MÚLTIPLAS VOZES

O sistema "Pegasus" e a interceptação telemática indevida

O Brasil não pode se tornar um estado de vigilância permanente em que seus cidadãos tenham seus direitos desrespeitados e a sua vida íntima exposta ao arbítrio estatal

José Mariano de Araujo Filho
9 de junho de 2021

MARCELLO CASAL JR/AGÊNCIA BRASIL

Uma permissão de uso do sistema "Pegasus", que permite interceptações telemáticas, seria cedida ao Banco Central, o que causa estranheza, pois a instituição não tem legitimidade para a realização de investigações criminais

Tem sido divulgado por diversos órgãos de imprensa do país o interesse do Ministério da Justiça e da Segurança Pública em adquirir um sistema denominado “Pegasus”, o qual seria utilizado para acesso indevido a equipamentos de telefonia celular e computadores.

Mencionada ferramenta seria desenvolvida e comercializada pela empresa israelense “NSO Group”, inclusive com precedente internacional de uso para interceptação de jornalistas e críticos a governos.

Em sua página na internet (https://www.nsogroup.com/about-us/board-of-directors) a empresa informa que é uma corporação cujo objetivo seria desenvolver a melhor tecnologia da categoria para ajudar as agências governamentais a detectar e prevenir o terrorismo e o crime.

Importante destacarmos, que em outubro de 2019, o “WhatsApp/Facebook” ingressou com uma ação judicial em uma corte da Califórnia, nos Estados Unidos, contra a empresa “NSO Group”. Nessa ação, a acusação foi o desenvolvimento de um “malware” para acessar mensagens de WhatsApp depois de decriptografadas no aparelho dos usuários daquele serviço de mensageria.

Em sua defesa, o “NSO Group” alegou que a responsabilidade pelo uso do seu software é dos clientes, nesse caso, Estados nacionais que realizaram a aquisição de sua solução.

O mencionado “malware” seria na realidade o "Pegasus", desenvolvido, inicialmente, para autoridades governamentais explorarem aparelhos de suspeitos de terrorismo e de outros crimes.

Numa busca rápida na internet, é possível obter-se um “folder” que traz maiores informações sobre o mencionado sistema “Pegasus” (https://www.documentcloud.org/documents/4599753-NSO-Pegasus.html):

“Pegasus é uma solução de inteligência cibernética líder mundial que permite que as agências de aplicação da lei e de inteligência extraiam inteligência valiosa de qualquer dispositivo móvel, de forma remota e secreta. Esta solução inovadora foi desenvolvida por veteranos de agências de inteligência de elite para fornecer aos governos uma maneira de lidar com os novos desafios de interceptação de comunicações no altamente dinâmico campo de batalha cibernético de hoje. Capturando novos tipos de informações de dispositivos móveis, a Pegasus preenche uma lacuna tecnológica substancial para fornecer a inteligência mais precisa e completa para suas operações de segurança.”

Uma análise superficial do “folder” indicado permite aferir que o sistema “Pegasus” é efetivamente um “software” para acesso remoto de dispositivos, valendo-se para isto de uma instalação furtiva que permite o acesso integral às informações armazenadas no equipamento alvo.

Pelo que já foi exposto em nosso texto, fica claro que o sistema “Pegasus” é efetivamente uma ferramenta algo semelhante a um “keylogger” e que se destina ao acesso furtivo de dados armazenados em dispositivos informáticos.

No caso em comento, impende analisarmos a legalidade da aquisição e utilização de uma ferramenta de acesso remoto para a obtenção de informações particulares, e, em caso positivo, em que circunstâncias seu uso seria permitido.

Em primeiro lugar é importante destacarmos que a ferramenta “Pegasus” atua precipuamente através de interceptação telemática, uma vez que é necessária a sua instalação furtiva num equipamento alvo, seja pelo acesso direto ao mesmo ou por acesso remoto através de redes de telecomunicação ao qual o equipamento esteja conectado, o que se configura em acesso telemático.

Desta forma, restaria uma análise quanto à legalidade de interceptaçãoes telemáticas e em que condições tal poderia ocorrer.

Poderíamos definir a interceptação telemática como a captação de dados armazenados num dispositivo informatizado com a finalidade de tomar conhecimento de seu conteúdo, sem que os interlocutores tomem conhecimento de que um terceiro estaria inserido nas informações constantes da comunicação realizada por aquelas partes.

No aspecto da legalidade dessa ação, importante mencionarmos que a interceptação telemática sem a devida autorização judicial é considerada crime previsto no artigo 10 da Lei 9.296/1996, dispositivo legal que regulamenta a previsão inserida no artigo 5º, XII, daquele diploma legislativo:

“Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. ”

Também há que ser destacado que a interceptação telemática somente pode ser realizada exclusivamente com autorização judicial, desde que presentes os seguintes requisitos: a) Indícios razoáveis de autoria ou participação em infração penal; b) Imprescindibilidade da medida; c) O fato investigado deve constituir crime punido com reclusão.

Dessa forma, torna-se inquestionável que qualquer tipo de recurso destinado a interceptação telemática deverá ter o seu uso devidamente autorizado pelo Poder Judiciário e para fim exclusivo de investigação criminal, o que implica que apenas os órgãos legalmente incumbidos de realizar esse tipo de atividade estariam legitimados a utilizar recursos tecnológicos destinados a esse fim.

Neste ponto é de todo importante que seja destacada informação divulgada por diversos órgãos de imprensa, dando conta de que as licenças de uso do sistema “Pegasus" obedeceriam à seguinte distribuição: das 249 (duzentas e quarenta e nove) licenças previstas no contrato de aquisição a ser firmado, 100 (cem) seriam disponibilizadas para a Polícia Federal e 40 (quarenta) seriam fornecidas para a Secretaria da Segurança Pública de Brasília.

Outras 15 (quinze) permissões de uso seriam destinadas ao Corpo de Bombeiros e às Polícias Civil e Militar do Distrito Federal, enquanto as autorizações restantes seriam disponibilizadas ao Banco Central, ao Ministério Público Federal e a órgãos de 13 (treze) Estados.

Citada informação, tornada pública por órgãos de imprensa, chama a atenção pelo simples fato de afirmar que licenças de uso do sistema seriam disponibilizadas para instituições que não estão legitimadas à realização de investigações criminais.

Sem o desejo de adentrarmos na questão da legitimidade para a realização de investigações criminais, única e legítima hipótese que autoriza uma interceptação telemática, causa espanto ao permitir que uma instituição financeira como o Banco Central do Brasil possa fazer uso de um sistema que permite interceptações telemáticas como o “Pegasus”.

Caso não seja para a realização de uma investigação criminal, que deve ser realizada por órgãos com previsão legal para este tipo de ação na Constituição Federal, qual seria o propósito de fornecer os meios necessários para uma interceptação telemática?

É evidente que uma questão como essa fica sem resposta ao analisarmos os aspectos legais que envolvem a aquisição de um sistema como o “Pegasus”, o qual, sempre importante frisarmos, é ferramenta destinada a interceptação telemática.

Alguns poderiam afirmar que a ferramenta na realidade pode ser utilizada para a coleta de dados em “fontes abertas”, mas, como mencionamos anteriormente, o “Pegasus” é muito mais do que apenas um sistema destinado a essa finalidade.

Dessa forma, caso a utilização desse sistema esteja relacionada à coleta de informações não estruturadas em fontes abertas, não se justificaria o seu uso por existirem outros sistemas muito melhores para essa finalidade, alguns inclusive desenvolvidos com código fonte aberto.

Qualquer comparação quanto ao uso de um sistema como o “Pegasus” para a realização de interceptações telemáticas tem que levar em consideração toda a sistemática imposta ao uso de equipamentos destinados a interceptações telefônicas, sistemas amplamente utilizados pelas Polícias Judiciárias brasileiras.

Qualquer licitação que se destina à aquisição de equipamentos destinados a interceptações deve por força de lei ser transparente e principalmente descrever a sua finalidade de uso, facilitando assim qualquer tipo de fiscalização a ser promovida por órgãos de controle de atividades policiais, evitando-se que abusos venham a ser praticados.

Dessa forma, causam estranheza as circunstâncias em que a propalada aquisição do sistema “Pegasus” vem sendo noticiada, haja vista a destinação que está sendo prometida às licenças que deverão ser adquiridas.

Finalizando, necessário que o Brasil não se torne um estado de vigilância permanente onde seus cidadãos tenham seus mais comezinhos direitos desrespeitados e a sua vida íntima exposta ao arbítrio estatal.

José Mariano de Araujo Filho
Delegado de polícia especialista na investigação de cibercrimes, professor universitário, professor da Academia de Polícia Civil do Estado de São Paulo

---

https://fontesegura.forumseguranca.org.br/multiplas-vozes/44ncpdr4zg