Riscos do uso de softwares espiões em atividades de persecução criminal e de inteligência

12/06/2024

No últimos dias 10 e 11, o Supremo Tribunal Federal fez audiência pública no âmbito da Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 1.143, ajuizada pela Procuradoria-Geral da República, com pedido para que o Congresso seja instado a regular o uso de *softwares* espiões em atividades de persecução criminal e de inteligência.

Silvabom/Freepik

A ação foi proposta originalmente como Ação Direta de Inconstitucionalidade por Omissão (ADO), em dezembro de 2023, pouco tempo após ser publicizada operação da Polícia Federal que prendeu dois servidores da Abin (Agência Brasileira de Inteligência) e afastou outros quatro, investigados por terem supostamente feito uso ilegal do *software FirstMile*, adquirido sigilosamente, segundo se tem notícia, por R$ 5,7 milhões, da empresa israelense *Cognyte*, em 2018.

O *FirstMile* é um programa malicioso que permite rastrear a localização de pessoas em tempo real, a partir dos respectivos números de celulares. Segundo apurações da Polícia Federal, o *spyware* teria sido utilizado pela Abin entre dezembro de 2018 e maio de 2021, para monitorar cerca de 1.800 pessoas, entre elas jornalistas, políticos e adversários do ex-presidente Jair Bolsonaro.

Esse fato gravíssimo não é isolado. Ainda em 2023, vieram a público notícias de que, no primeiro semestre de 2019, a PF manteve tratativas com representante da também israelense *NSO Group*, para aquisição do *software* de espionagem Pegasus.

Armas digitais

Spywares como o Pegasus são comparados a armas digitais, porque invadem dispositivos informáticos sem qualquer ação do usuário, permitindo acesso amplo e oculto a dados armazenados, monitoramento de todas as atividades e ganho de controle sobre as funcionalidades do aparelho. À distância, o *software* pode realizar qualquer função: abrir microfone e câmera, visualizar ou apagar arquivos, fotos, contatos, localização, acessar aplicativos e dados bancários.

Não bastasse, o *spyware* pode se autodestruir sem deixar qualquer vestígio no aparelho no qual foi introduzido à distância. Essa potencialidade é particularmente relevante no debate sobre seu uso na persecução penal, pois é impossível assegurar a cadeia de custódia da prova extraída por esse tipo de ferramenta.

O uso indiscriminado de *softwares* maliciosos também preocupa sob o ponto de vista da cibersegurança e da própria soberania nacional. Em regra, essas tecnologias são estrangeiras e comercializadas por empresas privadas que desenvolvem suas atividades de forma opaca, lucrando com a exploração de vulnerabilidades em dispositivos, sistemas e redes de comunicação.

O *hacking* governamental por meio de ferramentas de intrusão e monitoramento remoto suscita questões jurídicas complexas, tamanha é a dificuldade de se compatibilizar formas extremas de vigilância e de controle com a preservação de garantias fundamentais.

As intervenções em direitos acarretadas por programas como o Pegasus são muito mais intensas do que aquelas provocadas por interceptações telemáticas e captações ambientais, não se limitando aos âmbitos de proteção dos direitos à intimidade, à vida privada e ao sigilo das comunicações.

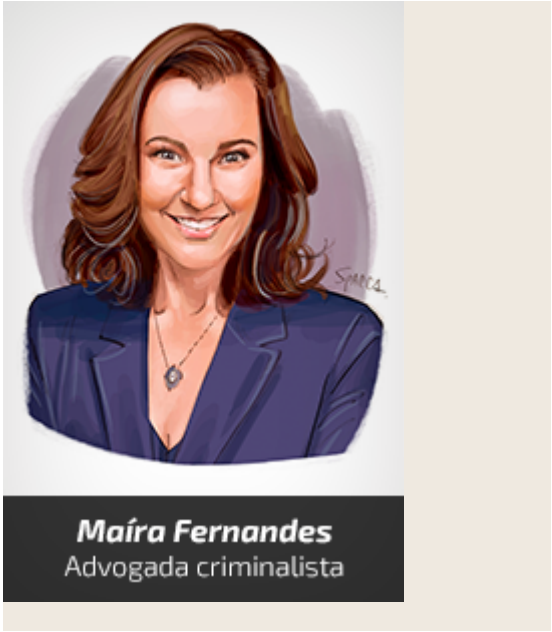
A autodeterminação informativa e as liberdades de expressão, de informação e de associação também sofrem impactos importantes, que podem ser em muito agravados quando essas tecnologias são usadas de forma desvirtuada e abusiva por governos autoritários.

Como revelou em 2021 a investigação *The Pegasus Project*, realizada por jornalistas de diversas nacionalidades sob a coordenação do consórcio *Forbidden Stories*, o *software* Pegasus foi utilizado por governos de mais de 24 países para monitorar advogados, ativistas, jornalistas e opositores — ou seja, para travar "guerra" contra um "inimigo" interno. Uma manifesta violação aos direitos humanos.

No mundo

No mundo, debates relacionados ao tema acontecem há anos, e alguns países como Alemanha, Austrália, Espanha, Estados Unidos, França, Itália e Holanda regulamentaram o uso dessas ferramentas sob condições altamente restritivas, que incluem a observância de "protocolos de busca" bastante rigorosos.

Spacca



No Brasil, diante da constatação de que agentes públicos estariam utilizando programas de intrusão virtual e de monitoramento remoto de aparelhos de comunicação sem respaldo legal, sem autorização judicial prévia ou qualquer tipo de controle *ex post*, o Ministério Público Federal pretende que o Congresso (ou o próprio STF, em caráter provisório) regulamente essa atividade, ao invés de coibi-la.

Se a pretensão for acolhida, direitos fundamentais serão paradoxalmente limitados como resultado de uma ação que foi ajuizada sob a justificativa de protegê-los.

Para além dessa questão, existe uma segunda, igualmente preocupante: se for acolhido o pedido formulado para que o Supremo estabeleça provisoriamente um regime para o uso dessas ferramentas, o Poder Judiciário adentrará um espaço de atuação exclusiva do Poder Legislativo.

A iniciativa do STF de promover a audiência pública dos dias 10 e 11 de junho é louvável e oportuna, em vista das notícias recentes sobre o uso ilegal e ilegítimo dessas tecnologias. No entanto, é o Parlamento, por sua representatividade popular, o espaço institucional adequado para o amadurecimento do debate democrático e para a deliberação sobre o tema.

A análise sobre o impacto de *softwares* espiões em direitos fundamentais demanda extrema prudência do Poder Legislativo. As diversas vozes sobre a questão devem ser também ouvidas no âmbito do Congresso, a fim de que os parlamentares possam decidir se (e quais) intervenções em direitos fundamentais provocadas por essas ferramentas serão admitidas e, em caso positivo, sob quais condições e limites.

Considerando que programas espiões fazem muito mais do que recolher dados e monitorar conversas, uma regulação proporcional deverá ser extremamente restritiva e indicar com clareza e grande detalhamento os procedimentos a serem seguidos pelos agentes do Estado para sua utilização.

É imprescindível, ainda, que sejam estabelecidos mecanismos de notificação dos usuários e de auditabilidade das ferramentas, além de obrigações quanto ao descarte de dados impertinentes e deveres de transparência sobre as atividades que as envolvem o uso de *malware*.

Pouco após o ajuizamento da ADO nº 84, posteriormente convertida na ADPF nº 1.143, foram apresentados os PLs nº 58/2024, de autoria do deputado Alberto Fraga, e nº 402/2024, de autoria do senador Alessandro Vieira, buscando, às pressas e em poucos artigos de lei, preencher o alegado vazio normativo nessa matéria.

Direitos fundamentais

Em que pese uma aparente boa intenção dos parlamentares, de regulamentar a questão para evitar violações à privacidade dos indivíduos, o momento não é de pressa, mas de cautela para que o Poder Legislativo possa, se o caso, editar uma disciplina robusta e comprometida com direitos fundamentais.

Nesse mesmo sentido, é necessário que, antes de avançar na regulação do uso de *spywares*, o Congresso aprove uma disciplina específica para as provas digitais no processo penal e para o tratamento de dados na persecução penal e na segurança pública. Sem que se estabeleça um ambiente normativo adequado de forma prévia, será impossível aprovar um regime para o uso de ferramentas de *hacking* governamental dotado de salvaguardas efetivas.

Nesse ínterim, a conduta de agentes públicos deverá ser pautada pela compreensão de que, na ausência de lei, o uso dessas ferramentas é proibido no Brasil. Qualquer tentativa de aquisição ou uso ilegal de *softwares* espiões, como aqueles tratados na ADPF nº 1.143, deve ser coibida, com firmeza, por todas as instituições governamentais, para a garantia e preservação dos direitos fundamentais e a proteção da soberania de nosso país.

Fonte: https://conjur.jumps.com.br/2024-jun-12/riscos-do-uso-de-softwares-espioes-em-atividades-de-persecucao-criminal-e-de-inteligencia/