MJ defende software intrusivo nacional contra estrangeiros

11/06/2024

O Ministério da Justiça e Segurança Pública, a Polícia Federal e a Agência Nacional de Telecomunicações (Anatel) defenderam nesta terça-feira (11/6) o desenvolvimento e a regulamentação de instrumentos nacionais de vigilância como forma de desestimular a aquisição de programas estrangeiros e privados de espionagem.

Andressa Anholete/SCO/STF

Audiência no Supremo discute contratação de softwares intrusivos

Representantes dos três órgãos participaram da audiência pública promovida pelo Supremo Tribunal Federal para discutir contratos públicos de aquisição de sistemas espiões e de extração de dados de aparelhos. A audiência foi convocada pelo ministro Cristiano Zanin, com dois dias de duração. O tema chegou ao tribunal por meio de uma ação da Procuradoria-Geral da República.

Zanin justificou a necessidade de uma audiência porque o tema envolve a "suposta violação sistemática de preceitos fundamentais no uso de tais equipamentos para monitorar magistrados, advogados, jornalistas, políticos e defensores de direitos humanos".

Vulnerabilidades

Consultor jurídico do Ministério da Justiça, **Victor Epitácio Cravo Teixeira** afirmou que tecnologias para a suspensão de sigilo devem integrar os sistemas das plataformas das prestadoras de serviços de telecomunicação. Segundo ele, no entanto, o acesso a informações deve ser sempre excepcional, aplicado somente em casos de investigação criminal e instrução de processos penais.

Para Teixeira, não se pode permitir que empresas privadas acessem informações a partir da exploração de vulnerabilidades da rede pública de telecomunicações.

Ele citou como exemplos os softwares Pegasus, que explora os sistemas operacionais de dispositivos móveis, dando acesso às funcionalidades de equipamentos como celulares e computadores, e FirstMile, que explora vulnerabilidades da rede de telecomunicações para obter dados de tráfego.

"As ferramentas de intrusão são fornecidas por empresas privadas ao arrepio da legislação que disciplina a suspensão legítima do sigilo das comunicações, sem apoio das prestadoras de serviços de telecomunicação, e exploram vulnerabilidades da rede pública e dos sistemas operacionais dos aparelhos celulares", disse ele.

Rodrigo Morais Fernandes, diretor de inteligência da Polícia Federal, argumentou em sentido semelhante. Segundo ele, a legislação atual disciplina plenamente o tema ao prever a possibilidade de interceptações e acesso a dados sigilosos no curso de investigações criminais ou instruções de processos penais, mediante autorização prévia.

Ele disse que a PF está em tratativas com a Anatel para tentar regulamentar o uso de ferramentas de geolocalização e acesso remoto a dispositivos. Segundo Fernandes, o objetivo é facilitar investigações, sem que se precise explorar vulnerabilidades da rede pública de telecomunicações.

"A funcionalidade do Pegasus é imprescindível, sim, para fins de segurança pública. Posso citar várias situações de como o emprego de uma ferramenta como essa seria fundamental para a identificação de organizações criminosas. (…) Temos tomado cuidado e tido tratativas com a Anatel no sentido de regulamentar isso."

Da forma como o uso de softwares espiões se dá hoje, afirmou o diretor da PF, é possível afirmar, ao menos em tese, que a infraestrutura brasileira pode ser usada para a espionagem internacional.

“A gravidade é tão grande que pode se dizer, em tese, que a infraestrutura brasileira pode estar servindo para a espionagem internacional. É muito fácil. Eu consigo, por meio desses aparelhos, interceptar qualquer telefone no mundo inteiro. Em situações de guerra, um alvo qualquer pode estar sendo monitorado por meio da rede de telefonia brasileira.”

Correção de problemas

Gustavo Santana Borges, da Anatel, também afirmou que o ideal é o desenvolvimento de ferramentas próprias, a serem usadas exclusivamente na persecução penal, de uma forma que os dados não possam ser acessados por meio da exploração de vulnerabilidades.

Segundo ele, ferramentas próprias para extração de dados e localização devem ser desenvolvidas ao mesmo tempo em que as vulnerabilidades são corrigidas. Caso contrário, a infraestrutura continuará aberta a ataques por meio de softwares privados.

“O uso de tais ferramentas estrangeiras poderia ser substituída por uma ferramenta que seja compatível, regulamentada, nacional, produzida com igual qualidade no sentido de provimento de dados, mas que não se alimente de vulnerabilidades, que seja a produção de dados sem essa exploração de dados de vulnerabilidades”, defendeu Borges.

“Uma vez existente uma alternativa para os órgãos competentes, *(deve haver esforço)* para a correção de vulnerabilidades. Porque os softwares, mesmo proibidos no país, serão comercializados em outros países. Então é preciso manter um cuidado para que as vulnerabilidades sejam estancadas.”

Entidade identificou 209 contratos

Se nesta terça as exposições durante a audiência no STF foram feitas por representantes de órgãos públicos, na segunda falaram principalmente entidades da sociedade civil e institutos que pesquisam softwares intrusivos.

As discussões no primeiro dia da audiência se centraram especialmente em um estudo feito em 2022 pelo Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.REC), que identificou 209 contratos para contratação de softwares de hacking, treinamento de funcionários, termos aditivos e atualização de softwares. O levantamento compreende o período de 2015 a 2021.

Segundo o estudo, há contratos do gênero em todos os estados brasileiros, feitos por diferentes órgãos. O pico ocorreu em 2020, quando houve um gasto de R$ 55 milhões com os softwares. Em 2019, o gasto havia sido de R$ 7 milhões, valor semelhante aos dos anos anteriores.

De acordo com **Raquel Saraiva**, presidente e fundadora do IP.REC, até órgãos que não têm competência investigativa, como Secretarias de Fazenda, adquiriram ferramentas intrusivas.

“Hoje, ferramentas de extração de dados em massa dominam secretarias estaduais, órgãos estaduais e estão presentes em todos os estados federativos, inclusive órgãos que, a princípio, não teriam competência investigativa. Entre essas ferramentas, destacamos o avanço da empresa israelense Cellebrite, que desenvolve um software responsável por extração de dados em massa.”

A maior parte dos contratos envolve programas de extração de dados de dispositivos. Nesse caso, é preciso ter o equipamento físico para retirar as informações.

No entanto, nesta terça, o representante da PF admitiu que a Polícia Civil em pelo menos um estado utiliza ou utilizou a ferramenta FirstMile, que se vale da exploração de vulnerabilidades no sistema de telecomunicações, para providenciar dados geográficos.

“Recebi o telefonema do delegado da Polícia Civil de um estado grande do país me indagando, dizendo a verdade de que ele cuida de casos sensíveis de sequestro e faz uso dessa ferramenta de geolocalização e que essa ferramenta é imprescindível”, disse Rodrigo Fernandes.

O FirstMile usa uma vulnerabilidade que permite saber a posição de uma pessoa a partir da comunicação de um aparelho com antenas de telecomunicação. O software ficou conhecido no caso batizado de “Abin Paralela”, em que a agência de inteligência utilizou a ferramenta para monitorar jornalistas, autoridades e ministros do Supremo.

Contratação generalizada

Segundo o levantamento do IP-REC, os Ministérios Públicos de 18 estados contrataram ou renovaram a contratação de softwares, em sua maioria de extração de dados. Contrataram ou renovaram serviços desse tipo os MPs de Rio Grande do Sul; Santa Catarina; Mato Grosso; Mato Grosso do Sul; Goiás, Distrito Federal; Rio de Janeiro; São Paulo; Minas Gerais; Rio Grande do Norte; Piauí; Pernambuco; Paraíba; Bahia; Alagoas; Roraima; Amapá; e Acre.

A entidade mostrou preocupação em especial com o Projeto Excel, criado pelo Ministério da Justiça e Segurança Pública do ex-presidente Jair Bolsonaro, que tinha como objetivo fornecer equipamentos de extração de dados em massa para secretarias estaduais. Em troca, as secretarias enviavam os dados ao governo federal.

"Não temos como precisar se as empresas têm acesso aos dados. Aí é que reside o perigo. Por não haver transparência. O que levanta questionamentos sobre como estão sendo usadas essas ferramentas", disse Raquel Saraiva.

Monitoramento e coleta de dados

Na segunda, as entidades também demonstraram preocupação com o risco de difusão de softwares ainda mais invasivos, como o Pegasus, que tem a capacidade de coletar e compartilhar, ao vivo, informações sonoras, visuais, geográficas e de uso, entre outras.

Segundo **Pedro José Nasser Saliba**, da Data Privacy Brasil, há ainda softwares que utilizam a invasão de redes públicas ou privadas. Um dos exemplos é a FirstMile, que é capaz de monitorar a movimentação de até dez mil alvos. Também existem softwares capazes de ativar microfones remotamente e identificar a localização de alvos.

De acordo com Saliba, foram softwares desse tipo os utilizados durante o governo de Bolsonaro para monitorar autoridades, jornalistas e até ministros do Supremo Tribunal Federal pela Abin.

"O que nos chamou a atenção é que ferramentas altamente intrusivas estavam sendo contratadas tanto pelo Exército quanto por secretarias estaduais de segurança."

Sem regulamentação

A Ordem dos Advogados do Brasil apontou a necessidade de regulamentação do tema. Segundo a entidade, as legislações que existem sobre o assunto são insuficientes. Enquanto não houver norma específica, defendeu a OAB, será necessário considerar ilegais os programas espiões.

"Não temos uma legislação aplicável ao caso, fazendo-se a necessidade de uma legislação sobre os softwares, que fixe seus limites e que preveja alternativas adequadas de proteção contra formas de abuso. Sendo possível (deve ser), de antemão, considerada ilegal a utilização desses programas por autoridades policias ou qualquer outro ente", disse **Alisson Alexsandro Possa**, da Comissão de Direito Digital do Conselho Federal da OAB.

Laura Schertel Mendes, que também representou a entidade, afirmou que, se por um lado há o aumento da eficiência das investigações utilizando softwares, é certo que, de outro lado, os sistemas têm um potencial invasivo muito grande.

"Estamos a falar de softwares espiões que se infiltram clandestinamente nos sistemas de informações, como computadores e celulares, permitindo o acesso a todas as informações armazenadas no aparelho, bem como ações produzidas em tempo real, como mensagens e e-mails digitados, mas não enviados", afirmou ela.

Audiência pública

A audiência no Supremo conta com a exposição de mais de 30 representantes de órgãos públicos, da sociedade civil e de entidades ligadas às universidades.

A discussão sobre a regulamentação dos softwares espiões chegou ao Supremo por meio de uma ação direta de inconstitucionalidade por omissão (ADO), mas Zanin a converteu em arguição de descumprimento de preceito fundamental (ADPF) por considerá-la a via processual mais adequada.

Na ação, a PGR afirma que, apesar de avanços na legislação para proteger a intimidade, a vida privada e a inviolabilidade do sigilo das comunicações pessoais, ainda não há uma regulamentação sobre programas de infiltração virtual remota.

Com isso, a PGR pediu que o Supremo fixe prazo razoável para que o Congresso Nacional edite norma para regulamentar a matéria, bem como estabeleça regras provisórias para proteger os direitos fundamentais à intimidade, à privacidade e à inviolabilidade do sigilo das comunicações pessoais e de dados até a aprovação de lei sobre o assunto.

ADPF 1.143

Fonte: https://conjur.jumps.com.br/2024-jun-11/ministerio-defende-software-intrusivo-nacional-para-inibir-sistemas-estrangeiros/