Software de espionagem para investigação traz desafio regulatório

No começo de dezembro, o fundador e presidente da SaferNet Brasil, Thiago Tavares, decidiu deixar o país e se exilar voluntariamente na Alemanha. A decisão ocorreu após a descoberta de que teve seu computador invadido pelo programa espião Pegasus.

123RF

Uso de softwares de espionagem que não deixam rastro como o Pegasus representam verdadeiro desafio regulatório mesmo se usados por autoridades policiais e MP
123RF

A decisão foi revelada em uma carta endereçada aos funcionários, colaboradores e integrantes de instituições parceiras. No texto, ele revela que foi ameaçado de morte após participar no dia 26 de outubro de uma mesa do "Seminário Internacional Desinformação e Eleições" do Tribunal Superior Eleitoral.

O drama de Tavares levantou o debate sobre o uso do Pegasus no país e de outras ferramentas de monitoramento eletrônico. Oficialmente, o software israelense só pode ser vendido para governos sob a justificativa de ser usado para combater o terrorismo. Extraoficialmente, contudo, ele tem sido usado para espionar jornalistas, ativistas e adversários políticos.

A software é capaz de invadir celulares, computadores e outros sistemas apenas com um clique de uma mensagem ou abertura de um vídeo enviado por WhatsApp. Instalado, a ferramenta concede acesso a qualquer informação do aparelho, sendo inclusive capaz de ativar o microfone e câmera.

Em julho deste ano, a defesa do ex-presidente Lula protocolou petição no Supremo com diálogos que revelam que procuradores do consórcio da "lava jato" demonstraram interesse pela ferramenta.

Na petição assinada pelos advogados **Valeska Teixeira Martins** e **Cristiano Zanin**, da defesa do ex-presidente, "a operação 'lava jato' teve contato com diversas armas de espionagem cibernética, incluindo o Pegasus".

Numa conversa no chat do grupo de procuradores em 31 de janeiro de 2018, é citada uma reunião entre os membros da franquia do Rio de Janeiro, com a central de Curitiba e representantes de uma empresa israelense que vendia uma "solução tecnológica" que "invade celulares em tempo real (permite ver a localização etc)".

Em 2016, reportagem exclusiva da **ConJur** revelava um *modus operandi* de operações de espionagens ilegais por parte da autoproclamada força-tarefa. Em fevereiro daquele ano, o então juiz Sergio Moro quebrou o sigilo telefônico de Lula, seus familiares e advogados para monitorar suas estratégias de defesa.

Quem pode usar?
No Brasil, as únicas autoridades que detém a prerrogativa de utilizar softwares espiões são aquelas que atuam em investigações criminais. O uso dessas ferramentas precisa ser autorizado pela Justiça e o monitoramento é feito com limites estabelecidos. Ou seja, as autoridades que podem pedir monitoramento com uso dessas ferramentas conforme o regramento brasileiro é a autoridade policial e o Ministério Público, sob autorização de um juiz competente sobre fatos e pessoas.

Um dos aspectos mais problemáticos do uso de ferramentas como o Pegasus é que não deixa rastros. A possibilidade de utilização de um programa pela autoridade policial ou MP necessariamente precisa ser auditável para controle, caso contrário, pode contaminar a produção de provas.

A Lei n. 9.296/1996, no artigo 2º, parágrafo único, afirma que a quebra de sigilo deve descrever com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.

Indo além, o Marco Civil da Internet do Brasil (Lei 12.965/2014) vai no mesmo sentido, garantindo, no artigo 10, § 2º, que o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer.

André Damiani, criminalista especializado em Direito Penal Econômico e LGPD, sócio fundador do Damiani Sociedade de Advogados, explica que o uso de aplicativo espiões por pessoa física constitui crime de invasão de dispositivo informático, antevisto no artigo 154-A do Código Penal, o que prevê pena de três meses a um ano de prisão, além de pena.

Se a arapongagem tiver como alvo autoridades como o presidente da República, governadores, prefeitos, presidente do Supremo ou das casas legislativas, essa pena é aumentada de um a dois terços.

O especialista refuta a alegação do uso de um programa como o Pegasus. "Utilizar o Pegasus a pretexto de combater ao terrorismo é uma afronta ao Estado democrático de Direito, violando os princípios e garantias constitucionais, tais como: vida privada, intimidade, a liberdade de manifestação do pensamento, de expressão, de informação, de comunicação e de opinião; confidencialidade e integridade dos sistemas informáticos pessoais, garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal etc", explica.

Aplicativo espião e LGPD

Damiani explica que é preciso criar uma LGPD para investigação criminal, já que a própria Lei n. 13.709/2018 define, no artigo 4º, § 1º, que o tratamento de dados pessoais para fins de segurança pública e atividades de investigação de infrações penais será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular.

A advogada **Iara Peixoto Melo**, sócia do Chenut Oliveira Santiago Advogados, é especialista em LGPD e explica que essa lei não é aplicável em investigações criminais, mas isso não quer dizer que não exista proteção a privacidade de investigados. "A parte que vejo mais interessante nesse caso é que essas questões levantadas pelo uso de ferramentas como Pegasus para investigação tem como particularidade serem transfronteiriças. Então, mesmo que temos tipificações específicas, é importante avançar no sentido de aderir a acordos internacionais", diz.

A especialista lembra que aprovação do Senado da adesão do Brasil à Convenção de Budapeste (Projeto de Decreto Legislativo 255/2021) que trata de crimes cibernéticos. "Esse seria um passo interessante, já que ela é assinada por 66 países, além de usada por outros 158 como orientação para suas legislações nacionais", diz.

Em julho deste ano, o professor de Direito Internacional, Direito Comparado e Novas Tecnologias da UFMG (Universidade Federal de Minas Gerais), **Fabrício Bertini Pasquot Polido**, defendeu em artigo publicado na **ConJur** que o país aderisse ao tratado internacional.

"Ao contrário de outros crimes que ocorrem dentro do território nacional, o cibercrime pode ser praticado além das nossas fronteiras. Nesse sentido, aderir a acordos de cooperação internacional pode ser um caminho para avançar nessa questão", explica Iara.

Date Created
26/12/2021