Arruda e Correra: Malware para coleta de provas no processo penal

22/07/2023

Há atualmente a ampla utilização de novas tecnologias para comunicação e negócios, tais como *criptomoedas*, *smart contracts* e *blockchain*. No Canadá, por exemplo, há recente decisão judicial que reconheceu o envio de *emoji* de sinal positivo em conversa por meio de aplicativo de telefone celular como formalização contratual [1].

O meio digital, além de relações jurídicas lícitas, também é palco de crimes, tais como o "estupro virtual" (artigo 213 do Código Penal), que entendemos viável apesar de divergências sobre sua tipificação [2]; o "revanche pornô" (artigo 218-C do Código Penal); o *cyberbullying e o cyberstalking*.

Os dois últimos podem ser praticados para a consumação do crime do artigo 147-A do Código Penal. O meio digital também é utilizado para articulação de terrorismo, tendo o grupo Al Qaeda [3] adotado o "rascunho" (sem envio) de uma caixa de correio eletrônico para coordenar ataques.

É possível formular questionamento sobre a viabilidade, no ordenamento pátrio, da utilização de *malware* ("vírus espião") [4] para acesso remoto a dispositivos digitais e coleta de dados para produção probatória. Quando um *malware* é instalado em um dispositivo, cria-se uma porta de acesso (*backdoor*) que permite a comunicação oculta e remota entre o dispositivo infectado e o invasor, possibilitando o monitoramento em tempo real e a captação de dados [5]. A dúvida é pertinente, na medida em que inexiste norma expressa contemplando esse método.

O mesmo questionamento pode ser aplicado à produção de provas por meio de geolocalização a partir de Estação Rádio Base (ERB), fora do âmbito do artigo 13-B do Código de Processo Penal. Afinal, como afirmam Valine Castaldelli Silva e Alexandre Ribas de Paulo [6], não há previsão legal para esse método probatório, que não pode ser confundido com dados informáticos estáticos, dados de comunicação via celular e localização pelo sistema GPS.

A questão se torna ainda mais relevante quando verificamos a necessidade de controle da compatibilidade das normas e ações estatais em face da Convenção Americana de Direitos Humanos (CADH) [7], especialmente artigo 11, item 02, que determinar o respeito à intimidade e vida privada.

Registre-se que, em comparação com países de tradição de *civil law* na Europa ocidental (constante fonte de inspiração do legislador pátrio), o referido método é previsto em lei na Alemanha (*StrafprozeBordnung (Stpo)* [8], §100b, conforme estudo de Juliana Filipa Souza Campos [9]; na Espanha, por meio da *Ley de Enjuiciamiento Criminal* [10], artigo 588 *septies*; na França em seu Código de Processo Penal, no artigo 706-102-1 [11] e na Itália no *Codice di Procedura Penale* [12], artigos 266 e 266 Bis.

No Brasil, o projeto do Novo Código de Processo Penal (com redação da Emenda Aglutinativa de Abril de 2021) [13] estabelece o método em seu artigo 304, II.

Em termos de *common-law* dos Estados Unidos, o *Federal Rules of Criminal Procedure* [14], na regra 41, contempla expressamente a possibilidade de acesso remoto a mídias digitais, viabilizando, portanto, o uso do *malware*.

Gustavo Alves Magalhães Ribeiro, Pedro Ivo Rodrigues Velloso Cordeiro e Débora Moretti Fumach [15] afirmam inexistir possibilidade de utilização de *malware* no direito pátrio, diante da impossibilidade de sua equiparação com captação ambiental, interceptação telemática e infiltração de agentes. É o mesmo posicionamento de Andreia Filipa Santos Duarte [16] ao tratar do ordenamento jurídico de Portugal, que apresenta o mesmo desafio aqui exposto, embora exista quem afirme [17] que o artigo 19, item 2 da "Lei do Cibercrime" [18] contempla o mecanismo de *malware*. Em síntese, para fins probatórios, seria vedada a interpretação ampliativa e analógica dos dispositivos vigentes.

A linha de pensamento exposta encontra respaldo na Corte Europeia de Direitos Humanos [19] que, em julgamento envolvendo a legislação da França e a utilização de monitoramento por GPS (geolocalização) como forma de produção probatória na esfera penal, afirmou que, à época dos fatos (anterior a 2010), a ausência de norma expressa na França sobre o tema impedia o uso da tecnologia, sendo insuficiente a mera existência de normas legais genéricas sobre provas.

Discordamos do entendimento acima exposto e acolhemos a possibilidade de aplicação imediata do *malware* no Brasil em sede processual penal. José Antônio Santos Cabral [20] afirma que, diante da ausência de norma legal expressa, bem como diante da necessidade de enfrentar um perigo concreto, admite-se que as novas tecnologias, que afetam direitos fundamentais, sejam aplicadas mediante ponderação sufragada no princípio da proporcionalidade.

Diego Roberto Barbiero [21] admite novas tecnologias como meio probatório em casos complexos que envolvam crime organizado. Felipe Giardini [22] admite a utilização do método em questão como prova atípica; afirma que a omissão legislativa sobre o meio probatório é involuntária e, dessa forma, não pode ser interpretada como vedação.

O *malware,* quando aplicado em dispositivos digitais, permite, conforme programação, a coleta dos seguintes elementos: 1) dados armazenados no dispositivo, 2) registros de comunicações realizadas entre presentes (gravação de áudio e vídeo) e 3) interceptação de dados de voz ou telemáticos transmitidos. A Lei 9.296/1996 [23], artigos 1º e 8-A, permitem a interceptação de voz, dados telemáticos, além da captação ambiental de sinais eletromagnéticos, ópticos ou acústicos. Há, ainda, no ordenamento pátrio, a possibilidade de busca e apreensão de equipamentos eletrônicos para acesso aos dados armazenados [24].

Assim, os procedimentos viabilizados por meio de *malware* estão previstos e admitidos na legislação processual penal. O fato do uso do 'vírus espião' não estar expressamente previsto em lei, em nosso entender, não afasta a legalidade da sua utilização, na medida em que simplesmente vai proporcionar, por meio remoto, a realização de diligências autorizadas em lei. Em outras palavras, não gera inovação quanto à prova produzida, apenas viabiliza sua produção por meio remoto.

O *malware*, portanto, pode ser utilizado como forma de produção probatória na esfera penal, respeitadas as mesmas exigências previstas na Lei 9.296/96 para interceptação de voz e telemática, bem como captação ambiental de sinais eletromagnéticos, ópticos e acústicos.

Importante destacar que não se concebe, em face dos métodos já aplicados, o "vírus espião" como uma forma mais invasiva. Não se pode acolher argumento no sentido de que, diante de sua lesividade à intimidade e vida privada, haveria necessidade de expressa autorização legal. O *malware* não opera qualquer prática não contemplada na Lei 9.296/96.

O STJ (Superior Tribunal de Justiça) [25], em recente decisão, entendeu como válida a prova produzida por meio remoto, mediante o "espelhamento" de um aplicativo de mensagens. Considerou, em síntese, que a medida realizada com autorização judicial estava abarcada pelo instituto do "agente infiltrado". Embora o *malware*, em nosso entender, não possa ser equiparado ao "agente infiltrado" (trata-se de um "vírus malicioso" e não da atividade de um agente), a decisão demonstra evolução do Poder Judiciário sobre a aplicação de tecnologias não expressamente contempladas na lei para produção de provas na esfera penal.

A verdade é que a demora do Poder Legislativo não pode impedir a aplicação de tecnologias que, simplesmente, buscam produzir provas já contempladas na legislação.

Por fim, caso o legislador pátrio pretenda modificar a legislação penal, deveria elaborar norma consolidando e sistematizando as provas digitais na esfera penal. Poderia tomar como base as legislações dos países da Europa ocidental. Não ignoramos as dificuldades decorrentes do transplante de normas para o Brasil, conforme obra de Watson [26]. Contudo, com as cautelas recomendadas pelo citado autor (atentar ao contexto sociocultural), entendemos possível a importação dos institutos, com a vantagem de aproveitarmos as experiências adquiridas pelos referidos países.

[1] CANADÁ. *Southwest Terminal Ltd. V. Achter Land & Cattle Ltd.* 2023 SKKB 116. Disponível em: https://cdn-conjur.s3.amazonaws.com/uploads/2023/07/2023skkb116-480130.pdf. Acesso em 10 jul. 2023.

[2] MARODIN, Tayla Schuste. *O Crime de Estupro Virtual: (Des)necessidade de Tipificação pelo Ordenamento Jurídico Brasileiro.* Dissertação de Mestrado. Pontifícia Universidade Católica do Rio Grande do Sul: 2021. Passim.

[3] UCHOA DE BRITO, Auriney. *Direito Penal Informático.* São Paulo: SaraivaJur, 2017. Ebook Kindle. Posição 774.

[4] RAMALHO, David Silva, "*O Uso de Malware como Meio de Obtenção de Prova em Processo Penal*", *Revista de Concorrência e Regulação*, ano IV, nº 16 (outubro/dezembro), 2013. p. 201.

[5] MENDES, Carlos Hélder Carvalho Furtado. *Tecnoinvestigação Criminal:* entre a Proteção de Dados e a Infiltração por Software. Salvador: JusPodivm, 2020. P. 164.

[6] CASTALDELLI SILVA, Valine; RIBAS DE PAULO, Alexandre. A (In)admissibilidade do Uso das Informações Obtidas por Meio da Estação Rádio Base (ERB) no *Ius Persequendi* Brasileiro. *Revista Cadernos do Programa de Pós-Graduação em Direito/UFRGS* v. 14 nº 1, p. 140-160, (2019). P. 150-151.

[7] ORGANIZAÇÃO DOS ESTADOS AMERICANOS. *Convenção Americana de Direitos Humanos.* Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/D0678.htm. Acesso em 17 mai. 2023.

[8] ALEMANHA. *StrafprozeBordnung (Stpo).* Disponível em: https://www.gesetze-im-internet.de/stpo/BJNR006290950.html. Acesso em 14 jul. 2023.

[9] CAMPOS, Juliana Filipa Souza. *O Malware como Meio de Obtenção da Prova em Processo Penal.* A Investigação Oculta em Ambiente Digital. Coimbra: Almedina, 2021. P. 120-121.

[10] ESPANHA. *Ley de Enjuiciamiento Criminal.* Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036. Acesso em 26 jun de 2023.

[11] FRANÇA. *Code de Procédure Pénale.* Disponível em: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISCTA000006167524/?. Acesso em 04 jul 2023.

[12] ITÁLIA. *Codice di Procedura Penale.* Disponível em: https://www.gazzettaufficiale.it/dettaglio/codici/codiceProceduraPenale. Acesso em 09 maio 2023.

[13]BRASIL. *Projeto de Lei 8.045 de 2010.* Código de Processo Penal. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=490263. Acesso em 04 jul 2023.

[14] ESTADOS UNIDOS DA AMÉRICA. *Federal Rules of Criminal Procedure.* Disponível em: https://www.uscourts.gov/sites/default/files/federal_rules_of_criminal_procedure_-december_2020_0.pdf. Acesso em 06 jul 2023.

[15] RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O Malware como Meio de Obtenção de Prova e a sua Implementação no Ordenamento Jurídico Brasileiro. *Revista Brasileira de Direito Processual Penal*, *[S. l.]*, v. 8, nº 3, 2022. DOI: 10.22197/rbdpp.v8i3.723. Disponível em: https://revista.ibraspp.com.br/RBDPP/article/view/723. Acesso em: 2 jul. 2023.

[16]DUARTE, Andreia Filipa Santos. *O Malware como Meio de Obtenção de Prova em Processo Penal.* Dissertação de Mestrado da Universidade de Coimbra. Coimbra: 2022. P. 44

[17] OLIVEIRA, Ana Teresa Seabra de. *Obtenção de Prova Digital:* Utilização de Malware pelos Órgãos da Polícia Criminal. Dissertação de Mestrado da Universidade do Minho. Minho: 2017. P. 71.

[18] PORTUGAL. *Lei 109/2009 (Lei do Cibercrime)*. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis. Acesso em 06 mar 2023.

[19] CORTE EUROPEIA DE DIREITOS HUMANOS. *Ben Faiza c. França* (de 8 de maio de 2018).

[20] CABRAL, José António Santos. *Código de Processo Penal Comentado.* Coimbra: Almedina, 2014. P. 427.

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

[22] GIARDINI, Felipe. Malware Estatal na Investigação Criminal. P. 63-80. PAULINO, Galtiênio da Cruz; SCHOUCAIR, João Paulo Santos; BALLAN JUNIOR, Octahydes; MAIA, Tiago Dias. *Técnicas Avançadas de Investigação.* Vol. 2. Brasília: ESMPU, 2022.

[23]BRASIL. *Lei 9.296/1996*. Regulamenta o inciso XII, parte final, do artigo 5° da Constituição Federal. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm. Acesso em 07 mar 2023.

[24] BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. *AgRg no HC 675.582/PE.* Quinta Turma. Relator: ministro Reynaldo Soares da Fonseca, DJe 30 ago. 2021.

[25] BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. *AGR em RESP. Nº 2257960 – MG.* Relator ministro Reynaldo Soares da Fonseca. J. 16 mai. 2023.

[26] WATSON, Alan. *Legal Transplants: An Approach to Comparative Law*. 2.ed. *Athens: University of Georgia*, 1993. Passim.

Fonte: https://conjur.jumps.com.br/2023-jul-22/arrudae-correra-malware-coleta-provas-processo-penal/