O USO DO *MALWARE* NA INVESTIGAÇÃO CRIMINAL: PONTOS DE TENSÃO E LIMITES

MALWARE IN CRIMINAL INVESTIGATIONS: TENSIONS POINTS AND LIMITS

Helena Costa Rossi
Mestranda em Direito Processual Penal na Faculdade de Direito da USP.
Associada ao IBCCRIM. Advogada.
Link Lattes: https://lattes.cnpq.br/6022530640899053
ORCID: https://orcid.org/0009-0004-3436-9807
helena.costa.rossi@gmail.com

Leandro Musa de Almeida
Mestrando em Direito Processual Penal na Faculdade de Direito da USP.
Procurador da República.
Link Lattes: https://lattes.cnpq.br/9427288378613350
ORCID: https://orcid.org/0009-0007-0798-9121
leandromusa@outlook.com

DOI: https://doi.org/10.5281/zenodo.10188525

Resumo: O avanço das técnicas de investigação de provas digitais tensiona o sistema de garantias dos direitos fundamentais. Em atenção a essa questão, o presente artigo busca analisar aspectos sensíveis sobre a técnica de investigação de provas digitais conhecida como *malware.* Com base em estudo doutrinário, amparado pelo exame da legislação espanhola e das disposições contidas no projeto de novo Código de Processo Penal (CPP), o presente trabalho busca averiguar se o emprego desse novo meio de obtenção de prova seria possível no Brasil e identificar parâmetros a serem observados pelo legislador brasileiro a fim de compatibilizar o uso da medida com os direitos fundamentais.

Palavras-chave: Técnicas de investigação; Provas digitais; Direitos fundamentais; Parâmetros legais; Métodos Ocultos.

Abstract: The development of special investigation techniques aiming to obtain digital evidence impacts fundamental rights. In attention to this issue, this article seeks to analyze sensitive aspects of the technique known as malware. Based on a doctrinal study, supported by the examination of the Spanish legislation and the provisions of the project for the new Brazilian Penal Procedure Code, this work seeks to ascertain whether the use of this new means of obtaining evidence would be possible in Brazil and to identify parameters to be observed by the Brazilian legislator to make the measure compatible with fundamental rights.

Keywords: Special investigation techniques; Digital evidence; Fundamental rights; Legal parameters; Hidden method.

1. Introdução

As possibilidades de sistematização de toda espécie de informações em formato digital vêm modificando os métodos de investigação e a busca de provas no processo penal. Diante da grande capacidade de armazenamento de dados digitais em servidores globais, importa discutir pontos de tensão com os direitos fundamentais, bem como os limites que devem ser impostos às medidas de obtenção de provas digitais, com vistas a garantir efetividade no combate às modernas formas de criminalidade com uma adequada tutela da privacidade.

O presente artigo trabalha com a hipótese de que as técnicas investigativas de obtenção de provas digitais avançam em velocidade superior à atualização legislativa, de modo que a ausência de parâmetros legais claros para essas medidas abre espaço para um cenário de insegurança jurídica e falta de garantias.

Nesse aspecto, volta-se o foco da análise à utilização de uma técnica específica de aquisição das provas digitais, o *malware*, para então buscar compreender as tensões e os limites do uso dessa técnica investigativa, ainda não prevista em lei no Brasil.

Como meio de obtenção de prova que é, o *malware* implica na restrição a direitos fundamentais. Além de permitir a obtenção de dados estáticos ou em fluxo, o *malware* possibilita a ativação de funcionalidades, como GPS, câmera e microfone, viabilizando o monitoramento de atividades em tempo real. Assim, o uso dessa técnica atinge informações que integram o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual, da privacidade e do livre desenvolvimento da personalidade.

Em vista da capacidade de restrição a direitos fundamentais, o presente artigo busca discutir os limites que devem ser impostos à utilização do *malware*, com vistas a garantir efetividade no combate às modernas formas de criminalidade, sem violação ou supressão de direitos.

A fim de alcançar o objetivo analítico do presente trabalho, adotou-se como metodologia o estudo crítico da doutrina especializada e das leis sobre a matéria. Especificamente, realizou-se uma análise mais detida da legislação espanhola e das disposições contidas no projeto de novo Código de Processo Penal (CPP).

2. O uso do *malware* na investigação criminal

O termo *malware* advém da conjunção das palavras em língua inglesa *malicious* e *software* e consiste em técnicas de invasão a dispositivos informáticos por meio da instalação de *software* oculto (Ramalho, 2019, p. 318-319).

A utilização de *malware* como meio de obtenção de prova está compreendida no que se denomina de *hacking* governamental (*government/lawful hacking*), que consiste na exploração de vulnerabilidades preexistentes nos sistemas (*backdoors*), além da utilização de outros programas maliciosos, pelas autoridades, para acessar determinadas informações contidas em dispositivos eletrônicos no contexto de investigações criminais.[1]

O *malware* permite recolher dados armazenados e monitorar a atividade do usuário em ambiente digital, inclusive com a ativação de funcionalidades de *hardware* como GPS, câmera e microfone, incluindo, ainda, todo o tipo de programas instalados de forma sub-

reptícia que podem comprometer as funções de um dispositivo informático, corromper ou alterar dados (Ramalho, 2019, p. 313-314).

Assim, é certo que o uso dessa técnica atinge informações que integram o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual, da privacidade e do livre desenvolvimento da personalidade, constituindo informações protegidas pelo sigilo constitucional (Silva, 1996, p. 202).

Apesar da severa afetação a direitos fundamentais, o elevado potencial de recolher elementos de provas digitais faz com que alguns ordenamentos jurídicos consagrem o uso do *malware*, seja de forma legal ou jurisprudencial. A fim de ilustrar esse uso na prática das investigações criminais, identificando possíveis pontos de tensão, o presente artigo se baseia na experiência espanhola.

Em 2015, a Espanha promulgou a *Ley Orgánica 13/2015*, que passou a autorizar expressamente a utilização de *malware* para fins investigativos. Até a mencionada norma, o cenário espanhol era muito semelhante ao nosso, já que não existia naquele ordenamento jurídico a previsão da utilização dessa técnica para recolha de provas no âmbito digital (Espanha, 2015). Mesmo sem autorização legal expressa, os tribunais espanhóis começaram a autorizar o uso de técnicas avançadas de investigação criminal, interpretando extensivamente a legislação até então existente e a própria Constituição.[2]

Especificamente quanto ao uso de programas-espiões, o art. 588 *septies* (a) (1) da *Ley de Enjuiciamiento Criminal* (LECRIM), introduzido pela reforma de 2015, estabelece que o juiz competente poderá autorizar a instalação de *softwares*, que permitam, de forma remota e telemática, o exame à distância do conteúdo de um computador, aparelho eletrônico, sistema de computador, dispositivo de armazenamento de dados de computador em massa ou banco de dados, sem que o proprietário ou usuário tenha conhecimento.

O mencionado dispositivo legal traz um rol de crimes que autorizam a técnica,[3] o qual não está isento de críticas. Uma parcela da doutrina considera a hipótese prevista na alínea *e* demasiadamente aberta, o que daria margem à utilização de analogia para permitir a utilização de programas-espiões em um número ilimitado de crimes, conforme a discricionariedade e a criatividade do magistrado espanhol.

Ainda para essa corrente, em razão do alto grau de invasividade, a medida deveria ser reservada apenas para os crimes mais graves e não para todos aqueles cometidos por meio de ferramentas informáticas (Blanco, 2021, p. 450). Há autores, como Winter (2017, p. 23-24), por outro lado, que entendem que o legislador trouxe essa hipótese em razão da peculiaridade dos crimes informáticos, que, em geral, não podem ser descobertos sem a utilização da tecnologia. Isso não significa, contudo, que qualquer delito cometido por meio de sistemas informáticos admite o uso de *malware*, uma vez que a medida sempre demanda a avaliação da proporcionalidade por parte do juiz.

Por sua vez, o art. 588 *septies* (a)(2) da LECRIM estabelece os elementos que a decisão judicial deverá conter, especificamente: (a) a indicação dos computadores, dispositivos eletrônicos, sistemas informáticos sujeitos à medida;[4] (b) o alcance da medida; (c) a forma como os dados ou arquivos informáticos pertinentes ao caso serão acessados e apreendidos; e (d) a indicação do *software* por meio do qual será executado o controle das informações.

A descrição na decisão judicial da forma como funciona o *software* empregado é de extrema importância porque permite uma análise posterior sobre a proporcionalidade da medida e da legitimidade na ingerência nos direitos fundamentais do sujeito afetado (Blanco, 2021, p. 454).

A decisão também deverá especificar os agentes que estarão autorizados a executar o procedimento, a eventual autorização para fazer e manter cópias de dados informáticos, bem como as medidas para a preservação da integridade, inacessibilidade e eliminação dos dados armazenados. Por fim, o art. 588 *septies* (c) estabelece que a medida terá a duração máxima de um mês, prorrogável por iguais períodos até um máximo de três meses.[5]

A Espanha, portanto, a partir de 2015, regulamentou de forma expressa e detalhada a possibilidade da utilização de *softwares*-espiões para fins de investigação penal. Evidentemente que a legislação não é imune a críticas, mas representa uma evolução no tratamento da matéria, servindo de orientação para o legislador nacional.

3. Previsões legislativas no novo CPP

No atual processo penal brasileiro, inexiste autorização legal para o uso do *malware*. A medida é tanto incompatível com a busca e a apreensão de objetos físicos quanto com a interceptação telemática, uma vez que possibilita a coleta da integralidade das informações armazenadas nos dispositivos acessados, bem como o monitoramento em tempo real de dados que não necessariamente derivam das telecomunicações, possibilitando ainda a própria manipulação dos dados (Grego; Gleizer, 2019, p. 1483-1518). Tampouco é possível fundamentar a medida combinando os elementos de normas procedimentais próximas, diante da natureza de invasividade e da especificidade da medida.

Em 2009, teve início no Senado Federal o Projeto de Lei 156, com o objetivo de elaborar um novo CPP brasileiro. O projeto foi aprovado pelo plenário daquela casa legislativa e, em 2010, foi remetido à Câmara dos Deputados, onde tramita até os dias atuais sob o número 8.045/10.

No dia 13 de abril de 2021, o então relator-geral da Comissão da Câmara dos Deputados que analisava as mudanças no CPP apresentou novo parecer (Brasil, 2010), substituindo o apresentado por ele em 2018, incorporando cerca de 30 novas propostas apensadas ao projeto de lei original (PL 8.045/10) que foi enviado pelo Senado. Nesse novo parecer, o relator-geral sugeriu, dentre outras coisas, a regulamentação da utilização de provas digitais.

O relatório sugere a inclusão no CPP de um capítulo integralmente dedicado às provas digitais. Dentre os dispositivos que consideramos relevantes para o objeto deste trabalho está o art. 304, que estabelece o rol dos meios de obtenção de prova digital. Conforme o texto da referida norma, constituem meio de obtenção de prova:

> I - a busca e apreensão de dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica, e o tratamento de seu conteúdo;
>
> II - a coleta remota, oculta ou não, de dados em repouso acessados à distância;
>
> III - a interceptação telemática de dados em transmissão; IV - a coleta por acesso forçado de sistema informático ou de redes de dados;
>
> V - o tratamento de dados disponibilizados em fontes abertas, independentemente de autorização judicial.

Cumpre destacar que em nenhum momento o novo capítulo sobre provas digitais prevê expressamente a utilização de *softwares* para obtenção de provas. O art. 304, II, do projeto de novo CPP apenas prevê como meio de obtenção de prova a coleta remota, oculta ou não de dados estáticos. Isso, contudo, não gera a conclusão de que essa coleta pode se dar por meio de *malware*, uma vez que a coleta também é viável sem a utilização de programas-espiões. Basta

imaginar a situação da autoridade que, por algum motivo, possui a senha de acesso a um dispositivo informático e nele ingresse remotamente, tal como ocorre em manutenções remotas feitas em computadores.

O mencionado dispositivo também não deixa claro se é possível pelas autoridades a ativação de funcionalidades de *hardware* como GPS, câmera e microfone. Com efeito, a utilização de programas maliciosos vai muito além da mera coleta de dados do dispositivo-alvo, podendo chegar ao ponto de tomar o controle total do equipamento sem que o utilizador note.

O inc. IV do art. 304, que trata do acesso forçado, também não é claro quanto a possibilidade da utilização de *malware*. Conforme art. 307 do projeto, a coleta por acesso forçado a dispositivo eletrônico, sistema informático ou redes de dados, ocorrerá somente após prévia desobediência de ordem judicial determinando a entrega da prova pretendida ou quando impossível identificar o controlador ou provedor em território nacional, e compreenderá os métodos de segurança ofensiva ou qualquer outra forma que possibilite a exploração, isolamento e tomada de controle. O dispositivo, além de não tratar expressamente de programas-espiões, não esclarece se o acesso forçado pode ser remoto e se também abrange dados dinâmicos.[6]

Importante notar que, embora a utilização de *malware* pareça viável com fundamento nos dispositivos acima mencionados, seria melhor que o legislador tomasse uma posição mais clara a respeito da medida e previsse expressamente a possibilidade da utilização de *softwares*-espiões, como fez o legislador espanhol.

O relatório também não traz um rol de crimes em que o método pode ser utilizado. Conforme já exposto acima, devido ao grau de intrusão que a medida implica na esfera de privacidade das pessoas, a utilização de *malware* só deve ser recomendada para crimes graves devidamente especificados pelo legislador.

Quanto à abrangência da medida, o projeto prevê expressamente no art. 308, § 2º, que a obtenção da prova digital pode se dirigir a uma terceira pessoa, desde que haja indícios de que o investigado utilize o dispositivo eletrônico, ou quaisquer outros meios de armazenamento de informação eletrônica, com ou sem o conhecimento do proprietário.[7]

Embora já seja um avanço, entendemos que o legislador brasileiro deve tomar uma posição clara no novo CPP quanto à possibilidade da utilização de *malware*. Em sendo aceita, deveria seguir a linha das legislações que já adotam a medida, tais como a Alemanha,[8] a Itália[9] e a Espanha, estabelecendo um rol específico de crimes que autorizam o acesso remoto por programa-espião. O legislador brasileiro também deveria tomar como parâmetro o projeto *Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean*, lançado pela Comissão Europeia e a *International Telecommunication Union* com o propósito de fomentar a uniformização da legislação nos países do Caribe em nove áreas relacionadas com tecnologias de informação (Ramalho, 2019, p. 336-337). O art. 27 do projeto, por exemplo, trata especificamente do uso de *malware* para fins de investigação criminal, impondo diversas restrições para a sua utilização, como uma forma de compatibilizar direitos fundamentais dos investigados com eficiência da persecução penal.

4. Pontos de tensão

Caso o texto do novo CPP seja aprovado de acordo com a redação atual, será imperativo que se observem limites mínimos para a sua utilização. A observância desses requisitos possui dupla finalidade: por um lado, proteger os direitos do imputado, e por outro, evitar que elementos de prova essenciais se tornem ineficazes por terem sido obtidos de modo irregular (Winter, 2017, p. 84).

A propósito da obtenção dos dados digitais, cumpre destacar que esses dados são caracterizados pela sua imaterialidade, uma vez que não são constituídos em linguagem natural, mas em sinais binários.[10] Por não possuírem uma materialidade imediatamente constatável, é imprescindível que o método empregado para coleta da prova garanta a integridade do dado digital, sem o qual não terá qualquer valor epistêmico. Como visto, uma vez instalado, o *malware* permite monitorar toda atividade ocorrida no sistema informático em tempo real. Ainda, permite acessar indistintamente todos os dados armazenados, além de afetar a própria integridade e confidencialidade do sistema (Ramalho, 2019, p. 350). Assim, o *malware* possui grau de invasividade ainda maior do que outras medidas já positivadas no ordenamento jurídico brasileiro, tais como a busca e a apreensão e as interceptações telefônicas e telemáticas, de sorte que as previsões procedimentais contidas nos dispositivos que regem essa medida não serão suficientes para autorizar uma aplicação analógica dessas regras (Winter, 2017, p. 6-7).

O seu maior grau de invasividade demanda, pois, um controle mais rígido desse meio de obtenção de prova e gera, naturalmente, a necessidade de limitar o seu escopo de aplicação e estabelecer condições para que seja utilizada de forma excepcional (*ultima ratio*) (Liguori, 2021, p. 259), de acordo com um procedimento claro que garanta a devida documentação da cadeia de custódia da prova.[11] Ainda considerando a gravidade da medida, entende-se que a lei deveria prever um rol taxativo de tipos penais (baseados em sua gravidade) que autorizem o uso da técnica.

Uma vez que certas ferramentas podem garantir ao invasor privilégios administrativos do sistema, com a possibilidade de alterações das informações ali contidas, é necessário garantir que os meios de prova colhidos não tenham sido alterados. Nesse sentido, propõe-se que seja realizado um relatório técnico da utilização desse meio de obtenção de prova, a fim de que se verifique se não se está diante de prova contaminada ou com deficiências técnicas (Ramalho, 2019, p. 352).

Por fim, a invasão não deve colocar em risco o funcionamento do sistema invadido, nem implicar em eventuais riscos para terceiros, considerando que o uso do *malware* pode contaminar dispositivos informáticos de pessoas inocentes. Assim, deve-se garantir que o programa invasor não produza danos colaterais desnecessários.

5. Conclusão

O avanço das técnicas de investigação, com especial atenção ao uso do *malware,* tensiona o sistema de garantias dos direitos fundamentais, no limiar entre a eficiência e o garantismo (Fernandes, 2008, p. 26).

Como se sabe, o procedimento probatório previsto na legislação representa uma garantia ao indivíduo, assegurando, ainda, a capacidade epistêmica da prova e seu caráter racional.

Com vistas a conferir segurança e objetividade aos meios de obtenção de provas digitais, com especial atenção ao uso do *malware*, pondera-se que a legislação deve avançar na positivação dos meios de pesquisa de prova já conhecidos na prática das investigações, prevendo-se também um procedimento próprio a ser adotado para a execução dessa medida (não bastando que seja apenas nomeada na legislação).

Nesse aspecto, o princípio da proporcionalidade deve ser observado rigorosamente, sendo ainda preciso insistir no caráter excepcional da medida, que somente será legítima depois de ser claramente positivada no ordenamento jurídico brasileiro, limitada a situações de violações graves a bens juridicamente tutelados.

Notas

[1] O *hacking* governamental pode ser utilizado como alternativa à criptografia. Trata-se de modalidade de investigação extremamente invasiva, tanto da perspectiva das informações acessíveis quanto da segurança dos dispositivos explorados. Segundo Carlos Liguori (2022, p. 258), a ausência de um arcabouço jurídico que o operacionalize em conformidade aos direitos fundamentais e ao devido processo legal impõe desafios ao seu uso e suas características particulares requerem o desenvolvimento de regulação jurídica específica para sua utilização.

[2] Exemplificativamente, o Supremo Tribunal Espanhol permitiu a utilização de dispositivos eletrônicos denominados IMSI *Catchers* ou *Cell Site Simulators* para obter, a partir da localização física de determinados celulares e da sua proximidade das antenas que lhes proporcionavam a rede telefônica, não só a localização física do equipamento, mas também o seu número IMSI (*International Mobile Subscriber Identity*) e, com base neles, o número do celular ao qual estava associado. A admissibilidade da utilização desses dispositivos foi encontrada pela Corte interpretando o regime que regulamentava a coleta e tratamento, para fins policiais, de dados pessoais por forças de segurança (art. 22 da *Ley Orgánica* 15/1999, de 13 de dezembro, sobre proteção de dados pessoais. Cf. Ramalho, 2019, p. 195-243).

[3] A saber: *a) Delitos cometidos en el seno de organizaciones criminales. b) Delitos de terrorismo. c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente. d) Delitos contra la Constitución, de traición y relativos a la defensa nacional. e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.* Cf Espanha (2015).

[4] O dispositivo, contudo, não é claro se é possível ao juiz autorizar o acesso a computadores que não os do investigado, mas que estão sendo por ele utilizados para comunicação ou para armazenar dados, ou mesmo equipamentos que não estão sendo utilizados pelo suspeito, mas que contêm dados importantes para a investigação. Lorena Bachmaier Winter (2017, p. 12) entende possível o acesso a outros equipamentos que não os do investigado, utilizando por analogia as regras da art. 588 bis (h) da LEC que permite a interceptação das comunicações que afetem terceiros, na medida em que o acesso remoto a um dispositivo por meio de um *software* implica sempre uma das comunicações. Hernán Blanco (2021, p. 45) também entende possível a medida, sem, contudo, recorrer as normas regulam a interceptação das comunicações. Este último autor cita Ortiz Pradillo (2009, p. 1-9) como opositor dessa interpretação.

[5] *Artículo 588 septies c. Duración. La medida tendrá una duración máxima de un mes, prorrogable por iguales períodos hasta un máximo de tres meses.* Cf. Espanha (2015).

[6] Art. 307. A coleta por acesso forçado a dispositivo eletrônico, sistema informático ou redes de dados, ocorrerá somente após prévia desobediência de ordem judicial determinando a entrega da prova pretendida ou quando impossível identificar o controlador ou provedor em território nacional, e compreenderá os métodos de segurança ofensiva ou qualquer outra forma que possibilite a exploração, isolamento e tomada de controle (Brasil, 2010).

[7] Com isso, é suprida a divergência que existe na doutrina espanhola gerada em razão da ausência de previsão normativa quanto o alcance da medida em relação a terceiros, cf. nota de fim 5.

[8] Em julho de 2017, o legislador inseriu no CPP alemão (*Strafprozeßordnung* ou StPO) a norma do § 100b, que autoriza a infiltração *online*, nomeada *online Durchsuchung* e limita a medida a um rol de crimes graves previstos em lei no § 100b (2). Como referência dogmática acerca da previsão legal de *malware* no ordenamento alemão, confira: Grego e Gleizer (2019).

[9] Em fevereiro de 2020, por meio da Lei 7, o CPP italiano consagrou expressamente. em seu art. 266 2 e 2-bis, a admissão da técnica denominada de *captatore informatico.* De forma sintética, a medida é admitida: a) nas infrações penais que envolvam organizações criminosas e condutas assemelhadas, como terrorismo, por exemplo; b) em crimes contra a Administração Pública cometidos por funcionários público e dirigentes do serviço público; e c) em crimes comuns específicos descritos no código italiano. Como referência dogmática acerca da previsão legal de *malware* no ordenamento, cf. Diddi (2020, p. 2).

[10] O termo "prova digital" pode ser entendido como conjunto de "dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou ideias" (Vaz, 2012, p. 63). Eduardo de Urbano Castrillo (2009, p. 47) oferece outra definição, que enfatiza os suportes físicos, conceituando a prova digital permite comprovar factos através dos meios de reprodução de palavras, sons e imagens, bem como dos instrumentos que permitem arquivar e conhecer ou reproduzir palavras, dados, números e operações matemáticas realizadas para fins contabilísticos ou outros.

[11] Segundo Geraldo Prado (2014, p. 80), a cadeia de custódia é o dispositivo que objetiva assegurar os elementos probatórios em sua integridade. Trata-se de uma garantia constitucional contra a prova ilícita. Na visão de Carlos Edinger (2016, p. 242), a cadeia de custódia pode ser compreendida como uma sucessão de elos, tidos como qualquer pessoa que tenha manejado o vestígio. Nas palavras de Antonio Eduardo Ramires Santoro (2020, p. 297), "deve ser preservada a cadeia de custódia para permitir o rastreio às fontes de prova", o que é especialmente sensível com relação às provas digitais, cujo manuseio indevido pode comprometer a capacidade epistêmica da prova.

Referências

ALEMANHA. Strafprozeßordnung [Código de Processo Penal]. de 7 de abril de 1987. Disponível em: https://dejure.org/gesetze/StPO. Acesso em 17 set. 2023.

BLANCO, Hernán. El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre. *InDret: Revista para el Análisis del Derecho*, n. 1, p. 431-501, 2021. https://doi.org/10.31009/InDret.2021.i1.15

BRASIL. Câmara dos Deputados. *Projeto de Lei 8.045, de 22 de dezembro de 2010*. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1998273&filename=Tramitacao-PL%208045/2010. Acesso em: 20 jul. 2022.

CASTRILLO, Eduardo de Urbano. *La valoración de la pueba Eletronica*. Valência: Tirant lo Blanch, 2009.

DIDDI, Alessandro. Le novità in materia di intercettazioni telefoniche. Penale Diritto e Procedura. *Penale Diritto e Procedura*, 31 ago. 2020. Disponível em: https://penaledp.it/le-novita-in-materia-di-intercettazioni-telefoniche/. Acesso em: 7 nov. 2021.

EDINGER, Carlos. Cadeia de custódia, rastreabilidade probatória. *Revista Brasileira de Ciências Criminais*, v. 24, n. 120, p. 237-257, maio/jun. 2016.

ESPANHA. *Ley Orgánica 13/2015, de 5 de octubre*. Boletín Oficial del Estado 239, de 6 out. 2015. Disponível em: https://www.boe.es/boe/dias/2015/10/06/pdfs/BOE-A-2015-10725.pdf. Acesso em: 20 jul. 2022.

FERNANDES, Antonio Scarance. Reflexões sobre as noções de eficiência e de garantismo no processo penal. *In*: FERNANDES, Antonio Scarance; GAVIÃO DE ALMEIDA, José Raul; ZANOIDE DE MORAES, Maurício (Orgs.). *Sigilo no processo penal*. Eficiência e garantismo. São Paulo: RT, 2008. p. 9-28.

GREGO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal: notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal*, v. 5, n. 3, p. 1483-1518, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.278

LIGUORI, Carlos. *Direito e Criptografia*: direitos fundamentais, segurança da informação e os limites da regulação jurídica na tecnologia. São Paulo: Saraiva, 2022.

ORTIZ PRADILLO, Juan Carlos. El 'remote forensic software' como herramienta de investigación contra el terrorismo. *ENAC, E-Newsletter en la lucha contra el cibercrimen*, n. 4, p. 1-9, 2009.

PRADO, Geraldo. *Prova penal e sistema de controles epistêmicos*: a quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons, 2014.

RAMALHO, David Silva. *Métodos ocultos de investigação criminal em ambiente digital*. Coimbra: Almedina, 2019.

RAMALHO, David Silva. O uso de malware como meio de obtenção de prova em Processo Penal. *Revista de Concorrência e Regulação*, v. IV, n. 16, p. 195-243, 2013.

SANTORO, Antonio Eduardo Ramires. A cadeia de custódia na interceptação telefônica. ***In***: BRITO CRUZ, Francisco; FRAGOSO, Nathalie (Orgs.). *Direitos fundamentais e processo penal na era digital*. São Paulo: InternetLab, 2020, v. 3. p. 290-325.

SILVA, José Afonso da. *Curso de Direito Constitucional.* 11. ed. São Paulo: Revista dos Tribunais, 1996.

VAZ, Denise Provasi. *Provas digitais no processo penal:* formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012.

WINTER, Lorena Bachmaier. Acusatorio versus inquisitivo. Reflexiones acerca del processo penal. ***In***: GLOECKNER, Ricardo Jacobsen. (Org.) *Sistemas processuais penais*. Florianópolis: Empório do Direito, 2017. p. 57-93.

WINTER, Lorena Bachmaier. Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015. *Boletín del Ministerio de Justicia*, ano LXXI, n. 2.195, p. 3-36, jan. 2017.

Informações adicionais e declarações do autor (integridade científica)

Declaração de conflito de interesses: o autor confirma que não há conflitos de interesses na condução desta pesquisa e na redação deste artigo. **Declaração de autoria:** todos e somente os pesquisadores que cumprem os requisitos de autoria deste artigo são listados como autores; todos os coautores são totalmente responsáveis por este trabalho em sua totalidade. **Declaração de originalidade:** a autora garantiu que o texto aqui publicado não foi publicado anteriormente em nenhum outro recurso e que futuras republicações somente ocorrerão com a indicação expressa da referência desta publicação original; ela também atesta que não há plágio de terceiros ou autoplágio.

Como citar (ABNT Brasil)

COSTA ROSSI, H.; MUSA DE ALMEIDA, L. O uso do malware na investigação criminal: pontos de tensão e limites. Boletim IBCCRIM, [S. l.], v. 31, n. 373, [s.d.]. DOI: 10.5281/zenodo.10188525. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/693. Acesso em: 22 nov. 2023.

Recebido em: 15.08.2023 - Aprovado em: 12.09.2023 - Versão final: 23.10.2023