Questão urgente do uso de softwares espiões pelo poder público na ADPF 1.143

10/06/2024

Em tempos nos quais a privacidade está cada vez mais ameaçada pela tecnologia digital, emerge uma questão crucial: o Estado pode usar softwares espiões sem violar os direitos humanos? A audiência pública marcada pelo STF (Supremo Tribunal Federal) para debater o uso de softwares espiões pelo poder público lança luz sobre esse debate urgente. Neste artigo, examino os riscos da utilização indiscriminada dessas ferramentas, a confusão entre inteligência e segurança pública, a necessidade de regulamentação específica, e a importância de proteger nossos dados pessoais.

Silvabom/Freepik

O Supremo marcou para hoje e amanhã (11/6) uma audiência pública a respeito do uso de softwares espiões pelo poder público, um marco significativo para os interesses da sociedade brasileira no contexto das tecnologias digitais. A ideia do evento consiste em ouvir diversas vozes da sociedade civil, do poder público e do setor privado, ressaltando a importância de se discutir a utilização de programas de monitoramento secreto por órgãos e agentes públicos. A ação de controle constitucional em foco, a ADPF 1.143, por si mesma, evidencia a necessidade de um debate mais profundo e de uma regulamentação legal nítida sobre o tema.

Nos últimos anos, temos assistido à contratação massiva de ferramentas de espionagem por diversas entidades públicas. O município de Palhoça (SC), por exemplo, investiu aproximadamente R$ 150 mil, enquanto Joaçaba (SC) gastou R$ 200 milhões. Contratos como esses, que totalizam quantias elevadas, são destinados a programas que supostamente solucionariam problemas de segurança pública, mas que, na verdade, estão sendo usados para espionar cidadãos sob o pretexto de segurança.

Esses dados estão disponíveis nos autos da referida ação de controle de constitucionalidade, e se alinham às descobertas do IP.rec, divulgadas em 2022 na publicação *Mercadores da Insegurança*, que desnuda o cenário de bilhões de reais gastos pelos governos estaduais e federal com a contratação de programas espiões para atividades de segurança pública. [1]

A situação evidencia uma confusão perigosa entre atividades de inteligência e de segurança pública. A atividade de inteligência, definida por lei no Brasil, trata da obtenção, análise e disseminação de informações relevantes para a defesa nacional e a segurança do Estado. No entanto, no contexto da segurança pública, e até subvertendo seus objetivos, o uso dessas ferramentas tem ocorrido de modo desvirtuado, aplicadas contra a própria população, transformando qualquer cidadão comum em alvo de vigilância estatal.

A ausência de regulamentação específica agrava ainda mais o cenário. Projetos de Lei como o 402 de 2024, do senador Alessandro Vieira, e o PL 4.510 de 2020, do deputado Carlos Zarattini, entre tantos outros, visam estabelecer limites e procedimentos claros para o uso dessas ferramentas ao fixar limites de legalidade para as atividades de inteligência.

Mas eles enfrentam resistência no Congresso. Em paraleleo a projetos específicos, além da tormentosa criação de uma LGPD penal, há também a reformulação do Código de Processo Penal, por meio do PL 8.045, de 2010. O CPP é imenso, exige técnica legislativa, já envolveu um grupo de trabalho que lidou com temas como coleta de prova digital e cadeia de custódia, de modo a sistematizar garantias individuais que estabeleçam um ambiente jurídico protetivo, adequado à perspectiva da sociedade da informação.

Hoje, celular, televisão, carro, computador, relógios, alto falantes, câmeras, lâmpadas e vários dispositivos inteligentes na casa de cada pessoa permitem identificar mais dados e informações do que ela sabe sobre ela mesma. Em meio a essa era de ouro da vigilância, a falta de uma legislação específica tem sido explorada pelo Estado, em nome da segurança, para cometer violações sistemáticas de nossos direitos, reduzindo garantias processuais penais e, paradoxalmente, promovendo um ambiente de insegurança jurídica.

Em vez de exigir das empresas privadas uma adequação estrita aos ditames constitucionais e legais vigentes, que já podem oferecer proteções jurídicas mínimas contra o vasto potencial digital, o poder público tem sido o primeiro a dar mau exemplo. E, pior, gasta muito dinheiro com essa estratégia nociva, em detrimento de, por exemplo, valorizar seus recursos humanos e capacitar adequadamente agentes de segurança pública.

A proteção de dados pessoais é um direito fundamental assegurado pela Constituição e pela Lei Geral de Proteção de Dados (LGPD). No entanto, o uso indiscriminado de softwares espiões pelo poder público ameaça e viola essa garantia. A prática de *hacking governamental*, que envolve a intrusão e manipulação de dispositivos pessoais, deve ser severamente regulamentada para evitar abusos e garantir a segurança dos sistemas e dados dos cidadãos.

Quando ela pode ser utilizada?

E, na hipótese de haver situações em que ela seria autorizada, quais os parâmetros para avaliar a regularidade de seu uso? Essas perguntas são hoje respondidas caso a caso, por cada autoridade em ação, e longe de qualquer escrutínio seja pelo próprio poder público, seja pela sociedade como um todo.

Agravando esse contexto, a recente adesão do Brasil à Convenção de Budapeste sobre cibercrime implica a necessidade de uma regulamentação harmoniosa do ponto de vista internacional para a produção de provas digitais, e ressalta a urgência de se estabelecerem normas legais objetivas e eficazes no âmbito nacional, que sirvam como nosso dever de casa.

O Iris (Instituto de Referência em Internet e Sociedade), em uma revisão sistemática de artigos científicos sobre hacking governamental, concluiu ser importante debater a legalidade, proporcionalidade e transparência dessas práticas, bem como a necessidade de controle público sobre o uso de tecnologias de vigilância. [2]

É crucial compreender que a ameaça dos programas espiões não é apenas uma questão tecnológica (restrita a especialistas) ou ideológica (restrita a um espectro de esquerda), mas uma temática de interesse nacional, que pode envolver situações cotidianas.

Para destacar essa importância, imagine um cenário no qual um agente de segurança pública, de boa-fé, utilizando intencionalmente um software espião de origem estrangeira para otimizar suas atividades de investigação, acidentalmente aciona uma ferramenta do programa e envia dados sensíveis para um destinatário desconhecido, ou abre uma porta para permitir o acesso indevido a informações críticas sobre operações policiais.

Esta situação, além de comprometer a segurança do agente, levanta sérias questões sobre a segurança nacional e a confiabilidade de softwares estrangeiros em atividades de interesse nacional.

Como se poderia confiar que um programa potente como o famoso Pegasus, produzido pela empresa israelense NSO Group, vá operar sempre de acordo com o sigilo dos dados presentes em equipamentos e sistemas das forças de segurança pública do Brasil? Não me parece fazer sentido esperar que um programa espião opere de forma íntegra, em especial quando seu código não é aberto, e não se pode avaliar com certeza os seus mecanismos de funcionamento. É um lembrete claro de que, mesmo com intenções legítimas, a falta de controle e conhecimento sobre as ferramentas tecnológicas pode levar a graves consequências.

A propósito, o programa Pegasus tem esse nome em uma referência ao cavalo de Troia. Na mitologia grega, durante a Guerra de Troia, os gregos ofereceram aos troianos um grande cavalo de madeira como presente de rendição. À noite, soldados gregos escondidos dentro do cavalo saíram e abriram os portões da cidade, permitindo que o exército grego invadisse e conquistasse a cidade.

Há décadas alguns vírus de computador são conhecidos como cavalos de troia, pois se passam por programas inofensivos para enganar a pessoa e infectar o seu dispositivo eletrônico. Mas normalmente eles exigem que a pessoa aceite o “presente de grego”.

Daí que o nome Pegasus foi, então, pensado para aludir a um cavalo de troia voador, capaz de infectar dispositivos sem contato e “pelo ar”, apenas explorando vulnerabilidades existentes, sem a necessidade de qualquer comportamento da vítima.

Constitucionalismo digital

O prognóstico de uma permeabilidade do STF para argumentos diversos sobre o tema é um passo importante, mas ainda insuficiente. É imperativo que o Supremo reafirme os direitos fundamentais dos cidadãos e inicie um movimento de constitucionalismo digital que proteja os direitos humanos na era da informação. A criação de uma legislação robusta e específica, que contemple a necessidade de ordem judicial para o uso de softwares espiões e estabeleça limites claros para sua utilização, é essencial para preservar a democracia e a liberdade no Brasil.

Em conclusão, a utilização de programas espiões pelo poder público, sem a devida regulamentação e controle, representa uma grave ameaça aos direitos fundamentais dos

cidadãos. É necessário que o Estado, enquanto guardião da justiça e da legalidade, adote uma postura estritamente legalista e promova a segurança pública sem violar os direitos humanos. Somente assim poderemos construir uma sociedade mais justa, segura e democrática.

* *Este artigo deriva da roda de conversa "O uso de software espião na persecução penal: problemas e desafios", promovida pelo IBCCrim (Instituto Brasileiro de Ciências Criminais), da qual participei ao lado de Pedro Amaral, do IP.rec (Instituto de Pesquisa em Direito e Tecnologia do Recife), e de Maíra Costa Fernandes, coordenadora do Depto. de Novas Tecnologias do IBCCrim, sob a apresentação de Renato Vieira, presidente do IBCCrim, disponível na íntegra aqui.*

_____

[1] AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César M.; RAMIRO, André (coord.). Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/publicacoes/mercadores-da-inseguranca conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 06 jun. 2022.

[2] DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. Hacking Governamental: uma revisão sistemática. Belo Horizonte: Instituto de Referência em Internet e Sociedade, fevereiro de 2023. Disponível em: https://irisbh.com.br/publicacoes/hacking-governamental-uma-revisao-sistematica/. Acesso em:

06 Jun. 2023.

Fonte: https://conjur.jumps.com.br/2024-jun-10/questao-urgente-do-uso-de-softwares-espioes-pelo-poder-publico-na-adpf-1-143/