Opinião: por que dados obtidos com hackers devem ser preservados

Na quarta-feira (24/7), a Polícia Federal anunciou a deflagração da fase ostensiva da denominada operação *spoofing*, que prendeu quatro pessoas acusadas de obtenção ilegal de informações extraídas do aplicativo Telegram de diversas autoridades públicas, entre elas, supostamente, o procurador da República Deltan Dallagnol e o ministro da Justiça, Sergio Moro. Horas depois, a imprensa anunciou que um dos acusados teria assumido ser a fonte anônima do site *The Intercept Brasil*, a quem teria enviado voluntariamente os dados obtidos.

Em meio a uma nuvem de informações e desinformações, anunciou-se na imprensa que a fragilidade do aplicativo Telegram teria sido utilizada para a obtenção ilegal de informação de centenas de alvos, entre os quais desembargadores federais, ministros do Superior Tribunal de Justiça e, inclusive, do atual presidente da República.

No dia seguinte, o ministro da Justiça teria ligado para autoridades que tiveram suas contas acessadas ilegalmente pelos acusados na operação. Segundo reportagem do *UOL*, o presidente o STJ, ministro João Otávio Noronha, confirmou o recebimento de uma dessas ligações, na qual foi cientificado de que as mensagens acessadas pelos supostos *hackers* seriam destruídas.

Um acalento atípico sob vários aspectos.

Em primeiro lugar, tratando-se de inquérito que corre em segredo de Justiça, ninguém, senão as autoridades policiais envolvidas, os membros do Ministério Público Federal, o juízo competente e os advogados dos acusados, poderia ter acesso às informações amealhadas durante as investigações. Nem mesmo o ministro da Justiça.

Em segundo lugar, não cabe à autoridade policial — muito menos ao ministro da Justiça — a decisão sobre a destinação dos elementos de informação arrecadados durante o cumprimento de medidas cautelares de obtenção de prova, como buscas e apreensão, interceptações telefônicas e telemáticas, quebras de sigilo bancário, entre outras. Como adiantou o ministro Marco Aurélio, do Supremo Tribunal Federal, somente o magistrado responsável pela autorização da arrecadação dos elementos probatórios pode decidir sobre sua destinação, seja ela a sua preservação, seu acautelamento ou sua destruição.

A afirmação do ministro da Justiça restou também confrontada por nota oficial da Polícia Federal publicada na quinta-feira (25/7), na qual se consignou que "caberá à justiça, em momento oportuno, definir o destino do material, sendo a destruição uma das opções".

Na mesma nota, contudo, a Comunicação Social da Polícia Federal afirmou que a operação *spoofing* não tem como objeto a análise das mensagens supostamente subtraídas de celulares invadidos. O órgão policial, portanto, já insinua que não deve periciar as informações arrecadadas com os supostos criminosos, devendo cingir-se ao aspecto formal da obtenção de mencionadas mensagens.

Não é essa a prática, no entanto, que se observa na Polícia Federal e na jurisprudência das cortes superiores segundo a chamada doutrina da "serendipidade" ou do "encontro fortuito de provas".

A origem da palavra serendipismo é inglesa e foi criada pelo escritor britânico Horace Walpole em 1754, a partir de um conto persa infantil. A história conta as peripécias de três príncipes do Ceilão que viviam fazendo descobertas inesperadas, cujos resultados eles não estavam procurando realmente.

Muito comum no caso de interceptações telefônicas, a teoria da serendipidade reconhece que um prova obtida em uma escuta telefônica, por exemplo, ainda que não relacionada diretamente com o crime inicialmente apurado, não configura prova ilícita e pode servir de propulsor para a persecução de novos processos.

Segundo a teoria mais restritiva, defendida por Luiz Flávio Gomes e Silvio Maciel[1], a legalidade da prova fortuita estaria condicionada à conexão entre os fatos investigados ou entre os alvos da investigação. Sendo assim, caso se encontrassem partícipes novos do mesmo fato que deu ensejo à medida cautelar ou fatos novos dos alvos já investigados, possível a utilização da prova. No entanto, fatos novos relacionados à terceiros, ainda que indiciários da prática de delitos, não materializariam provas lícitas. Tal construção é conhecida como teoria da serendipidade de primeiro grau.

Posicionamento oposto foi cristalizado pelo Superior Tribunal de Justiça, com particular destaque para o julgado de lavra da Corte Especial de relatoria do ministro João Otávio Noronha (STJ – APn 690-TO), na qual se consolidou que "a prova é admitida para pessoas ou crimes diversos daquele originalmente perseguido, ainda que não conexos ou continentes, desde que a interceptação seja legal".

A serendipidade não se aplica somente aos casos de interceptação telefônica. Na lição de Geraldo Prado: "Também na busca e apreensão poderá ocorrer encontro fortuito. Na execução de uma ordem judicial para a apreensão de uma arma o executor da medida poderá encontrar um quilo de cocaína ou o cadáver insepulto de vítima de homicídio. Por evidente que haverá de apreender a droga e tomar as devidas providências em relação ao cadáver"[2].

Com efeito, munidos de um mandado de busca e apreensão expedido por autoridade competente, que visava angariar elementos a respeito de uma suposta invasão ao aplicativo de troca de mensagens de diversas autoridades, os cumpridores da ordem arrecadaram o conjunto dos vestígios materiais resultantes da prática, em tese, criminosa. Assim, o material apreendido constitui corpo de delito e tem que ser submetido a perícia.

Afinal, não se destrói uma droga apreendida sem laudo, não se enterra um cadáver sem laudo e, pelas mesmas e exatas razões, não se descarta um computador usado para hackear alguém sem laudo. É o que dispõe o artigo 158, do Código de Processo Penal.

A ordem de busca foi legalmente exarada e não há dúvida de que a apreensão do material passou a ser lícita e permitida. O exame do material apreendido deve passar, inexoravelmente, pela análise de seu conteúdo. Até para se provar que aquelas trocas de mensagem foram mesmo extraídas do Telegram, que não houve adulteração e que foram extraídas do aplicativo em sua integralidade.

Mais do que isso. Segundo determinados precedentes, não só a autoridade policial poderia, como deveria investigar os fatos fortuitamente levados a seu conhecimento no bojo de uma investigação. Para além da mera possibilidade do uso de prova, em julgamento de sua relatoria, o ministro Jorge Mussi

(STJ – HC 189.735) consignou que, quando deparado com elementos que denotem a prática de novos ilícitos, "há dever funcional apurá-los, ainda que não possuam liame algum com os delitos cuja suspeita originariamente ensejou a quebra do sigilo telefônico".

Pois bem. Se ao examinar as mensagens para verificar sua higidez, a polícia fortuitamente identificar elementos de relevo jurídico-criminal, evidente que não só pode como deve investigar, segundo a jurisprudência hoje vigente.

Exemplificativamente: uma joalheria é assaltada e o dono do comércio noticia o crime na delegacia. Durante a investigação do roubo, em busca e apreensão, descobre-se o paradeiro das supostas joias em poder dos criminosos. Elas serão submetidas a perícia para ver se são as mesmas que foram roubadas da joalheria. Se no decorrer da perícia se percebe que metade destas joias são de aço, e não de ouro, o dono da joalheria não só pode como deve responder pela defraudação cometida contra seus clientes.

Tal qual as mensagens supostamente hackeadas, o "corpo de delito" foi encontrado em poder de criminosos, que injustamente subtraíram a posse dos bens de seu proprietário. Mas, ao analisá-los, descobriu-se, acidentalmente, ato criminoso diverso, desta feita perpetrado pela vítima do roubo contra os consumidores, que há anos vinham comprando gato por lebre. Evidente que o fato de o joalheiro ter sido vítima de roubo não dá a ele imunidade sobre atos ilícitos descobertos acidentalmente, em seu desfavor.

Retornando ao caso da operação *spoofing*, nos moldes do artigo 158 do Código de Processo Penal, as mensagens encontradas em poder dos supostos hackers devem ser submetidas à perícia forense, para a aferição do *modus operandi* utilizado para sua extração, bem como para análise sobre a integridade dos dados obtidos, supostamente, de maneira ilegal. E segundo a corrente jurisprudencial predominante nas cortes superiores, caso se verifiquem, acidentalmente, indícios de irregularidades ou de práticas delitivas no teor de tais mensagens, devem ser encaminhadas aos órgãos competentes para investigação.

Portanto, seguindo os precedentes pretorianos sobre a teoria da serendipidade, os dados arrecadados na operação deveriam ser preservadas, mesmo sob a perspectiva judicial, ante a possibilidade de revelação de condutas relevantes do ponto de vista jurídico-penal, seja para o reconhecimento de responsabilidade criminal, seja para seu afastamento.

---

[1] *Interceptação Telefônica*. RT, 2011. P. 108.
[2] *Limite às Interceptações Telefônicas e Jurisprudências do Superior Tribunal de Justiça*. Lumem Juris, 2006. P. 60.

Date Created
27/07/2019