbito da quarta emenda, que proíbe a busca domiciliar sem decisão judicial e sem uma justa causa. A discussão é jurisprudencial e está centrada no critério da expectativa razoável de privacidade. Caso determinada medida ofenda essa expectativa, deve haver um mandado judicial amparado em uma causa provável[16].

Diferentemente do que ocorre no âmbito norte-americano, os ordenamentos jurídicos europeus têm evoluído para exigir a necessidade de lei para o emprego de *malwares* em investigações

[15] Para mais informações, vide https://www.aclu.org/press-releases/fbi-renames-carnivore-internet-wiretap

[16] Um bom exemplo da aplicação do critério da razoável expectativa de privacidade é o caso *United States vs. Nicodemo S Scarfo e Frank Paolercio*. Nesse caso, o FBI de Nova Jersey obteve autorização judicial para acessar e instalar por sessenta dias um *keylogger* em um computador que acessava um banco de dados denominado Factors. Em razão disso, os agentes daquele departamento investigativo iam de tempos em tempos ao escritório do suspeito visando obter senhas e diversas outras informações relevantes. Embora a defesa tenha suscitado que tal atuação superou os limites do mandado, dado que o dispositivo implantado registrou tudo o que foi digitado enquanto a autorização se deu apenas para o acesso àquele código, o Tribunal negou o requerimento da defesa sob o fundamento de que não houve interceptação de comunicações. Posteriormente, sobrevieram diversos outros casos jurisprudenciais sempre em torno do mesmo parâmetro da razoável expectativa de privacidade.

criminais, como ocorre, por exemplo, na Itália[17], na Espanha[18], na França[19] e em Portugal[20].

Embora escape dos objetivos do presente artigo esmiuçar experiências e casos internacionais de emprego de *malwares*, cumpre tratar especificamente de um precedente da Alemanha que teve grande influência na compreensão do tema em nosso país. Em 2008, a Corte Constitucional alemã julgou reclamação constitucional ajuizada contra dispositivos da Lei de Proteção da Constituição do Estado de Nordrhein-Westfalen que permitiam "às autoridades locais de inteligência fazerem a busca remota

---

17 Na Itália, o malware chegou a ser admitido por julgados oscilantes da Corte de Cassação sem lei específica. Posteriormente, foi editada lei sobre a matéria. Vide CAPPARELLI, Bruna. Técnicas investigativas italianas articuladas com a utilização dos denominados captadores informáticos: qui custodiet custodes? *Revista Brasileira de Ciências Criminais*, São Paulo, v. 137, p. 253-286, nov. 2017; CAPRIOLI, Francesco. O "captador informático" como instrumento de busca da prova na Itália. Revista Brasileira De Direito Processual Penal, Porto Alegre, v. 3, n. 2, p. 483-510, mai./ago. 2017.

18 A operacionalização de malwares em atividades investigativas na Espanha vinha sendo autorizada pelo meio judicial antes mesmo da entrada em vigor de uma norma reguladora, a Ley Orgánica 13/2015, de 05 de outubro de 2015, que acrescentou novos dispositivos à Ley de Enjuiciamiento Criminal.

Vide: VACIAGO, Giuseppe; RAMALHO, David Silva. Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings. Digital Evidence and Eletronic Signature Law Review, v. 13, 2016; ALAMILLO, Javier Rubio. La informática en la reforma de la Ley de Enjuiciamiento Criminal. Diario La Ley, n. 8662, 2015; PÉREZ ESTRADA, Miren Josune. La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 5, n. 3, p. 1297-1330, set./dez. 2019.

19 Na França, o malware passou a ser regulado pela loi nº 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure

20 Vide ALVES, Daniel Bento. Uso de *malware* em investigação criminal. *Actualidad Jurídica Uría Menéndez*, v. 16, n. 47, p. 19-30, out./dez. 2017.

de informações e o monitoramento online de computadores de suspeitos de cometerem práticas criminosas"[21] (BVerfGE 120, 274)[22].

Não obstante a base constitucional para o questionamento da referida norma tenha sido o direito fundamental à autodeterminação informativa, reconhecido no histórico precedente BVerfGE 65[23], de 1983, sobre a lei do censo, a Corte Constitucional alemã entendeu por reconhecer um novo direito fundamental: o da confiabilidade e da integridade dos sistemas informáticos, o qual deveria abranger equipamentos que armazenam dados e informações e que, em alguma medida, pudessem refletir a imagem da personalidade do indivíduo[24].

Isto é, para além dos dados e informações contidos em um determinado sistema, deveria também haver uma proteção inerente ao próprio dispositivo informático. Nas palavras de Luis Grego e Orlandino Gleizer, "o Tribunal constrói, assim, um novo direito fundamental, com um âmbito de proteção próprio, para dar conta de novos setores em que

---

21 MENDES, Laura Schertel. Uso de softwares pela polícia: prática legal? Programas permitem controle remoto da câmera e microfone do aparelho, JOTA, 2015. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015. Acesso em: 20/06/2022.

22 Disponível em: <https://www.servat.unibe.ch/dfr/bv120274.html>. Acesso em: 22 mai. 2022.

23 Disponível em: <https://www.servat.unibe.ch/dfr/bv120274.html>. Acesso em: 22 mai. 2022. A Corte declarou a lei do censo inconstitucional por autorizar que o Estado realizasse o cruzamento de dados coletados dos cidadãos para aferição da distribuição geográfica da população, permitindo um processamento automático daqueles elementos e restringindo o direito dos indivíduos em ter ciência e decidir sobre quais deles deseja divulgar. A decisão garantiu aos cidadãos proteção contra a recolha, armazenamento, uso e transmissão ilimitada de dados pessoais, salvo na hipótese de interesse geral da comunidade e sempre dentro dos limites da Constituição. Surgiu, assim, o direito à autodeterminação informativa, nos moldes que se espraiaram por diversos ordenamentos jurídicos

24 Posteriormente, por ocasião do julgamento do BVR 966/09, a Corte Constitucional alemã julgou constitucional a Lei de Prevenção dos Perigos do Terrorismo Internacional pelo Departamento Federal de Investigações (BKA) que permitiu o emprego de *malware* apenas para os delitos de terrorismo.

a personalidade tem de poder livremente desenvolver-se e dos novos perigos que ali se põe".[25]

Esse importante precedente da Corte Constitucional alemã evidencia que as repercussões do *malware* em investigações criminais alcançam, portanto, não apenas aqueles direitos fundamentais já historicamente conhecidos, como também outros que estão sendo desenvolvidos por razão da evolução das tecnologias de informação e a consequente necessidade de proteção de dados pessoais.

3.2. O impacto sobre as garantias processuais do acusado.

Para além dos direitos fundamentais, a utilização de *malwares* em investigações criminais também tem o potencial de oferecer sensíveis riscos a diversas garantias processuais.

Os dados digitais notabilizam-se por sua efemeridade, vez que podem ser alterados e suprimidos com facilidade, além de poderem ser acessados a partir de equipamentos conectados em rede. Tal realidade, associada à constatação de que o operador do *malware* pode controlar várias funcionalidades do sistema informático invadido, levanta questionamentos quanto à confiabilidade e integridade dos dados e informações colhidos por meio de um *software* malicioso, cujas implicações impactam o exercício da garantia do contraditório e ampla defesa.

As funcionalidades dos *malwares* permitem também a sua utilização em investigações com caráter prospectivo, isto é, sem identificação mínima de possíveis suspeitos e relativa a delitos que podem sequer ainda ter se consumado[26]. Tais situações, contudo, levantam

---

[25] GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal*, vol. 5, n. 3, p. 1483-1518, set./dez. 2019, p. 1493.

[26] Mais uma vez, as investigações realizadas pelo FBI envolvendo o site de pedofilia *Play Pen* serve de ilustração. No bojo de referida investigação e com a utilização de *malwares* o FBI monitorou inúmeros usuários do site para investigar quais deles eram reais consumidores de pornografia infantil e autores de delitos de natureza criminal. ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. E quando o policial vira hacker? As principais justificativas, técnicas e discussões jurídicas sobre hacking estatal. Disponível em: <https://www.

questionamentos sobre os limites da ação do Estado na realização da persecução penal, especialmente quando ausente alguma regulamentação acerca da utilização de um *software* malicioso. Isso porque a sua operacionalização pode jamais chegar ao conhecimento do investigado, dificultando a ciência por parte dele quanto à real origem das provas obtidas em seu desfavor e, consequentemente, obstaculizando o exercício da sua defesa e a produção de eventual contraprova. Para além disso, terceiros que não estão relacionados aos fatos investigados e sobre os quais não pesa qualquer suspeita real podem acabar sendo atingidos pelas medidas investigativas.

Outra dificuldade é no tocante à identificação do juiz natural responsável pela apreciação do requerimento de uso do *malware*. Isso porque o uso da internet permite que os sistemas informáticos conectem diversos equipamentos eletrônicos em redes de diferentes extensões e complexidades. Soma-se a isso o fato de que a armazenagem de dados não se faz mais exclusivamente no interior de um equipamento, mas de forma externa, nas denominadas nuvens, bem como que existem expedientes de navegação na rede mundial de computadores que visam justamente fazer a ocultação do equipamento informático que realizou uma ação e do local onde está situado o usuário.

Por fim, afirma-se que princípio do *nemo tenetur se detegere* igualmente estaria sob risco de indevidas constrições em razão da invasividade dos *softwares* espiões, que permitem o monitoramento audiovisual de condutas realizadas nos ambientes de maior intimidade do indivíduo e nos quais ele tem uma real expectativa de não estar sendo visto ou ouvido[27]. Logo, como o emprego do meio investigativo não é do conhecimento do investigado, coloca-se em dúvida se em tais circunstâncias uma declaração autoincriminadora, por exemplo, poderia ser admitida e valorada em seu desfavor.

---

internetlab.org.br/pt/privacidade-e-vigilancia/e-quando-o-policial-vira-hacker/>. Acesso em: 22 mai. 2022.

[27] MENDES, Carlos Hélder C. Furtado. Tecnoinvestigação criminal... Op. cit., p. 96.

4. (A)tipicidade dos *malwares* no Brasil como meio de obtenção de prova.

O emprego de meios de obtenção de prova, geralmente e em diferentes graus, restringe direitos fundamentais e garantias processuais constitucionalmente asseguradas. Em razão disso, apesar de no ordenamento jurídico brasileiro viger o princípio da liberdade na produção da prova, na conformidade do art. 369 do Código de Processo Civil, aplicável analogicamente ao processo penal, há posicionamentos no sentido de que somente meios de obtenção de prova legalmente previstos poderiam ser utilizados no âmbito processual penal[28]. O rol dos meios de obtenção de prova seria, assim, taxativo.

Nesse sentido, distinguir-se-iam os meios de obtenção de prova típicos daqueles atípicos. Os típicos, são os previstos no ordenamento jurídico por meio de uma norma legal autorizadora e regulamentadora do respectivo procedimento. A atipicidade, por sua vez, pode ser de duas ordens: ou o meio de obtenção de prova não está previsto legalmente em absoluto, ou, embora haja norma autorizadora da sua utilização, não há disciplina legal que indique hipóteses de cabimento, pressupostos e limites para que isso ocorra[29]. Em caso de atipicidade dos meios de investigação de prova, questiona-se a legitimidade da sua utilização mediante a aplicação analógica de dispositivos relativos a meios de investigação de prova típicos[30].

---

[28] Nesse sentido, vide: MORAES, Maurício Zanoide de. *Presunção de inocência no processo penal brasileiro*: análise de sua estrutura normativa para a elaboração legislativa e para a decisão judicial. Rio de Janeiro: Lumen Juris, 2012, p. 315-316.

[29] Segundo Guilherme Madera Dezem, "tem-se que uma prova é atípica em duas situações: (1) quando ela seja prevista no ordenamento, mas não o seja seu procedimento probatório; (2) quando nem ela nem seu procedimento probatório sejam previstos em lei". DEZEM, Guilherme Madeira. *Curso de Processo Penal*. São Paulo: Revista dos Tribunais, 2015, p. 445.

[30] A possibilidade de utilização da analogia para legitimar a operacionalização de meios de obtenção de prova é relevante no que tange às novas tecnologias de comunicação e informação, na medida em que a legislação não consegue acompanhar a velocidade com que tais técnicas evoluem. Nesse sentido, Gianluca Martins Smanio observa que novas tecnologias ou o uso inovativo de técnicas já existentes costuma surgir na rotina dos agentes policiais. É

No que se refere ao uso de *malwares*, a discussão centra-se justamente em verificar se a sua utilização se coaduna, ainda que por aplicação analógica, com algum dos meios de obtenção de prova já regulamentados, ou, diversamente, se é necessária prévia regulamentação legal para tanto.

A esse respeito, Gustavo Soares Torres defende que inovações tecnológicas que ainda não tenham sido reguladas como meio de investigação devem ser toleradas de forma excepcional, desde que encontrem espaço em "condutas investigativas análogas ou fruto da interpretação extensiva de instrumentos já consolidados no ordenamento jurídico"[31].

Tratando especificamente dos *malwares*, Diego Roberto Barbiero defende que, enquanto não há legislação que autorize o uso de tal meio de investigação, é possível concretamente empregá-lo em casos complexos que envolvam crime organizado e organizações criminosas. Isso se daria porque "impedir o uso da tecnologia investigativa por não haver o Poder Legislativo, até o momento, deliberado sobre o tema de forma individualizada e concreta resulta, em larga medida, no desbalanceamento das forças de segurança em relação às da criminalidade organizada"[32] Diante desse posicionamento, o autor entende ser cabível a interpretação extensiva

somente num segundo momento, diante da eventual difusão do uso de uma nova técnica, que questionamentos acerca da sua eventual atipicidade, da possibilidade de utilização de analogia ou da necessidade de sua regulamentação própria exsurgem. Nesse interim, pode ocorrer que novas tecnologias sejam empregadas na seara investigativa sem prévia regulamentação, de forma que "deve-se observar que não se pode ser conivente com o uso da nova técnica sem regulamentação legislativa por muito tempo, por estarmos tratando de restrições a direitos fundamentais cada vez mais intensas permitidas pelas novas tecnologias da informação". SMANIO, Gianluca Martins. *A vigilância policial em meio digital*... Op. cit., p. 158.

[31] SOARES, Gustavo Torres. *Investigação criminal e inovações técnicas e tecnológicas*. Belo Horizone: D' Plácido, 2020, p. 327.

Nesse caso, o método investigativo poderia ser empregado, mesmo impactando direito fundamentais, "obedecido o mandamento de proporcionalidade, seja compensado seu déficit de regulamentação por método judicial que a trate como praeter legem, excepcional, provisória, decorrente de interpretação extensiva ou aplicação analógica e inserida em contexto de evolução legislativa progressiva".

[32] BARBIERO, Diego Roberto. *Implantação de Malwares em Investigações Complexas*. Curitiba: Juruá, 2021, p. 139.

por ser semelhante à interceptação telefônica, a busca e apreensão, a captação de sinais sonoros, e cabível ao juiz deferir a medida, desde que necessária, adequada e proporcional[33].

Por sua vez, Greco e Gleizer propugnam, de modo contrário, que "se quisermos dotar as nossas instâncias persecutórias de uma faculdade de intervir nesse direito [confiabilidade e integridade dos sistemas informáticos], precisaremos, assim, de lei específica".[34]

Assim, diante de tal controvérsia, passa-se nos tópicos seguintes, a verificar se é possível encaixar o *malware* nos referidos ordenamentos legais com o fim de se responder à inicial formulada no presente artigo.

4.1. O *MALWARE* COMO BUSCA E APREENSÃO?

Em primeiro lugar, convém verificar se o *malware* pode ser analogicamente considerado um meio de busca domiciliar, tal como ocorre nos Estados Unidos da América.

A respeito de tal hipótese, Eduardo Guardia consigna que não existe um regime apropriado para a busca de prova digital e que "a precisão terminológica exige diferenciação entre as diversas operações técnicas que viabilizam a obtenção de dados digitais". Isso porque "os processos de busca, captação, registro e monitoramento de dados, demandam atuações específicas dos órgãos policiais, que repercutem de modo particular nos direitos e garantias individuais".[35]

Ademais, tanto a previsão constitucional do art. 5º, inciso XI, quanto a disciplina do Código de Processo Penal são bastante específicos em tratarem da proteção da casa, do domicílio. É impossível, nesse contexto, comparar casa com dispositivo informático, sobretudo porque a Constituição de 1988, diferentemente da norte-americana,

---

[33] BARBIERO, Diego Roberto. *Implantação de Malwares*... Op. cit., p. 150.

[34] GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal... Op. cit., p. 1498.

[35] 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.

estabeleceu um campo de proteção próprio para os dados, no âmbito do art. 5º, inciso XII.

Outro argumento interessante para afastar essa analogia foi dado por Luiz Augusto Sartori de Castro. Segundo o autor, é indevida qualquer hipótese de encaixe do *malware* na disciplina legal da busca domiciliar, uma vez que tanto o sistema constitucional como legal identifica a busca como um meio invasivo de atuação do estado que deve ser implementado de forma ostensiva. Nesse contexto, a Constituição exige que a medida seja diurna e o Código de Processo Penal impõe que a entrada no domicílio seja tentada com o consentimento do morador e que seja garantida a presença de testemunhas. Tais características reforçam que a busca domiciliar não é um meio de investigação oculto. Diante disso, Castro afirma que é vedado "o uso de meio fraudulento ou artificioso visando reduzir a percepção do acusado quanto à efetiva realidade dos fatos, justamente o que ocorre quando se usa um malware para propiciara realização de uma busca e apreensão".[36]

Diante de tais considerações, fica claro não haver encaixe do emprego de malware na sistemática da busca domiciliar.

4.2. O *malware* na Lei n. 9.296/1996?

A Lei n. 9.296/1996 trata da interceptação do fluxo de comunicações em sistemas de informática e telemática para o uso em investigações criminais e em instrução processual penal. Ao passo que o primeiro sistema consiste no tratamento das informações por meio do uso de equipamentos e procedimentos na área de processamento e dados, o segundo diz respeito à manipulação e utilização da informação mediante o uso combinado do computador e meios de telecomunicações[37].

Para a utilização dessa técnica, é necessária uma autorização judicial e o preenchimento dos requisitos legais previstos no art. 2º da norma: (i) a existência de indícios razoáveis da autoria ou participação em infração penal; (ii) a prova não puder ser feita por outros meios

[36] 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, p. 7.

[37] BADARÓ, Gustavo Henrique. *Processo Penal*. 2ª ed. Rio de Janeiro: Elsevier, 2014, p. 357.

disponíveis; e (iii) o fato investigado constituir infração penal punida, no mínimo, com pena de reclusão. Uma questão importante a seu respeito é o fato de que ela apenas abrange aquelas comunicações caracterizadas por sua instantaneidade, realidade presente nas comunicações telefônicas e em determinados tipos de dados. O acesso a correspondências, comunicações telegráficas e dados não instantâneos, quando desejados, deverá ocorrer pela via das medidas de busca e apreensão.

Disso já se vê, portanto, as limitações e diferenças que permeiam o emprego desse meio de obtenção de prova se comparado ao *malware*. De início, deve-se ponderar que, na interceptação telemática ou telefônica, o acesso à informação interceptada faz-se por expediente técnico externo ao sistema informático alvo; diferentemente, quando se utiliza um *malware*, o responsável pela infiltração insere-se num dos sistemas informáticos, isto é, naquele responsável pela emissão ou recepção da informação. Via de consequência, o agente malicioso possibilita uma coleta de dados muito mais ampla e invasiva do que aquela realizada a partir dos meios de obtenção de prova disciplinados na Lei n. 9.296/1996; para além da captação de um tráfego específico de dados, por vezes codificado e cujo conteúdo permanecesse inacessível, o *software* permite a coleta mais ampla deles, com possibilidade de acesso ao conteúdo decodificado das comunicações assim como aos dados que permaneçam armazenados no sistema informático [38-39]. Sob uma perspectiva constitucional, é possível ainda dizer que enquanto a interceptação das comunicações incide diretamente sobre o direito à livre comunicação, a esfera de afetação do *malware* é maior, posto que também recai sobre o direito à intimidade e à imagem.

---

[38] MENDES, Laura Schertel. Uso de softwares espiões pela polícia: prática legal? **Jota**, 2015. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015>. Acesso em: 22 mai.05. 2022.

[39] Carlos Hélder C. Furtado Mendes observa 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 ative), na medida em que permite a interceptação após sua decodificação internamente nos dispositivos informáticos" Tecnoinvestigação criminal*: ... Op. cit., p. 175.

Logo, a Lei n. 9.296/1996 não pode funcionar como fundamento para o emprego do *malware* no Brasil, sob pena de ampliar de forma desmedida o âmbito de abrangência dessa norma, autorizando o seu uso para fins que não são por ela previstos.

4.3. O *malware* na Lei n. 12.850/2013?

A Lei n. 12.850/2013 disciplinou alguns meios de obtenção de prova que poderão ser utilizados para investigar organizações criminosas e delitos correlatos. Um primeiro deles, que está descrito no art. 10 da norma, previu a figura do agente infiltrado, o qual "pode ser entendido como o funcionário de investigação criminal ou um terceiro (subordinado à polícia) que atua ocultando sua qualidade, visando conquistar a confiança dos possíveis criminosos e, consequentemente, à obtenção de provas que possam incriminá-los"[40]. Consoante já afirmou a jurisprudência do STF em paradigmático julgamento envolvendo a diferenciação entre agente infiltrado e agente de inteligência, enquanto a atuação daquele "possui finalidades repressivas e investigativas, visando à obtenção de elementos probatórios relacionados a fatos supostamente criminosos e organizações criminosas específicas", a deste último "tem uma função preventiva e genérica, buscando informações de fatos sociais relevantes ao governo"[41].

---

[40] GONÇALVES, Vinícius Abdala. *O agente infiltrado frente ao processo penal constitucional*. Belo Horizonte: Arraes, 2014, p. 12.

[41] Nesse sentido foi o que afirmou a 2ª Turma do STF ao julgar o HC 147.837, em 16.02.2019, cujo acórdão foi relatado pelo Ministro Gilmar Mendes. Sobre a diferenciação entre agente infiltrado e agente de inteligência no âmbito da segurança pública, Luis Fernando de França Romão sustenta que "*i)* a infiltração é apenas um método de trabalho, comum tanto às atividades de Inteligência quanto às investigações criminais; *ii)* a lei veda a infiltração de agentes policiais de Inteligência no âmbito de investigação criminal, não no âmbito das atividades de Inteligência; *iii)* a finalidade e a amplitude da ação policial são critérios para distinção entre a infiltração em ação de Inteligência (função preventiva e voltada às complexidades das conjunturas sociais) e a efetuada em investigação criminal (reativa, concentrada em apuração exclusiva dos fatos imputados e de que pode decorrer prisão); *iv)* a fiscalização judicial é critério distintivo da ação de infiltração de agentes policiais em tarefa de investigação, e exige-se decisão judicial prévia nos termos da Lei nº 12.850/2013; *v)* como só a infiltração do agente policial no âmbito da

A partir da Lei n. 13.964/2019, a referida norma passou a também admitir em seus arts. 10-A, B, C e D a ação de "agentes de polícia infiltrados virtuais", modalidade que, por agir sobre um ambiente virtual, guarda maior aproximação com o *malware*. Esse meio de obtenção de prova somente poderá ser utilizado após uma autorização judicial e ante o preenchimento dos requisitos previstos nos arts. 10, *caput*, e 10-A da Lei n. 12.850/2013, consistentes: (i) na existência de indícios de infração penal; (ii) a prova não puder ser produzida por outros meios disponíveis; (iii) estiver demonstrada a necessidade dessa medida e (iv) forem indicados o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas.

O ordenamento jurídico brasileiro admitiu, portanto, a criação de perfis falsos pelas autoridades investigativas a fim de que elas estabeleçam relações de confiança em um ambiente criminoso virtual, bem como se integrem na atividade criminosa, com o intuito de obter informações. Vale destacar que a novidade da lei não está na criação de um perfil falso e a consequente obtenção de informações públicas dos usuários na internet (fotos, mensagens, endereço, nomes de amigos e familiares etc.), uma vez que a coleta de dados em fontes abertas já era possível mesmo sem autorização judicial. A particularidade do agente infiltrado virtual é que ele poderá atuar no sentido de obter dados alocados na internet de forma

investigação criminal passa por controle judicial, é vedado o compartilhamento em investigação criminal de informações provenientes de infiltração de agentes de Inteligência; *vi)* embora o meio excepcional de obtenção de prova da infiltração de agentes policiais seja cabível apenas nas persecuções penais de delitos relacionados a organizações criminosas, os procedimentos probatórios regulados pela Lei nº 12.850/2013 devem ser respeitados por analogia em casos de omissão legislativa, e há incidência legítima para exigir prévia autorização judicial do agente policial para obtenção de prova em investigações criminais que envolvam outros delitos, como o de associação criminosa, verificado no caso *Black blocs*". ROMÃO, Luis Fernando de França. Agente infiltrado e agente de inteligência: distinções a partir de estudo de caso julgado pelo Supremo Tribunal Federal. *Revista Brasileira de Inteligência*, Brasília, v.16, n. 14, p. 85-99, 2019, p. 96-97.

restrita, isto é, aqueles nos quais o interlocutor renuncia à sua intimidade em razão da confiança depositada em um terceiro[42].

A despeito de tal inovação que foi trazida na Lei n. 12.850/2013, a utilização do *malware* não poderá ser realizada a partir do regime jurídico previsto para o agente infiltrado virtual. Isso porque aquela norma não trata especificamente da implantação de um agente malicioso no dispositivo informático de um terceiro com o objetivo de acessar os dados e informações que estão nele armazenados ou sendo a partir dele produzidos[43]. Diante disso, e em sendo o *malware* uma técnica investigativa bastante invasiva, não é possível a realização de uma interpretação ampla do conceito de infiltração sem que isso implique uma violação ao princípio da legalidade processual.

Outra figura retratada na Lei n. 12.850/2013 e cuja diferenciação é importante de ser feita em relação ao *malware* corresponde à ação controlada, que está regulada no art. 8º da norma. Segundo Fernanda Regina Vilares:

> "A ação controlada consiste no retardamento da atuação estatal com relação à prática delituosa cometida por membros de organização criminosa sob a condição de mantê-la (a prática criminosa) sob vigilância policial com o escopo de efetivar a atuação policial no momento mais oportuno no que tange à obtenção de informações para subsidiar a investigação criminal. Há uma flexibilidade diante da flagrância delitiva para tentar aumentar a eficiência da investigação."[44]

---

[42] CASTRO, Henrique Hoffmann Monteiro de. Lei 13.441/17 instituiu a infiltração policial virtual. Disponível em: <https://www.conjur.com.br/2017-mai-16/academia-policia-lei-1344117-instituiu-infiltracao-policial-virtual>. Acesso em: 22 mai. 2022.

[43] ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. E quando o policial vira hacker? As principais justificativas, técnicas e discussões jurídicas sobre hacking estatal. Disponível em: <https://www.internetlab.org.br/pt/privacidade-e-vigilancia/e-quando-o-policial-vira-hacker/>. Acesso em: 22 mai. 2022.

[44] VILARES, Fernanda Regina. *Ação controlada*: limites para as operações policiais. Belo Horizonte: D'Plácido, 2017, p. 50.

A despeito de o inciso III do art. 3º da Lei n. 12.850/2013 qualificar a ação controlada como sendo um meio de obtenção de prova, a professora paulista sustenta, com acerto, que tal expressão, na verdade, "indica o controle e a vigilância que as autoridades devem manter sobre a prática criminosa para colher o maior número de elementos informativos possível, sem que a situação flagrancial desapareça"[45], não se tratando propriamente de um meio de obtenção de prova. A ação controlada seria, portanto, um método, e não uma técnica, porquanto ela não se refere "ao conjunto de meios de obtenção de prova e técnicas de investigação eleitos pela autoridade policial para solucionar uma 'situação indeterminada'", apesar de esses meios poderem vir a ser utilizados para procurar e extrair dados relevantes durante o processo de monitoramento estatal[46].

Disso se depreende que a ação controlada dispõe de uma natureza mais ampla do que qualquer meio de obtenção de prova sigiloso existente, inclusive aquele decorrente do uso de agentes maliciosos, não se confundindo com essas medidas. É dizer, a ação controlada é um método que poderia se valer de tais *softwares* como uma técnica a ser utilizada em investigações contra organizações criminosas, não consistindo em um fundamento legitimador da sua utilização. Todavia, ante a inexistência de uma norma autorizadora ou reguladora do *malware* no Brasil, sequer a sua utilização é possível de ser feita no transcurso de uma ação controlada.

Logo, tampouco a ação controlada prevista na Lei n. 12.850/2013 respalda a utilização do *malware* no ordenamento jurídico nacional.

4.4. O *malware* na Lei n. 8.069/1990?

A Lei n. 8.069/1990 dispõe sobre o Estatuto da Criança e do Adolescente e dá outras previdências. A partir da Lei n. 13.441/2017, essa norma passou a prever em seus arts. 190-A, B, C, D e E a possibilidade de "infiltração de agentes de polícia na internet para a investigação de crimes contra a dignidade sexual de crianças e adolescentes", figura bastante similar àquela prevista na Lei n. 12.850/2013.

---

45 VILARES, Fernanda Regina. *Ação controlada*... Op. cit., p. 51.

46 VILARES, Fernanda Regina. *Ação controlada*... Op. cit., p. 51-52.

A utilização desse agente infiltrado dependerá de autorização judicial, sendo que os requisitos para a sua realização, estão disciplinados no art. 190-A da norma: (i) a demonstração da necessidade da medida; (ii) a indicação do alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas; (iii) a prova não puder ser produzida por outros meios e (iv) a investigação disser respeito aos crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D da Lei n. 8.069/1990, bem como nos arts. 217-A, 218, 218-A e 218-B do Código Penal.

O agente infiltrado da Lei n. 8.069/1990 tampouco poderá se valer de um *malware* para promover uma investigação, haja vista que esta norma igualmente não trata especificamente do emprego de dispositivos espiões em atividades daquela natureza. Diante desse cenário, e do fato de que a referida técnica traz consigo significativos impactos sobre a esfera de intimidade e à imagem dos indivíduos, o seu emprego sobre tais contornos legais implicaria uma violação ao princípio da legalidade processual.

5. Caminhos para a implantação do *malware* no Brasil.

Na atual conformação do ordenamento jurídico nacional, não existe um corpo normativo que regule ou autorize a utilização do *malware* em investigações criminais[47]. Tal realidade, somada à constatação de que o uso de *softwares* maliciosos representa risco de restrições sérias a direitos fundamentais e garantias processuais, implica sua inadmissibilidade como um meio de obtenção de prova[48].

---

[47] Em consulta ao sítio eletrônico dos Tribunas Federais e Estaduais de 2ª instância, bem como do STJ e STF mediante a utilização dos termos '*malware*' e '*software* malicioso', as ações judiciais que foram identificadas relativas ao uso do *malware* não estão vinculadas ao seu emprego por uma autoridade investigativa, mas sim a fraudes realizadas por terceiros mediante a instalação de um vírus no dispositivo eletrônico da vítima, em regra visando a subtração de dinheiro de contas bancárias.

[48] ALVES, Daniel Bento. Uso de *malware* em investigação criminal... Op. cit., p. 21.

Diante disso, para que a operacionalização de *malwares* seja possível na seara investigativa do Brasil, é necessário que o legislador discipline um comando legal específico nesse sentido (*nulla coactio sine lege*)[49], medida que servirá para conter abusos pelo Estado e servir como um instrumento de garantia aos cidadãos[50].

A regulação do *malware* em lei ainda possibilitará uma adequada operacionalização deste particular meio de obtenção de prova segundo a regra da proporcionalidade. Com efeito, nada obstante a proteção da intimidade e da privacidade esteja constitucionalmente resguardada no Brasil, o que também encontra referência em diversas esferas do sistema global de proteção e defesa dos direitos humanos[51], é verdade que as variadas estratégias atualmente existentes para o acesso de informações em uma investigação criminal não guardam a mesma intensidade e invasividade se comparadas àquela possibilitada pelo agente malicioso. Nestes casos, os requisitos exigidos para a autorização da medida investigativa devem ser articulados a partir das próprias características diferenciais desta técnica, que guardam um caráter excepcional, a modo de contemplar a adequação, necessidade e proporcionalidade (em sentido estrito) que se esperam na sua utilização[52].

---

[49] LOPES JR, Aury; MENDES, Carlos Hélder Carvalho Furtado. "Vírus espião" como meio de investigação: a infiltração por *softwares*. Disponível em: <https://www.conjur.com.br/2019-jun-07/limite-penal-virus-espiao-meio-investigacao-infiltracao-softwares>. Acesso em: 22 mai. 2022.

[50] Segundo Paulo Pinto de Albuquerque, "quando o meio de obtenção de prova implicar um elevado grau de intrusão na privacidade do suspeito (ou um potencial aditivo de perigo inerente ao ataque aos direitos fundamentais (...), ele deve ser previsto por uma lei expressa". ALBUQUERQUE, Paulo Pinto. *Comentários do Código de Processo Penal*. Lisboa: Universidade Católica Editora, 2011, p. 332.

[51] ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. *Revista de Investigações Constitucionais*, Curitiba, v. 4, n. 3, p. 167-200, set./dez. 2017, p. 171-173.

[52] A regra da proporcionalidade deve ser compreendida a partir de três subelementos diversos e independentes: adequação, necessidade e proporcionalidade em sentido estrito. O meio será "adequado" quando ele promover o fim buscado; será "necessário" quando a realização do objetivo perseguido não puder ser promovido, com a mesma intensidade, por meio de outro ato que limite, em menor medida, o direito fundamental atingido; e haverá uma

A importância de uma reserva de lei em relação a esta matéria pode ser verificada, por exemplo, a partir da experiência de Portugal. Por ocasião da aprovação da Lei do Cibercrime (Lei nº 109/2009, de 15 de setembro), instalou-se um debate quanto à admissibilidade ou não do uso do *malware* como um meio de obtenção de prova naquele país, e até mesmo com relação a qual dispositivo legal teria instituído essa previsão (se o art. 15º ou o art. 19º, nº 2, da norma)[53]. Além disso, mesmo os autores que entendem ser possível o uso de agentes maliciosos a partir da referida lei são críticos ao regime a eles aplicável, apontando a sua inconstitucionalidade[54].

Tal cenário, para além de dar causa a uma grande insegurança jurídica, pode ensejar uma indevida violação de direitos fundamentais de terceiros. Por essa razão é que a previsão em lei de um regime jurídico próprio ao *malware* deve ocorrer de forma conjunta à formalização de um conjunto de garantias que visem regular o seu uso, tanto no plano

---

"proporcionalidade em sentido estrito" quando um sopesamento entre a intensidade da restrição ao direito fundamental atingido e a importância da realização do direito fundamental que com ele colide e que fundamenta a adoção da medida restritiva revelar uma maior vantagem na promoção da medida. SILVA, Virgílio Afonso da. O proporcional e o razoável. *Revista dos Tribunais*, São Paulo, v. 91, n. 798, p. 23-50, 2002, p. 36-41.

53 Nesse sentido, vide: ALVES, Daniel Bento. Uso de *malware* em investigação criminal... Op. cit., p. 25-30. BATISTA, Lydie Jorge. *O malware como meio de obtenção de prova*... Op. cit., p. 123-131.

54 Nesse sentido, David Silva Ramalho, que admite a possibilidade de uso de *malware*, sustenta (i) que não existe uma regulação clara e precisa das suas condições e pressupostos; (ii) que não é feita uma definição dos tipos de dados que podem ser apreendidos e da finalidade possível de ser conferida ao seu uso; (iii) que o catálogo de crimes possíveis de autorizar a utilização de um agente malicioso é excessivamente amplo, absorvendo até mesmo crimes de reduzida gravidade; e (iv) que o prazo de duração dessa medida é indevido por ser igual ao aplicável às escutas telefônicas, técnica que é menos gravosa. RAMALHO, Silva David. Métodos Ocultos de Investigação Criminal em Ambiente Digital, Lisboa: Almedina, 2017, p. 351-355. Paulo Pinto de Albuquerque, por sua vez, embora sustente a previsão do malware por dispositivo legal diverso, igualmente conclui pela inconstitucionalidade deste meio de obtenção de prova na Lei do Cibercrime em razão de a norma implicar uma intrusão na privacidade da pessoa visada desproporcional e que é feita sem um controle prévio ou posterior da "pesquisa" por um juiz. ALBUQUERQUE, Paulo Pinto. *Comentários do Código de Processo Penal*... Op. cit., p. 502.

constitucional como infraconstitucional, a bem de haver um adequado equilíbrio entre eficiência e garantismo na esfera processual.

Dadas as particularidades do *malware*, é de se questionar, em um primeiro momento, se a própria ordem constitucional vigente no Brasil oferece uma esfera de proteção adequada aos efeitos dele decorrentes, para o que é interessante observar a experiência alemã.

Segundo o Tribunal Constitucional Federal alemão, os direitos fundamentais então existentes não eram capazes de abarcar toda a esfera de afetação do *malware*, razão pela qual havia uma lacuna geral de proteção aos indivíduos. A insuficiência do direito à inviolabilidade do domicílio, por exemplo, deve-se ao fato de que ele não encontraria respaldo caso o sistema informático se encontrasse fora do espaço privado: se o sujeito começasse a escrever um e-mail no seu domicílio, editasse-o em um local público e o enviasse quando retornasse novamente à sua residência, na mesma atividade ele estaria protegido e desprotegido pelo direito. Por outro lado, o direito à autodeterminação informacional, que também é uma criação jurisprudencial germânica, relaciona-se a uma escolha do indivíduo em armazenar ou não informações nos sistemas informáticos (fotografias, vídeos, dados bancários, correspondência etc.). A sua insuficiência, quando da intervenção por um *software* malicioso, decorre do fato de que o cidadão não tem um poder de disposição sobre diversos dados que são criados automaticamente pelos sistemas informáticos e que são altamente sensíveis, os quais poderão ser acessados por meio do dispositivo espião[55]. Por essa razão, houve o reconhecimento de um novo direito fundamental, que foi denominado de direito à integridade e confidencialidade dos sistemas informáticos.

Esse novo direito constitui uma dimensão do direito geral à personalidade, trazendo como objeto da proteção o próprio sistema informático pessoal e, por consequência, o indivíduo que o utiliza. Em um contexto de dependência das pessoas em relação a sistemas dessa natureza, faz-se necessário assegurar a confiança dos indivíduos neles, de modo a garantir uma proteção sobre a sua confidencialidade e integridade. Enquanto a confidencialidade diz respeito à limitação do acesso

[55] BATISTA, Lydie Jorge. *O malware como meio de obtenção de prova*... Op. cit., p. 116-117.

da informação apenas às pessoas autorizadas, a integridade refere-se à proteção do sistema contra manipulações[56].

No Brasil, vem-se entendendo pela necessidade de uma readequação da teoria do direito para enfrentar os desafios impostos por técnicas investigativas como o *malware*. Nesse sentido, Aury Lopes Jr. e Carlos Hélder Carvalho sustentam que o direito à integridade e confidencialidade dos sistemas informáticos pode ser incorporado à Constituição de 1988 por força da cláusula de abertura prevista em seu art. 5º, § 2º, que dispõe que "os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte"[57]. Laura Schertel Mendes, por sua vez, sustenta que uma compreensão dinâmica do texto constitucional, a partir da qual se faz uma tutela ampla do direito à personalidade e da vida privada do cidadão, autoriza a integração desse novo direito fundamental à esfera nacional[58].

Uma incorporação adequada do *malware* ao ordenamento jurídico brasileiro demanda, portanto, a previsão de um direito fundamental que efetivamente abranja os demais efeitos desse novo meio de obtenção de prova. Somente assim para que se tenha um regime jurídico adequado às inovações da modernidade, capaz de equilibrar uma ampla proteção da intimidade/imagem/livre comunicação/dados dos indivíduos, com as inovações que são necessárias para melhor combater as formas de criminalidade mais complexas. No plano infraconstitucional, por sua vez, como se verá, diversos aspectos também precisam ser observados para uma devida absorção desta técnica ao Brasil[59].

---

[56] MENDES, Laura Schertel. Uso de softwares espiões pela polícia: prática legal?... Op. cit.

[57] LOPES JR, Aury; MENDES, Carlos Hélder Carvalho Furtado. "Vírus espião" como meio... Op. cit.

[58] MENDES, Laura Schertel. Uso de softwares espiões pela polícia: prática legal?... Op. cit.

[59] Na mesma linha do aqui propugnado, é a posição de Alves em relação ao ordenamento português, segundo o qual, "para além de ser expressa, a consagração legal de um método oculto de investigação criminal - dado o potencial de agressividade relativamente a direitos fundamentais - tem também, nas palavras de Costa Andrade, "de prever expressa e explicitamente a medida de compressão de direitos fundamentais, fixar a sua compreensão,

5.1. Referências para a determinação de um regime processual para o *malware*.

O fato de a utilização do *malware* em uma investigação implicar uma afetação a diversos direitos fundamentais demanda que a sua regulamentação seja feita de forma bastante restrita e cautelosa. Da mesma forma que haverá problemas quando da adaptação de uma norma já existente, que foi pensada para outros fins, para autorizar essa medida, problemas também surgirão com a previsão dessa técnica em uma norma específica, só que de forma pouco qualificada. Em face disso, e adotando como referencial a experiência comparada, alguns elementos podem ser mencionados como necessários a uma norma processual que vise regular a utilização de um dispositivo malicioso.

Uma *primeira questão* diz respeito à necessidade de haver uma previsão expressa em lei no sentido de que o *malware* constitui o último recurso possível de ser acionado pelas autoridades em uma atividade investigativa. Não basta, portanto, que sem essa técnica as apurações se tornem mais difíceis; é necessário que sem ela as apurações sejam praticamente impossíveis.

Uma *segunda questão* é a necessidade de que o uso do *malware* somente seja autorizado judicialmente e mediante uma decisão amplamente fundamentada. Para tanto, deve-se exigir a verificação da proporcionalidade da medida ao caso concreto, através de uma análise da sua adequação, necessidade e proporcionalidade em sentido estrito, prevendo-se em lei que a não identificação desses pressupostos, bem como a sua realização de forma inadequada ou insuficiente, ensejará a nulidade da intervenção.

Uma *terceira questão* está relacionada à previsão de um catálogo taxativo e restrito dos delitos que poderão autorizar o uso do *malware*, os quais não apenas devem dispor de elevadas penas, como guardar pertinência com o uso de um agente malicioso.

---

extensão e vinculação finalístico--teleológica bem como definir os seus limites". ALVES, Daniel Bento. Uso de *malware* em investigação criminal... Op. cit., p. 28-29.

Uma *quarta questão* é a necessidade de haver uma descrição da forma como será feito o uso do *malware*, indicando-se o procedimento para a sua instalação (físico ou remotamente); o tipo de dispositivo malicioso que será utilizado, bem como o uso que será conferido a ele no dispositivo eletrônico (obtenção de dados armazenados, acesso à câmera, registro das palavras que estão sendo digitadas etc.). Paralelamente, a norma reguladora deve prever a utilização de técnicas que realizem o mínimo de alterações no sistema informático e que permitam a sua reversão ao final, além do que elas devem proteger o sistema acessado de intervenções não autorizadas de terceiros.

Uma *quinta questão* trata da limitação do rol de sujeitos possíveis de serem alcançados pela medida, a fim de obstar que ele alcance qualquer pessoa. Uma proposta nesse sentido é a de que o *malware* alcance apenas o suspeito e o intermediário[60].

Uma *sexta questão* atine à determinação do período que o *malware* poderá ser utilizado e da quantidade de vezes que o seu uso poderá ser renovado, que devem ser pequenos e limitados, exigindo-se, ainda, que em todas as renovações seja novamente verificado os requisitos para a sua admissibilidade[61].

Uma *sétima questão* diz respeito à previsão de um procedimento rígido e detalhado para a operacionalização do *malware*, dentre o que pode ser mencionado (i) a identificação de todas as pessoas que tomarem contato com a execução do *malware* no dispositivo infectado; (ii) a identificação das operações efetuadas para instalar o *malware*, para capturar

---

[60] Suspeito seria aquela pessoa em relação à qual exista um indício de que cometeu ou se prepara para cometer um crime ou, em alternativa, nele participou ou se prepara para participar, enquanto intermediário é aquele indivíduo que, pela proximidade com o suspeito ou o arguido, afigure como potencial interlocutor. BATISTA, Lydie Jorge. *O malware como meio de obtenção de prova*... Op. cit., p. 136.

[61] Na Alemanha, esse prazo poderá ter uma duração máxima de três meses, renovável por igual período; na Espanha, o período da intervenção não poderá exceder os três meses; e na França o intervalo poderá ser de um mês, renovável por igual período, quando feito a requerimento do Procurador da República, e de quatro meses, também renovável por um mesmo período, quando feito por iniciativa do juiz de instrução. BATISTA, Lydie Jorge. *O malware como meio de obtenção de prova*... Op. cit., p. 53-60.

os dados informáticos e, ao final, remover o dispositivo malicioso; (iii) a identificação da data e horário de início e fim das atividades; (iv) a elaboração de relatórios intercalares sobre os resultados da operação, os quais deverão ser apresentados ao juiz para fins de acompanhamento da necessidade de permanência da medida; (v) a elaboração de relatório final minucioso, no qual deve conter informações como o estado em que se encontrava o sistema informático acessado e as alterações sofridas após o acesso, os dados recolhidos e os essenciais para a descoberta dos fatos apurados, o modo de garantia da cadeia da custódia etc.; (vi) a eliminação do *malware* ao final da operação; (vii) o envio dos dados recolhidos tanto ao juiz que autorizou a medida como a uma autoridade de proteção de dados específica[62], que devem fazer a sua verificação e controle, especialmente a fim de verificar a pertinência com o delito investigado; (viii) a eliminação dos dados que não se relacionarem diretamente à investigação, assim como a elaboração de um relatório sobre esse material que descreva o seu deslinde.

Uma *oitava questão* é a necessidade de ser assegurado o acesso dos relatórios elaborados pelo acusado, a fim de que ele possa fazer o controle da legalidade desse meio de obtenção de prova, exercer o seu direito de defesa e até mesmo impedir a utilização de informações íntimas ou pessoas que não guardem relação com a investigação.

Uma *nona questão* é a necessidade de que seja estabelecido um meio de supervisão da autoridade encarregada da proteção de dados pessoais, tal como firmado pela norma alemã. Somente ela terá os caracteres necessários para zelar pelo direito à autodeterminação informativa, tanto de investigados como daqueles que possam ter sido colateralmente atingidos, cabendo-lhe conhecer as funcionalidades das ferramentas e lançar mão de recomendações e medidas protetivas para coibir vazamentos de dados e outras violações aos direitos previstos na Lei Geral de Proteção de Dados (LGPD)[63].

---

[62] Na Alemanha, por exemplo, os dados recolhidos são encaminhados automaticamente para análise da Comissão de Proteção de Dados e de dois funcionários federais, podendo um deles ser o juiz. BATISTA, Lydie Jorge. *O malware como meio de obtenção de prova*... Op. cit., p. 53.

[63] Tal autoridade não deve ser aquela mesma criada pela LGPD, tendo em vista que essa norma expressamente exclui do seu campo de aplicação as

6. Conclusão

A utilização de *malwares* como meio oculto de obtenção de prova tem o potencial de trazer eficiência às investigações de natureza processual penal. Todavia, o fato de esses *softwares* serem inseridos e operarem de forma secreta no sistema informático alvo, assim como alcançarem diversos níveis das informações e dados pessoais dos indivíduos, levanta questionamentos quanto à sua compatibilidade com os direitos fundamentais e garantias processuais dos investigados.

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. A sua positivação, ademais, deve levar em conta a excepcionalidade que deve revestir o seu emprego, bem como a necessidade de haver formas rígidas de controle da sua operacionalização.

Referências bibliográficas

ALAMILLO, Javier Rubio. La informática en la reforma de la Ley de Enjuiciamiento Criminal. *Diario La Ley*, n. 8662, 2015.

ALBUQUERQUE, Paulo Pinto. *Comentários do Código de Processo Penal*. Lisboa: Universidade Católica Editora, 2011.

ALVES, Daniel Bento. Uso de *malware* em investigação criminal. *Actualidad Jurídica Uría Menéndez*, v. 16, n. 47, p. 19-30, out./dez. 2017.

ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. E quando o policial vira hacker? As principais justificativas, técnicas e discussões jurídicas sobre hacking estatal. Disponível em: <https://www.internetlab.org.br/pt/privacidade-e-vigilancia/e-quando-o-policial-vira-hacker/>. Acesso em: 22 mai. 2022.

investigações, mas aquela encarregada da proteção de dados no âmbito de investigações e segurança pública em norma ainda não editada, mas cujo projeto tem sido chamada de LGPD Penal.

ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. Vigilância das comunicações pelo Estado brasileiro. Disponível em: <https://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf>. Acesso em: 22 mai. 2022.

ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. *Revista de Investigações Constitucionais*, Curitiba, v. 4, n. 3, p. 167-200, set./dez. 2017. https://doi.org/10.5380/rinc.v4i3.51295

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

BARBIERO, Diego Roberto. Implantação de Malwares em Investigações Complexas. Curitiba: Juruá, 2021.

BATISTA, Lydie Jorge Batista. *O malware como meio de obtenção de prova em processo penal*. 2018. Dissertação (Mestrado em Direito) Faculdade de Direito da Universidade de Lisboa, Lisboa, 2018.

BUJOSA VADELL, Lorenzo Mateo; BUSTAMANTE RÚA, Mónica María; TORO GARZÓN, Luis Orlando. La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. Revista Brasileira de Direito Processual Penal,v. 7, n. 2, p. 1347, 2021. https://doi.org/10.22197/rbdpp.v7i2.482

CAPPARELLI, Bruna. Técnicas investigativas italianas articuladas com a utilização dos denominados captadores informáticos: qui custodiet custodes?. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 137, p. 253-286, nov. 2017.

CAPRIOLI, Francesco. O "captador informático" como instrumento de busca da prova na Itália. *Revista Brasileira De Direito Processual Penal*, Porto Alegre, v. 3, n. 2, p. 483-510, mai./ago. 2017.

CASTRO, Henrique Hoffmann Monteiro de. Lei 13.441/17 instituiu a infiltração policial virtual. Disponível em: <https://www.conjur.com.br/2017-mai-16/academia-policia-lei-1344117-instituiu-infiltracao-policial-virtual>. Acesso em: 22 mai. 2022.

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.

DEZEM, Guilherme Madeira. *Curso de Processo Penal*. São Paulo: Revista dos Tribunais, 2015.

GOMES FILHO, Antônio Magalhães. Notas sobre a terminologia da prova (reflexos sobre o processo penal brasileiro). In: YARSHELL, Flávio Luiz; MORAES,

Maurício Zanoide de (Orgs.). *Estudos em homenagem à professora Ada Pellegrini Grinover*. São Paulo: DPJ Editora, 2005.

GONÇALVES, Vinícius Abdala. *O agente infiltrado frente ao processo penal constitucional*. Belo Horizonte: Arraes, 2014.

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.

GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set./dez. 2019.

LOPES JR, Aury; MENDES, Carlos Hélder Carvalho Furtado. "Vírus espião" como meio de investigação: a infiltração por *softwares*. Disponível em: <https://www.conjur.com.br/2019-jun-07/limite-penal-virus-espiao-meio-investigacao-infiltracao-softwares>. Acesso em: 22 mai. 2022.

MENDES, Carlos Hélder C. Furtado. *Tecnoinvestigação criminal*: entre a proteção de dados e a infiltração por *software*. Salvador: Juspodivm, 2019.

MENDES, Laura Schertel. Uso de softwares espiões pela polícia: prática legal? Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015>. Acesso em: 22 mai. 2022.

MORAES, Maurício Zanoide de. *Presunção de inocência no processo penal brasileiro*: análise de sua estrutura normativa para a elaboração legislativa e para a decisão judicial. Rio de Janeiro: Lumen Juris, 2012.

PÉREZ ESTRADA, Miren Josune. La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información. *Revista Brasileira De Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1297-1330, set./dez. 2019.

RAMALHO, Silva David. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Lisboa: Almedina, 2017.

RIBOLI, Eduardo Bolsoni. "Eu sei o que vocês fizeram no verão passado": o uso de software de espionagem como meio de obtenção de prova penal. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 27, n. 156, p. 91-139, jun. 2019.

ROMÃO, Luis Fernando de França. Agente infiltrado e agente de inteligência: distinções a partir de estudo de caso julgado pelo Supremo Tribunal Federal. *Revista Brasileira de Inteligência*, Brasília, v.16, n. 14, p. 85-99, 2019.

SILVA, Virgílio Afonso da. O proporcional e o razoável. *Revista dos Tribunais*, São Paulo, v. 91, n. 798, p. 23-50, 2002.

SOARES, Gustavo Torres. Investigação criminal e inovações técnicas e tecnológicas. Belo Horizone: D' Plácido, 2020.

SMANIO, Gianluca Martins. *A vigilância policial em meio digital*: entre o garantismo e a eficiência. 2021. Dissertação (Mestrado em Direito). Faculdade de Direito da Universidade de São Paulo, São Paulo, 2021.

TONINI, Paolo. *A prova no processo penal italiano*. São Paulo: Revista dos Tribunais, 2002.

VACIAGO, Giuseppe; RAMALHO, David Silva. Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings. *Digital Evidence and Eletronic Signature Law Review*, v. 13, 2016.

VALENTE, Manuel M. G. Editorial dossiê "Investigação preliminar, meios ocultos e novas tecnologias". Revista Brasileira de Direito Processual Penal, Porto alegre, v. 3, n. 2, p. 473-482, mai./ago. 2017.

VILARES, Fernanda Regina. *Ação controlada*: limites para as operações policiais. Belo Horizonte: D'Plácido, 2017.

Authorship information

Gustavo Alves Magalhães Ribeiro. Mestrando em Direito Penal pela Faculdade de Direito da USP. Bacharel em Direito pela Faculdade de Direito da USP. Advogado. gustavo_alvesribeiro@hotmail.com

Pedro Ivo Rodrigues Velloso Cordeiro. Doutorando em Direito Processual Penal pela Faculdade de Direito da USP. Mestre em Direito e Estado pela Faculdade de Direito da Universidade de Brasília. Advogado, pedroivo.cordeiro@gmail.com

Débora Moretti Fumach. Doutoranda em Direito Processual Civil pela Faculdade de Direito da USP. Mestre em Direito Público - Administration et Politiques Publiques pela Université Paris 2 Panthéon-Assas (Título revalidado pela UNB). Promotora de Justiça. debmoretti@hotmail.com

Additional information and author's declarations
(scientific integrity)

Conflict of interest declaration: the authors confirm that there are no conflicts of interest in conducting this research and writing this article.

Declaration of authorship: all and only researchers who comply with the authorship requirements of this article are listed as authors; all coauthors are fully responsible for this work in its entirety.

- *Gustavo Alves Magalhães Ribeiro*: conceptualization, methodology, data curation, investigation, writing – original draft, validation, writing – review and editing, final version approval.
- *Pedro Ivo Rodrigues Velloso Cordeiro*: conceptualization, methodology, data curation, investigation, writing – original draft, validation, writing – review and editing, final version approval.
- *Débora Moretti Fumach*: conceptualization, methodology, data curation, investigation, writing – original draft, validation, writing – review and editing, final version approval.

Declaration of originality: the authors assure that the text here published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; they also attest that there is no third party plagiarism or self-plagiarism.

Editorial process dates
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Submission: 23/05/2022
- Desk review and plagiarism check: 30/05/2022
- Review 1: 17/06/2022
- Review 2: 23/06/2022
- Review 3: 27/06/2022
- Review 4: 01/07/2022
- Preliminary editorial decision: 04/09/2022
- Correction round return: 04/10/2022
- Final editorial decision: 12/10/2022

Editorial team

- Editor-in-chief: 1 (VGV)
- Reviewers: 4

How to cite (ABNT brazil):

RIBEIRO, Gustavo A. M.; CORDEIRO, Pedro Ivo R. V.; FUMACH, Débora M. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. *Revista Brasileira de Direito Processual Penal*, vol. 8, n. 3, p. 1463-1500, set./dez. 2022. https://doi.org/10.22197/rbdpp.v8i3.723