Contornos sobre a utilização de captadores informáticos no Processo Penal

A crescente introdução de inovações tecnológicas no campo investigativo tem tornado cada vez mais complexa a abordagem jurídica desses instrumentos no âmbito processual penal. Exemplo disso é a adoção de métodos informáticos atípicos, como os captadores informáticos, que nada mais são que *malwares* [1] do tipo "cavalo de troia" (ou *trojan*), por meio dos quais é possível interceptar, em tempo real, todas as comunicações eletrônicas realizadas pelo dispositivo eletrônico alvo.

Spacca

Trata-se de um novo e poderosíssimo instrumento investigativo que não se encontra atualmente regulamentado pelo direito brasileiro, constituindo meio de obtenção de prova atípico, não obstante sua utilização demande uma série de cuidados particulares, principalmente de modo a não malferir garantias constitucionais dos indivíduos afetados.

Nesse sentido, o vácuo legislativo acaba por deixar o uso das técnicas de captação à mercê da discricionaridade dos investigadores, enquanto as elaborações jurisprudenciais se limitam a referenciar decisões correlatas – como por exemplo casos de interceptações telefônicas -, as quais, no entanto, não conseguem abranger a complexidade imposta pelas novas tecnologias.

Como bem assinala Gabriella Di Paolo [2] acerca da realidade estadunidense, "impulsionada por casos que trouxeram à tona ferramentas de investigação inéditas, portanto, sem regulamentação específica, a jurisprudência geralmente enfrentou o problema questionando se não seria adequado evitar ou limitar seu uso à luz dos princípios constitucionais ou se, ao contrário, poderiam ser atribuídos ao regime normativo referente às atividades instrutórias tipificadas pelo legislador".

Já na Itália, após um período em que os tribunais tentaram, em um papel de suplência, conformar as novas tecnologias de captação às bases jurídicas já estabelecidas (mormente as relativas às

interceptações telefônicas), em 2017 uma mudança legislativa [3] introduziu no Código de Processo Penal italiano regras para o uso dos captadores de dados informáticos nas investigações criminais.

Ainda que se possa tecer diversas críticas à iniciativa normativa italiana (como, por exemplo, limitar o alvo das captações à "dispositivos móveis" e não abordar mais detalhadamente os tipos de desdobramentos da vigilância posterior à introdução do *malware*), fato é que a positivação avançou significativamente no campo do tratamento de questão extremamente sensível no tocante às garantias fundamentais.

Diversos exemplos

E não se trata de preciosismo italiano: há diversos exemplos de sistemas jurídicos que têm optado por abordagens legislativas exclusivas dedicadas às diferentes formas de vigilância eletrônica, como a possibilidade de "registros remotos sobre equipos informáticos" aprovada pela Espanha (Capítulo IX da Lei Orgânica n. 13/2015), bem como a inovação no ordenamento da França estatuída pela Lei n. 2011/267, de março de 2011, a qual passou a autorizar a instalação de dispositivo técnico com a finalidade de acessar, registrar, armazenar e transmitir dados informáticos de sistemas automatizados de processamento de dados utilizados por pessoas investigadas [4].

Spacca

Em uma rápida pesquisa jurisprudencial em busca de entendimentos relacionados a captadores informáticos, verifica-se que o Brasil está em um momento anterior a de países como Estados Unidos, Itália e França: não se encontram julgados debatendo a questão, de modo que a tipificação do referido meio de obtenção de prova parece, hoje, ainda distante.

Não obstante esse panorama, entende-se que o debate deve ser fomentado antes mesmo que o uso da técnica ganhe corpo nas investigações, a fim de mitigar possíveis violações à princípios constitucionais ou a necessidade de declaração de nulidades que poderiam ser evitadas caso fossem seguidos requisitos mínimos para a produção das provas obtidas com o uso dos métodos de captação de dados informáticos.

Basta, para tanto, pensar que a introdução de um *malware* em um dispositivo eletrônico talvez seja, considerando o mundo ultraconectado em que vivemos, a intromissão mais gravosa na vida privada de um cidadão, porquanto permite a vigilância em tempo real, de uma só vez, sobre ligações telefônicas, comunicações em texto e por meio audiovisual em aplicativos como WhatsApp, Facebook e Instagram, assim como acesso a contas de e-mails e a arquivos das salvos em laptops, smartphones, tablets e afins.

Conclui-se, assim, ser razoável que métodos de vigilância eletrônica já amplamente difundidos no mundo, como é o caso dos captadores informáticos, sejam submetidos a um regime de regulatório legal diferenciado, e não relegados à mera proteção geral das garantias individuais.

Por isso é que estamos com Lorenzo Picotti quando, ao analisar a relevância das normas jurídicas frente à imposição da evolução tecnológica, reafirma a função histórica e política do Direito na regulação das "relações sociais, de forma publicamente previsível e com base em um consenso democraticamente expresso", arrematando que "também no ciberespaço são necessárias regras jurídicas reconhecíveis e compartilhadas, dotadas de eficácia e sujeitas à aplicação coercitiva, na hipótese de não adesão ou respeito por parte dos destinatários, recorrendo, portanto, também a meios sancionatórios formais e coercitivos, reservados a autoridades e juízes imparciais, em conformidade com os princípios do Estado de direito" [5].

_____

[1] 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. ALVES MAGALHÃES RIBEIRO, Gustavo; RODRIGUES VELLOSO CORDEIRO, Pedro Ivo; MORETTI FUMACH, Débora. 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, n. 3, 2022. DOI: 10.22197/rbdpp.v8i3.723. Disponível em: https://revista.ibraspp.com.br/RBDPP/article/view/723.. Acesso em: 25 abr. 2024.

[2] DI PAOLO, Gabriella. **“Tecnologie del controllo” e prova penale**: l’esperienza statunitense e spunti per la comparazione. Trento: CEDAM, 2008. p. 16-22.

[3] Art. 4 do Decreto Legislativo n. 216, de 29 de dezembro de 2017.

[4] Art. 706-102-1 do Código de Processo Penal francês, incluído pelo art. 36 da Lei n. 2011-267, de 14 de março de 2011.

[5] PICOTTI, Lorenzo. Quale diritto penale nella dimensione globale del cyberspace? *In* WENIN, Roberto; FORNASARI, Gabriele (Org.). **Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali**. Napoli: Editoriale Scientifica, 2015. p. 312-313.

Autores: Aury Lopes Jr., Alexandre Morais da Rosa, Alexandre Claudino Simas Santos