Opinião: A ‘Lava jato’ e a não investigação de software espião

No último 18, o consórcio jornalístico encabeçado pelo jornal *The Guardian* divulgou uma lista com mais de 50 mil pessoas afetadas pelo Pegasus, *software* espião vendido pela empresa israelense NSO

A lista confirma o que o Citizen Lab já desconfia desde 2016 : ao contrário do que publiciza a NSO Group, não há controle sobre como governos usam a ferramenta. O vazamento indica, por exemplo, que diversos jornalistas, opositores políticos e ativistas de direitos humanos foram espionados pelo *software*.

O escândalo de proporções globais levantou preocupações importantíssimas no campo dos direitos humanos, sobretudo no que diz respeito à segurança das comunicações. Figuras como Angela Merkel vieram à público defender restrições à programas espiões. Ao mesmo tempo, Edward Snowden iniciou campanha por uma moratória internacional para a indústria de *software* ofensivo, alertando que não há regulamentação para esse setor.

Como defende Snowden, empresas como a NSO Group comercializam livremente armas informáticas, que embora sejam vendidas como ferramentas para investigar fatos criminosos, são utilizadas para espionar dissidentes políticos. Mais do que isso, a naturalização desses serviços abre espaço para um nebuloso mercado, no qual caçadores de *bugs* escrutinam sistemas para encontrar vulnerabilidades e vender os achados para corporações, como a NSO Group.

A relevância desses temas é global. No entanto, uma importante questão jurídica parece passar em branco nas terras brasileiras.

Desde 2019, a imprensa brasileira relata que representantes da NSO Group abordam secretarias, órgãos de segurança, Ministério Público e serviços de inteligência ofertando a ferramenta. Há elementos concretos de que o Pegasus foi oferecido aos militares brasileiros em reunião demonstrativa. Além disso, o Ministério da Justiça e Segurança Pública chegou a iniciar o Pregão Eletrônico nº 3/21 para "aquisição de solução de inteligência". Nesse episódio, a empresa brasileira responsável por comercializar o Pegasus cogitou proposta. Porém, após pressão da mídia e da sociedade civil, retirou-se do processo licitatório.

2023 - www.conjur.com.br - Todos os direitos reservados.

Somado a isso, no último 26 a defesa do ex-presidente Luiz Inácio Lula da Silva protocolou petição no Supremo Tribunal Federal alegando, com base em supostos chats entre procuradores da força-tarefa da "lava jato", que o *software* Pegasus foi ofertado aos servidores públicos. Nas conversas, que não são confirmadas pelos procuradores, discute-se o funcionamento e a viabilidade processual da ferramenta.

Do ponto de vista processual penal, não há respaldo para o uso de software espião em investigações criminais. O artigo 5º, XII, da Constituição, permite que as comunicações pessoais sejam violadas apenas para fins de investigação criminal ou instrução processual penal, nas hipóteses e na forma que a lei estabelecer. Embora o projeto do novo Código de Processo Penal pretenda inovar neste aspecto, no atual ordenamento jurídico brasileiro, o único regramento para a interceptação de comunicações é a Lei nº 9.296/96. Por isso, além de interpretar a quebra do sigilo das comunicações privadas como medida restrita ao processo penal, tribunais utilizam a Lei nº 9.296/96 como parâmetro para decidir sobre quebras de sigilo de conversas armazenadas [1].

Ainda que a falta de disposição legal não represente suficiente entrave para medidas restritivas de direito atípicas no processo penal, em dois casos paradigmas, o Superior Tribunal de Justiça já invalidou provas obtidas em contextos nos quais a autoridade policial se substitui ao usuário da aplicação [2]. São julgados que demonstram um problema fundamental: quando o investigador toma controle do dispositivo, não há como garantir que as mensagens foram preservadas em sua originalidade ou que o alvo da medida é, de fato, responsável por produzir o conteúdo.

Os julgados evidenciam que não há viabilidade da ferramenta Pegasus dentro do processo penal. Ainda que uma ordem judicial autorizasse o seu uso, as provas obtidas seriam ilícitas. Logo, o Estado brasileiro deveria desenvolver arcabouço jurídico próprio antes de voltar os olhos para tais alternativas probatórias.

Ante o cenário, causa perplexidade que autoridades brasileiras tenham mostrado interesse nas propostas comerciais dos vendedores do Pegasus. Além disso, parece estranho que, após conhecer o funcionamento do sistema, ditos servidores não procederam qualquer reflexão jurídico-penal sobre o que lhes foi oferecido.

Embora o Pegasus seja vendido como *software* proprietário, sabe-se que a ferramenta reúne diferentes vulnerabilidades não conhecidas pelo desenvolvedor para permitir a tomada de controle do sistema operacional de um dispositivo, em especial smartphones. Não se trata da interceptação de dados que passam por aplicações específicas, mas sim uma verdadeira invasão.

No Código Penal brasileiro (CP), a conduta de invadir dispositivo informático com o fim de obter dados ou informações sem autorização expressa ou tácita do usuário é crime, conforme artigo 154-A, do CP. Vê-se que o uso do Pegasus por agentes estatais se amolda à conduta típica, embora deva-se destacar que o injusto penal não restaria caracterizado em um cenário no qual há previsão legal e ordem judicial autorizando o uso da ferramenta. A discussão, portanto, não é sobre a prática da invasão, ainda que se possa discutir a ilegalidade de uma ordem judicial que autorizasse o uso do Pegasus no atual panorama jurídico. O que interessa, é refletir a potencial aplicabilidade do §1º, do artigo 154-A, CP.

2023 - www.conjur.com.br - Todos os direitos reservados.

Diz o §1º, do artigo 154-A, que *"na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput"*. Conforme a descrição típica conjugada ao elemento subjetivo do *caput*, o fato de oferecer *software*, sabendo que este será usado para viabilizar invasão não autorizada de um dispositivo informático, é crime na legislação brasileira.

Em trabalhos passados, o crime do §1º do artigo 154-A foi criticado por criminalizar atos meramente preparatórios. Dita censura permanece, pois, como afirmam D'Avila e Santos ao analisar a recomendação da Convenção de Budapeste que influenciou a lei local, o crime é *"desprovido de lesão ou perigo de lesão ao objeto de tutela da norma"* [3]. Além da crítica, apontou-se que, diante da necessidade de representação (artigo 154-B), o §1º do artigo 154-A carece de correlação entre o software comercializado e dano, já que sem identificar a vítima, não haverá condição de procedibilidade.

Abrem-se, então, dois questionamentos sobre a oferta do Pegasus às autoridades brasileiras: 1) ao exporem o *software* à venda, os representantes comerciais praticaram o crime do §1º do artigo 154-A CP? 2) se sim, ao tomar conhecimento do fato típico, os servidores públicos deveriam ter comunicado a possível existência de crime?

A resposta ao questionamento 1 não é simples. No âmbito da segurança pública, o Estado pode adquirir instrumentos cuja posse é proibida ao cidadão. O principal exemplo é a arma de fogo, que por vezes é produzida e ofertada por pessoas jurídicas de natureza privada.

Segundo o artigo 17 do Estatuto do Desarmamento, vender ou expor à venda arma de fogo sem autorização ou em desacordo com determinação legal ou regulamentar é crime. Diferente do §1º do artigo 154-A o artigo 17 exclui a tipicidade quando a venda é realizada conforme o complemento legal. As obrigações impostas às empresas não constam apenas no estatuto, mas também em decretos, como o nº 9.847/2019, que permite a comercialização e garante o controle das armas de fogo. O campo é tão amplamente regulado, que ainda que a parte final do tipo não existisse, o estabelecimento que cumprisse todas as normas atinentes à comercialização jamais cometeria o crime do artigo 17, já que uma consideração conglobada da norma eliminaria o caráter típico da ação.

Situação idêntica não se encontra no campo dos *softwares* espiões. Além da ausência de legislação processual penal ou de precedentes judiciais autorizativos, não foram encontradas disposições legais que regulem a indústria. Ao que indica a pesquisa, a União nunca emitiu leis ou decretos que permitissem o desenvolvimento e comercialização de softwares voltados para a invasão de dispositivos eletrônicos.

2023 - www.conjur.com.br - Todos os direitos reservados.

No campo das consultorias de cibersegurança, a falta de regulamentação não implica em risco penal, já que um teste de penetração para diagnóstico de vulnerabilidades só ocorre com o consentimento do titular do dispositivo. Assim, ao desenvolver *software* malicioso, o consultor não realiza o tipo do §1º do artigo 154-A. Ou seja, não *"produz programa de computador com o intuito de permitir a prática da conduta definida no caput"*. Contudo, no caso Pegasus, salvo alguma desconhecida norma que permita a consideração conglobada, sopesando os fatos narrados pela imprensa, há de se concluir que a proposta dos representantes comerciais possivelmente se amolda à conduta descrita no §1º do artigo 154-A, CP, embora a falta de notícias de que o programa tenha sido utilizado em terras brasileiras elimine, por ora, a condição de procedibilidade para a ação penal.

Diante da conclusão de que a oferta do software pode ser subsumível ao tipo formal, resta questionar se os servidores públicos abordados pelos revendedores têm o dever de levar o fato ao conhecimento da autoridade competente. Para esse raciocínio hipotético, considerar-se-á que o *software* foi ofertado para membros do Ministério Público Federal (MPF), embora deva-se destacar que, independentemente da contestada veracidade, os chats apresentados em petição ao STF são provas ilícitas que não podem compor uma acusação criminal.

Analisando o estatuto dos servidores civis da União (Lei n.º 8.112/90), encontram-se duas disposições pertinentes. A primeira, no artigo 116, VI, diz que é dever do servidor *"levar as irregularidades de que tiver ciência em razão do cargo ao conhecimento da autoridade superior ou, quando houver suspeita de envolvimento desta, ao conhecimento de outra autoridade competente para apuração"*. Somado a isso, o artigo 126-A estimula o servidor a dar ciência à autoridade competente de informação, conhecida em decorrência do exercício do cargo, que suspeite indicar a prática de crimes.

Para a carreira do Ministério Público, o dever é ainda mais direto. Diz o artigo 43, VIII, da Lei Orgânica, que deve o Parquet *"adotar, nos limites de suas atribuições, as providências cabíveis em face da irregularidade de que tenha conhecimento ou que ocorra nos serviços a seu cargo"*. Dito dever é coerente com os princípios constitucionais que regem a Administração Pública, em especial a moralidade e o zelo a atos probos.

No âmbito penal, há duas disposições aplicáveis ao servidor que toma conhecimento, no exercício de suas funções, de infração penal praticada por particular. A primeira é o artigo 66, I, da Lei de Contravenções, que pune o servidor que deixa de comunicar à autoridade competente *"crime de ação pública, de que teve conhecimento no exercício de função pública, desde que a ação penal não dependa de representação"*. Vê-se que, para o presente exercício, a contravenção seria inaplicável, já que o crime do §1º do artigo 154-A é condicionado a representação.

O segundo crime é a prevaricação. Segundo o artigo 319, do CP, prevarica o servidor que deixa de praticar, indevidamente, ato de ofício, para satisfazer interesse ou sentimento pessoal. Trata-se da prevaricação omissiva, na qual o servidor abstém-se de praticar dever funcional indicado em lei, que deveria fazê-lo em razão de sua atribuição. Dito arbítrio omissivo carece do elemento subjetivo especial, ou seja, depende que o móvel da ação seja a satisfação de um interesse pessoal, pretensão, ambição ou anseio do agente.

2023 - www.conjur.com.br - Todos os direitos reservados.

Frente ao tipo penal descrito, caso os chats obtidos pela operação "spoofing" correspondam à realidade, é possível ruminar se a conduta dos procuradores da força-tarefa "lava jato" flerta com o crime de prevaricação.

Prosseguindo com a cogitação, é de se exigir que Parquets especializados em Direito Penal saibam que não existe lei ou precedente judicial permitindo o uso de *softwares* espiões no processo penal. Também é exigível que profissionais desse calibre conheçam o Código Penal. Portanto, salvo tenham comunicado formalmente o que lhes foi apresentado ao superior hierárquico ou a autoridade policial competente, é possível que a omissão do dever funcional seja caracterizada. Somado ao comportamento omissivo, há elementos nos supostos chats de que a compra do Pegasus fazia parte do projeto de criação de uma espécie de *bunker* tecnológico, capaz de facilitar as investigações levadas à cabo pela "lava jato" e, por conseguinte, trazer prestígio à força-tarefa e aos procuradores. Logo, manter o conhecimento da proposta restrito ao grupo poderia satisfazer as ambições pessoais dos servidores.

É preciso pontuar, que diante da falta de informações sobre o uso do Pegasus em terras brasileiras, ainda que os Parquets tivessem adotado as medidas cabíveis frente ao potencial fato criminoso, é provável que o inquérito policial sequer fosse instaurado, já que em diligência preliminar, não se encontraria vítima apta a satisfazer o requisito do artigo 5º, II, do Código de Processo Penal. Ainda assim, não parece que uma reflexão interna dos procuradores sobre a condição especial da ação elimine o dever de, ao menos, formalizar as razões pelas quais o fato típico não foi comunicado ao Estado. Parece claro que no curso de um inquérito civil o procurador que se deparara com documentos que comprovam a prática do crime de estelionato deve extrair cópias e remetê-las à autoridade competente, mesmo que o crime seja condicionado à representação.

Para mais, ainda que a omissão em comunicar a oferta do Pegasus não se adeque a qualquer conduta típica, é possível afirmar que, ao deixar de praticar um dever inerente à função, os servidores omitiram-se a ponto de violar os deveres de honestidade, imparcialidade, legalidade, e lealdade às instituições. Portanto, parece viável discutir a prática de ato de improbidade administrativa do artigo 11, *caput* e inciso II, da Lei nº 8.429/92.

Em conclusão, independentemente da concordância sobre o potencial caráter típico da omissão, os argumentos ora apresentados sinalizam que, ao compreenderem o funcionamento do *software* ofertado, os servidores públicos abordados pelos representantes da NSO Group têm o provável dever de tomar as ações adequadas em face da proposta, seja levando o fato ao conhecimento da autoridade competente ou adotando as providências cabíveis para apurar eventual prática do crime do §1º do artigo 154-A do Código Penal.

Caso o raciocínio esteja correto, dito dever perdurará até que sobrevenha norma autorizativa sobre o tema, pois, em especial após o escândalo revelado pelo consórcio jornalístico, tornou-se público e notório que o Pegasus não é uma ferramenta de inteligência, mas sim uma arma informática.

[1] HC 315.220/RS e RHC 67.379/RN.

2023 - www.conjur.com.br - Todos os direitos reservados.

[2] STJ, Resp 1806792/SP e HC 99.735/SC.

[3] D'AVILA, Fabio Roberto; SANTOS, Daniel Leonhardt. Direito Penal e Criminalidade Informática: Breves aproximações dogmáticas. Revista Duc In Altum Cadernos de Direito, vol. 8, n. 15, p. 89-115, mai.-ago. 2016. p. 108.

Date Created
06/08/2021

2023 - www.conjur.com.br - Todos os direitos reservados.