

SOFTWARES ESPIÕES COMO MEIO DE COLETA DE PROVAS NO PROCESSO PENAL: VIGILÂNCIA DIGITAL E O DIREITO FUNDAMENTAL À INTIMIDADE

SPY SOFTWARE AS A MEANS OF COLLECTING EVIDENCE IN CRIMINAL PROCEEDINGS: DIGITAL SURVEILLANCE AND THE FUNDAMENTAL RIGHT TO PRIVACY

Luis Fernando de Menezes[1]
Centro Universitário Univel – Cascavel/PR, Brasil
luisfernandomnzs@gmail.com

Marco Felipe Torres Castello[2]
Centro Universitário Univel – Cascavel/PR, Brasil
prof.marcofelipe@gmail.com

RESUMO: O avanço tecnológico trouxe consigo novas formas de investigação criminal, entre elas o uso de "softwares" espiões, comumente chamados de "spywares". Este estudo propõe-se a analisar a efetiva utilização dessas ferramentas digitais na produção de provas que servem à persecução penal. Dada a ausência de regulamentação específica no Brasil acerca da utilização dessas ferramentas para fins de investigação criminal, a pesquisa visa perquirir a legitimidade do seu uso em face do direito à intimidade e do devido processo legal, ambos de estatura constitucional. Além disso, caso admitida a possibilidade de utilização de "spywares" na investigação criminal, o estudo objetiva trazer reflexões acerca da natureza jurídica desse meio de obtenção de provas. Isso porque os programas espiões podem proporcionar acesso a uma vasta gama de dados pessoais, incluindo comunicações, localização e hábitos de navegação (Mendes, 2020). Essas capacidades levantam questões sobre sua natureza jurídica e os limites de sua aplicação. A equiparação da utilização desses programas espiões à interceptação telefônica baseia-se na similaridade do processo de captação de comunicações em tempo real, por exemplo. De outro lado, esses programas podem admitir não a interceptação em tempo real, mas o acesso a dados armazenados e "metadatas", hipótese em que se aproximará da busca e apreensão digital (Konno Júnior, 2020). Esta dualidade complica sua classificação jurídica e, consequentemente, a definição dos requisitos legais para sua utilização. O estudo propõe-se a

[1] Residente Jurídico no Ministério Público do Estado do Paraná, mestrando em Direito, Inovações, e Regulações no Centro Universitário UNIVEL – Cascavel/PR, pós-graduado em Ciências Criminais pelo Complexo de Ensino Renato Saraiva (CERS); bacharel em direito pelo Centro Universitário UNIVEL – Cascavel/PR, bacharel em ciências aeronáuticas pela Pontifícia Universidade Católica de Goiás (PUC/GO); Advogado. E-mail para contato: luisfernandomnzs@gmail.com. OrcID: https://orcid.org/0009-0000-9454-5578

[2] Promotor de Justiça no Ministério Público do Estado do Paraná, mestrando em Direito, Inovações, e Regulações no Centro Universitário UNIVEL – Cascavel/PR, pós-graduado em Direito Penal e Processo Penal e em Direito Constitucional pela Universidade Damásio de Jesus; bacharel em Direito pela Universidade Federal de Mato Grosso do Sul (UFMS). E-mail para contato: prof.marcofelipe@gmail.com. OrcID: https://orcid.org/0009-0007-4906-9702.

examinar a legislação vigente, especialmente a Lei nº 9.296/1996 (Lei de Interceptações Telefônicas), os artigos 240 e seguintes do Código de Processo Penal e o Marco Civil da Internet (Lei nº 12.965/2014), buscando identificar possíveis lacunas e a necessidade de regulamentação específica. O contexto inafastável da evolução tecnológica dos instrumentos disponíveis à investigação apresenta o desafio de equilibrar a proteção à privacidade com a necessidade de prover instrumentos eficazes de investigação criminal. Por meio da pesquisa exploratória, de natureza bibliográfica e documental, aplicando o método dedutivo, a pesquisa, além de pontuar decisões judiciais e entendimentos doutrinários sobre o tema, também abordará experiências internacionais, como o caso do programa "Pegasus", utilizado por governos para vigilância digital, e decisões de Cortes internacionais sobre o tema. Por fim, o estudo busca propor critérios para o uso legítimo de programas espiões em investigações criminais, analisando a possibilidade de utilização da vigilância digital como instrumento legítimo ou não na produção de provas no processo penal, ante um necessário equilíbrio entre a eficácia investigativa e a proteção dos direitos fundamentais no Estado Democrático de Direito.

Palavras-chave: Programas espiões; Vigilância digital; Direito à intimidade; Persecução penal.

REFERÊNCIAS

KONNO JÚNIOR, Janio. Interceptação telemática ou busca e apreensão de dados em nuvem e a preservação da cadeia de custódia. *In:* JORGE, Hugo Vinícius Nogueira (Coord.). **Tratado de Investigação Criminal Tecnológica.** Salvador: Editora Juspodivm, 2020. p. 253-268.

MENDES, Carlos Hélder C. Furtado. **Tecnoinvestigação Criminal:** entre a proteção de dados e a infiltração por *software*. Salvador: Editora Juspodivm, 2020.

SUPREMA CORTE DOS ESTADOS UNIDOS DA AMÉRICA. **Caso NSO Group Technologies Limited, et al., Petitioners v. WhatsApp Inc., et al.** Sentença de 7 de dezembro de 2022. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.supremecourt.gov/DocketPDF/21/21-1338/249362/20221207141455354_Supplemental_Brief%20of%20Respondents.pdf. Acesso em: 25 ago. 2024.