CÂMARA DOS DEPUTADOS

PROJETO DE LEI N.º 58, DE 2024

(Do Sr. Alberto Fraga)

Disciplina a utilização, para fins de atividades de inteligência estatal, de investigação criminal, de controle ou de fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal, define crimes, e dá outras providências.

DESPACHO:
APENSE-SE AO PL-199/2021.

APRECIAÇÃO:
Proposição Sujeita à Apreciação do Plenário

PUBLICAÇÃO INICIAL
Art. 137, caput - RICD

PROJETO DE LEI N.º _____, DE 2024

(Do Senhor Deputado Alberto Fraga).

Disciplina a utilização, para fins de atividades de inteligência estatal, de investigação criminal, de controle ou de fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal, define crimes, e dá outras providências.

O **CONGRESSO NACIONAL** decreta:

Art. 1º A utilização, para fins de atividades de inteligência estatal da União, de investigação criminal, de controle ou fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal ou corporativa, diversa do previsto no inciso XII, do artigo 5º da Constituição Federal e na Lei nº 9.296, de 24 de julho de 1996, dar-se-á na forma desta lei.

Parágrafo único. O uso dos programas informáticos e as ferramentas previstas no *caput* são considerados espécies de técnicas e meios sigilosos previstos no parágrafo único do art. 3º da Lei nº 9.883, de 7 de dezembro de 1.999.

Art. 2º O emprego de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal ou corporativa somente será possível no caso de obtenção de dados negados necessários e relevantes para o cumprimento da operação de inteligência estatal ou de investigação criminal, de controle ou de fiscalização fazendária federais que dependam de autorização judicial, ouvido necessariamente o Ministério Público.

Parágrafo único. O emprego das técnicas e dos meios sigilosos especiais previstos nesta lei dependerá de autorização judicial, cabendo ao juízo competente decidir sobre pedidos de identidade fictícia dos agentes públicos encarregados dos casos.

Art. 3º O pedido de autorização judicial para utilização de ferramentas tecnológicas que consistem em programas de acesso a dispositivos eletrônicos para interceptação, captação, coleta, visualização ou qualquer outra forma de acesso a dados, informações e comunicações de investigados, alvos ou pessoas em geral, contidas em aparelhos digitais de comunicação pessoal, *smartphones*, tabletes e dispositivos eletrônicos similares, deverá conter, concomitantemente:

I – a descrição dos fatos que justifique, de maneira suficiente, a expedição de mandado judicial para o uso de técnica ou meio sigiloso especial, no estrito cumprimento das atribuições legais da atividade de inteligência ou de investigação criminal ou de controle;

II – a indicação e a qualificação da pessoa que possui a informação, registro, documento ou coisa a ser obtida, salvo impossibilidade manifesta, devidamente justificada;

III – a demonstração de que a sua realização é necessária, adequada e proporcional ao caso concreto e que se enquadra nas

atribuições legais da atividade de inteligência, investigativa, ou de controle, devendo explicitar, dentre outras coisas, que:

a) não há outro meio ou técnica menos invasivo de direito fundamental mediante o qual se possa obter a informação;

b) as técnicas ou meios sigilosos especiais requeridos são adequados à obtenção da informação pretendida;

c) a existência de controle de acesso de pessoas cadastradas para uso do sistema com mecanismos de identificação e registro permanente do usuário, para fins de auditabilidade, rastreabilidade e controle individualizado;

IV – a descrição do ambiente virtual em que o mandado judicial será executado, salvo impossibilidade manifesta, devidamente justificada;

VI – a indicação das pessoas ou autoridades a quem o mandado judicial será dirigido;

VII – o prazo pretendido de uso dos meios e técnicas sigilosos especiais, não excedente a 90 (noventa) dias, podendo o juiz competente, de maneira fundamentada, a pedido, autorizar renovações, de igual período, desde que comprovada a necessidade da renovação e continuarem presentes os requisitos legais;

VII – vinculação da operação de inteligência ou da investigação criminal a inquérito policial, processo investigativo ou judicial ou plano de operação de inteligência aprovado previamente.

Art. 4º O procedimento correrá sob segredo de justiça desde a sua distribuição, não podendo conter dados que possam revelar a operação de inteligência ou investigação policial a ser efetivada ou identificar os agentes públicos responsáveis.

§1º O juiz competente deverá assegurar a confidencialidade:

I – de qualquer informação sobre as fontes das informações; e,

II – dos dados iniciais constantes do requerimento de autorização judicial, se sua revelação puder colocar em risco a segurança da Sociedade, do Estado ou de qualquer pessoa.

§ 2º O juiz em sua decisão de autorização deverá constar, expressamente, os nomes dos servidores do cartório ou da secretaria responsáveis pela tramitação da medida e da expedição dos respectivos ofícios.

§ 3º O juiz determinará que as ferramentas ou programas informáticos sejam utilizados apenas para identificar, localizar ou rastrear telefones celulares ou outros aparelhos de comunicação dos investigados, sem outorgar o acesso às comunicações privadas de terceiros, não relacionados com os sujeitos da investigação.

§ 4º O magistrado ainda determinará que não sejam gravadas ou armazenadas conversas privadas de terceiros, cujos celulares ou dispositivos de comunicação estejam localizados nas proximidades da ferramenta de captação de dados, devendo haver o descarte imediato dos respectivos dados e comunicações, com a ressalva daqueles relacionados aos alvos e investigados, que serão armazenados para uso investigativo, de relatório de inteligência, de controle ou judicial.

Art. 5º Para qualquer ação prevista nesta lei, a instituição, ou órgão, de inteligência, policial, ou de controle, deverá possuir normativas internas detalhadas sobre o uso do programa informático ou ferramenta, incluindo previsão de termo de responsabilidade dos usuários, asseguradas a auditabilidade e a rastreabilidade.

§ 1º As normativas deverão prever que no caso de qualquer transferência, remessa ou compartilhamento de dados específicos exigir-se-á o estrito respeito às regras de sigilo e classificação, sendo obrigatório que as

autoridades recebedoras do material compartilhado assinem termo de responsabilidade com compromisso de manutenção do sigilo, nos termos da legislação vigente.

§ 2º Deverá ser assegurada que qualquer cooperação ou assistência técnica e científica, em atividade de natureza policial, de inteligência, ou controle, a ser prestada eventualmente aos Estados, Distrito Federal e Municípios, respeite as regras de sigilo existentes, exigindo-se das autoridades que se beneficiem das ferramentas que assinem termo de responsabilidade e se comprometam a manter o sigilo.

§ 3º As normativas deverão prever treinamento específico para seus investigadores, analistas, policiais, agentes ou oficiais de inteligência e quaisquer outros agentes públicos que operem tais ferramentas, a fim de que o uso seja adequado à proteção dos direitos fundamentais dos alvos, de investigados e de terceiros.

§ 4º A instituição, ou órgão, de inteligência, policial, de controle ou fiscalização deverá disponibilizar os sistemas eletrônicos de que trata esta lei para que sejam dotados de campos indicativos do êxito de tais ferramentas para a respectiva atividade de inteligência, controle, fiscalização ou investigação, a fim de que haja permanente aperfeiçoamento do seu uso, possibilitando reavaliar a necessidade de prorrogar as respectivas licenças pela constatação da eficácia ou inefetividade da ferramenta na prática.

§ 5º É vedado, sob qualquer hipótese, o armazenamento de dados em sistemas de empresas privadas no exterior ou de governos estrangeiros.

Art. 6º Ao final de cada operação ou diligência será obrigatória redação de relatório circunstanciado da utilização da ferramenta ou programa informático, classificado na forma da legislação vigente.

Parágrafo único Para fins desta lei, a instituição, ou órgão, deverá estabelecer sistema de registro inalterável, com identificação do usuário e senha, data e hora de acesso ao sistema, armazenados por no mínimo 30 anos e submetidos aos órgãos de controle da atividade dos usuários ou investigadores mediante solicitação ou requisição.

Art. 7º Constitui crime utilizar programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal ou quebrar segredo da Justiça referente ao seu uso, sem autorização judicial ou com objetivos não autorizados em lei.

Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 1º Na mesma pena incorre quem autoriza ou permite armazenamento de dados ou de informações de que trata esta lei em sistemas de empresas privadas no exterior ou de governos estrangeiros.

§ 2º A pena será aplicada em dobro ao agente público que descumprir a determinação de sigilo das investigações ou das operações que envolvam o uso de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal ou corporativa ou revelar o conteúdo dos dados durante o tempo do sigilo ou da classificação.

Art. 8º Com relação ao juiz competente, o Conselho Nacional de Justiça poderá promover:

I – unicamente para o caso de operações de inteligência estatal da União, previsão de juízo federal específico, em âmbito nacional ou regional;

II - realização de pesquisas estatísticas para avaliar os resultados;

III – no caso de operações de inteligência da União, a capacitação dos juízes e dos servidores da Justiça, de modo a buscar a sua especialização em temas relacionados ao exercício das funções dos órgãos e instituições solicitantes; e

III - avaliação sobre a distribuição de competência em processos decorrentes desta lei.

Art. 9º Esta Lei entra em vigor na data de sua publicação.

JUSTIFICATIVA

O Projeto de Lei apresenta proposta de disciplina da utilização, para fins de atividades de inteligência estatal, de investigação criminal ou de controle, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal ou corporativa, além de definir crimes por quebra de sigilo, uso ou armazenamento indevido.

O tema tem sido debatido publicamente, muitas vezes de modo polêmico, por vezes sensacionalista, especialmente por se relacionar a risco de ações que possam comprometer a privacidade e a intimidade dos cidadãos. De outro lado, o avanço das comunicações e da criptografia, especialmente esta, enseja perniciosa proteção às atividades ilícitas, criminosas, relacionadas a crimes comuns e às organizações criminosas. Cita-se, ainda, a atuação da interferência estrangeira no país e a crescente espionagem estatal, as quais comprometem interesses estratégicos nacionais, de natureza política ou econômica, ou de ambas, seja no âmbito público e privado de interesse estratégico, por exemplo, os desenvolvedores de equipamentos de uso dual.

Assim, se por uma linha há que se garantir, de modo efetivo, a proteção dos direitos individuais fundamentais citados, previstos na Constituição, há que se permitir alguma margem de atuação das instituições e dos órgãos encarregados de atuar contra a criminalidade ou contra a espionagem, por exemplo. A solução dá-se por uma única via, o estrito controle legal, a ser

realizado previamente e posteriormente pelo Poder Judiciário, sempre ouvido o Ministério Público.

Por essa razão, de modo oportuno, a Procuradoria-Geral da República ingressou com a Ação de Inconstitucionalidade por Omissão (ADO), que recebeu o número de ADO 80, sob relatoria do nobre Ministro Cristiano Zanin.

Nessa ADO, a douta Procuradora-Geral que firma a inicial, Dra. Elizeta Maria da Paiva Ramos, afirma a pretensão do Parquet de ir:

> *"contra a ausência de atuação normativa do Congresso Nacional, representada pela omissão parcial na regulação do uso, por órgãos e agentes públicos, de programas de intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal – smartphones, tablets e dispositivos eletrônicos similares – a fim de dar efetividade aos mandamentos constitucionais de proteção estatal da intimidade e da vida privada, e de inviolabilidade do sigilo das comunicações pessoais e de dados, estatuídos no art. 5º, X e XII, da Constituição Federal".*

Corretíssima está a PGR e em falta com a Sociedade está o Parlamento, razão pelo qual o Relator oficiou, há poucos dias, ao Congresso Nacional para que resolva essa omissão[1]. O projeto de lei que ora apresento, como texto embrionário, surge da leitura da peça inicial, extraindo dela elementos de controle, alguns de modo textual, dentro do espírito pretendido.

Ademais, procurei na minha experiência como policial e de profissionais que consultei agregar outras balizas de controle, incluindo a previsão de tipo penal específico, na linha de outras legislações.

Nesse sentido, destaco a lapidar afirmação da PGR:

> *"Nessa linha, torna-se essencial que o Congresso Nacional elabore normas primordialmente para regular o*

1 https://g1.globo.com/politica/noticia/2024/02/01/em-meio-as-investigacoes-da-abin-paralela-zanin-da-prazo-para-que-congresso-apresente-propostas-para-regulamentacao-de-softwares-espioes.ghtml

uso e controle das três principais ferramentas disponíveis no mercado: 1) spywares, como o Pegasus do NSO Group, que intercepta dados ao infectar um dos dispositivos envolvidos na comunicação; 2) Imsi Catchers, como o Pixcell (NSO Group) e o GI2 (Cognyte/Verint), que simulam estações rádio-base capturando dispositivos próximos; 3) dispositivos que rastreiam a localização de um alvo específico através da rede celular, como o First Mile (Cognyte/Verint) e o Landmark (NSO Group).

Por esse motivo, incumbe a essa Corte Suprema declarar a omissão parcial do Congresso Nacional em editar normatização que regulamente o uso, por órgãos e agentes públicos, de programas de intrusão virtual remota e/ou de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal – smartphones, tablets e dispositivos eletrônicos similares – fixando prazo razoável para que seja dada plena efetividade aos mandamentos contidos no art. 5º, X e XII, da CF, com definição das referidas balizas provisórias à salvaguarda dos direitos fundamentais à intimidade, à vida privada e ao sigilo das comunicações, até que seja suprida a mora legislativa inconstitucional”..

Enfim, de modo resumido, em um tema de solução relativamente simples, embora reconheço que não seja fácil, de mediar, de modo razoável e proporcional, interesses privados da Sociedade com seus interesses coletivos, seja o combate à criminalidade ou a proteção dos ativos estratégicos do País, incluindo a contraespionagem e o controle contra a corrupção, dotando o Brasil de uma legislação moderna que possa atender ao crescente desenvolvimento tecnológico, os quais trazem benefícios e, lamentavelmente, desafios, especialmente no âmbito criminal.

Pontuo, ainda, ter colocado previsão de incumbências para o Conselho Nacional de Justiça, de modo que a legislação possa ter algum controle posterior, especialmente no que tange às especificidades da atividade de

inteligência estatal da União, por envolver segredos estatais, de que, neste caso, seja melhor estabelecer juízos específicos para o controle judicial, diversamente da atividade de investigação policial ou de controle, que pode e deve ser de ampla competência.

A leitura do Projeto de Lei mostra que o texto é claro, sem questões legislativas complexas. Como afirmei, parafraseando o teórico da guerra Carl von Clausewitz: "No Parlamento tudo é muito simples, mas até a coisa mais simples é difícil".

Enfim, trata-se de texto embrionário, baseado em peça da PGR, como disse, inclusive com extração de partes textuais adaptadas, ao qual ofereço ao Parlamento como contribuição do meu dever parlamentar, ouvidos os reclamos da cidadania e de agentes públicos, de garantir controle e transparência para soluções necessárias para enfrentamento de problemas graves, dando maior segurança a estes agentes públicos no seu ofício, e ao mesmo tempo estabelecendo medidas protetivas para ações que possam oferecer riscos às garantias individuais, as quais exigem estrito controle.

Nesse sentido, conclamo aos colegas parlamentares o debate, o aperfeiçoamento e a aprovação desta proposição, por atender aos interesses do Estado e da Sociedade em temas tão sensíveis como os aqui tratados.

Sala das Sessões, em 2 de fevereiro de 2024.

Deputado Alberto Fraga

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL	https://normas.leg.br/?urn=urn:lex:br:federal:constituicao:198810-05;1988
LEI Nº 9.296, DE 24 DE JULHO DE 1996	https://normas.leg.br/?urn=urn:lex:br:federal:lei:1996-0724;9296
LEI Nº 9.883, DE 7 DE DEZEMBRO DE 1999	https://normas.leg.br/?urn=urn:lex:br:federal:lei:1999-1207;9883

FIM DO DOCUMENTO