



Número: **1031456-33.2021.4.01.3400**

Classe: **AÇÃO POPULAR**

Órgão julgador: **2ª Vara Federal Cível da SJDF**

Última distribuição : **20/05/2021**

Valor da causa: **R\$ 1.000,00**

Assuntos: **Anulação, Suspensão, Rescisão**

Segredo de justiça? **NÃO**

Justiça gratuita? **SIM**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Procurador/Terceiro vinculado	
ALESSANDRO VIEIRA (AUTOR)		RENATO RIBEIRO DE ALMEIDA (ADVOGADO)	
ADVOCACIA GERAL DA UNIAO (REU)			
MINISTERIO DA JUSTICA (REU)			
Ministério Público Federal (Procuradoria) (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
54882 0367	20/05/2021 13:11	Ação Popular - Licitação 03_2021	Inicial

**EXCELENTÍSSIMO SENHOR DOUTOR JUIZ FEDERAL DA __ VARA FEDERAL
DE BRASÍLIA/DF**

ALESSANDRO VIEIRA, brasileiro, casado, Senador da República, RG 811924 SSP/SE, CPF 719.437.905-82, título de eleitor 018291022135, com endereço profissional na Praça dos Três Poderes, Palácio do Congresso Nacional, Senado Federal, Anexo 2, Ala Afonso Arinos, Gabinete 08, endereço eletrônico sen.alessandrovieira@senado.leg.br, vem respeitosamente perante Vossa Excelência, por seu advogado subscritor, com fundamento nos artigos 1º, § 1º e 2º, parágrafo único e alíneas “a”, “c” e “d” da Lei nº 4.717/1965, propor a presente

**AÇÃO POPULAR
com pedido liminar**

em desfavor da **UNIÃO**, pessoa jurídica de direito público, representada em juízo pela Advocacia Geral da União, com sede no Setor de Autarquias Sul, Quadra 3, Lotes 5 e 6, Ed. Multi Brasil Corporate, CEP 70070-030, Brasília/DF, na qualidade de pessoa jurídica em nome da qual foi praticado o ato impugnado.

I - DOS FATOS

1. O Ministério da Justiça e da Segurança Pública lançou o Edital de Licitação Nº 03/2021, com objetivo de atender necessidades operacionais da Diretoria de Inteligência da Secretaria de Operações Integradas, conforme documenta o objeto do certame no subitem 1.1, como:

“(…)
a escolha da proposta mais vantajosa para a aquisição de **Solução de Inteligência em Fontes Abertas, Mídias Sociais, Deep e Dark Web** compreendendo o fornecimento, instalação e configuração, bem como o suporte técnico, em atendimento às necessidades operacionais da Diretoria de Inteligência da Secretaria de Operações Integradas (DINT/SEOPI)...”

2. A motivação para a contratação foi apresentada pelo item 3 e seguintes subitens do Termo de Referência que acompanha o edital, e aponta que a proposta foi baseada no DOD (SEI 11176453) que supostamente indicaria a necessidade de aquisição do

1/16

Av. Paulista, 1765, 13º andar. CEP. 01311-000. São Paulo – SP
www.ribeirodealmeida.adv.br contato@ribeirodealmeida.adv.br Tel. (11) 2450-7371



serviço. Cabe ressaltar ainda que o referido documento não foi encontrado na base de dados SEI do Ministério da Justiça:

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

sei

Pesquisa Pública

Nº do Processo ou Documento:

Pesquisa Livre:

Pesquisar em: Processos Documentos Gerados Documentos Externos

Interessado / Remetente:

Unidade Geradora:

Tipo do Processo:

Tipo do Documento:

Data do Processo / Documento: Período explícito 30 dias 60 dias

Sua pesquisa pelo termo não encontrou nenhum protocolo correspondente.

Sugestões:

- Certifique-se de que todas as palavras estejam escritas corretamente.
- Tente palavras-chave diferentes.
- Tente palavras-chave mais genéricas.

3. O Termo de Referência elenca ainda, entre as justificativas para o registro de preços, uma série de atribuições da DINT/SEOPI, como órgão subsidiário ao Secretário de Operações Integradas, e da SEOPI como agência central do SISP, submetido ao SBI, e organizadora das AISP's regionais, baseando-se nos Arts. 29 e 31 do Decreto 9662/19 da Presidência da República, *in verbis*:

Art. 29. À Secretaria de Operações Integradas compete:

I - assessorar o Ministro de Estado nas atividades de inteligência e operações policiais, com foco na integração com os órgãos de segurança pública federais, estaduais, municipais e distrital;

II - implementar, manter e modernizar redes de integração e de sistemas nacionais de inteligência de segurança pública, em conformidade com disposto na Lei nº 13.675, de 11 junho de 2018;

III - promover a integração das atividades de inteligência de segurança pública, em consonância com os órgãos de inteligência federais, estaduais, municipais e distrital que compõem o Subsistema de Inteligência de Segurança Pública;

(...)

Art. 31. À Diretoria de Inteligência compete:

I - assessorar o Secretário de Operações Integradas com informações estratégicas no processo decisório relativo a políticas de segurança pública;

II - planejar, coordenar, integrar, orientar e supervisionar, como agência central do Subsistema de Inteligência de Segurança Pública, as atividades de inteligência de segurança pública em âmbito nacional;

III - subsidiar o Secretário de Operações Integradas na definição da política nacional de inteligência de segurança pública, especialmente quanto à doutrina, à forma de gestão, ao uso dos recursos e às metas de trabalho;



- IV - promover, com os órgãos componentes do Sistema Brasileiro de Inteligência, o intercâmbio de dados e conhecimentos, necessários à tomada de decisões administrativas e operacionais por parte da Secretaria de Operações Integradas;
- V - propor ações de capacitação relacionadas com a atividade de inteligência de segurança pública, em parceria com a Diretoria de Ensino e Estatística da Secretaria Nacional de Segurança Pública e com outros órgãos e instituições, no País ou no exterior;
- VI - desenvolver, acompanhar, avaliar e apoiar projetos relacionados com a atividade de inteligência de segurança pública;
- VII - elaborar estudos e pesquisas para o aprimoramento das atividades de inteligência de segurança pública e de enfrentamento ao crime organizado;
- VIII - planejar, supervisionar e executar ações relativas à obtenção e à análise de dados para a produção de conhecimento de inteligência de segurança pública destinados ao assessoramento da Secretaria de Operações Integradas; e
- IX - acompanhar as atividades operacionais demandadas pela Diretoria e executadas por outros órgãos do Ministério da Justiça e Segurança Pública que envolvam aplicação de instrumentos e mecanismos de inteligência policial.

4. A referida Licitação obteve grande repercussão midiática, pois existe a indicação de que seriam potencialmente adquiridos softwares de espionagem pelo Governo Federal, na aparelhagem do que se intitularia “ABIN paralela”. Tal instituição **consistiria em um órgão de espionagem afastado da Agência Brasileira de Inteligência (ABIN) e com maior ligação com o Presidente da República**, para uma alegada utilização pessoalista destes meios de investigação.

5. Conforme demonstrado, trata-se da tentativa de **licitação de objeto potencialmente ilícito, desmotivada e que partiu de autoridade incompetente**, pois **usurpou a competência da ABIN e do Gabinete de Segurança Institucional (GSI)**. Além de **violar direitos fundamentais como o direito ao sigilo de dados pessoais**, que só poderia ser violado com a devida previsão legal ou autorização judicial.

6. Nesse sentido criou-se a necessidade de intervir na licitação em questão, por potencial violação aos **princípios da administração pública e aos direitos difusos**, pelas razões que seguem:

A. A empresa NSO GROUP

7. Segundo reportagem do portal de notícias UOL¹, fontes que fazem parte do Sistema Brasileiro de Inteligência (SISBIN) enfatizaram a participação da NSO Group no presente pregão por meio de revendedor brasileiro, perfazendo proposta ao edital no valor de R\$ 60,9 milhões.

¹ Lucas Valença, Carlos Bolsonaro intervém em compra de aparelho espião e cria crise militar. Disponível em: <<https://noticias.uol.com.br/politica/ultimas-noticias/2021/05/19/briga-entre-militares-e-carlos-bolsonaro-racha-orgaos-de-inteligencia.htm?cmpid=copiaecola>>



8. Ocorre que a NSO Group é uma empresa estrangeira, israelense, de tecnologia e inteligência fundada em 2010, localizada atualmente próximo a Tel Aviv, comprada em 2014 pela empresa de capital de risco americana Francisco Partners, alegando ser seu objetivo criar ferramentas contra crime e terrorismo.

9. Porém, não é apenas por esse tipo de atividade que o grupo é conhecido. A empresa acumula fama duvidosa na mídia quanto à sua real atuação e objetivo de seus serviços. Segundo o veículo de comunicação mundialmente conhecido **BBC News**²:

“(…) E alguns pesquisadores da área dizem que, na verdade, a NSO é uma revendedora de armas cibernéticas, algo de que a empresa já fora acusada no passado.

Em 2016, a companhia foi apontada como criadora de um software malicioso capaz de instalar um programa espião (spyware) em dispositivos iPhone e acessar uma enorme quantidade de dados: mensagens de texto, fotos, emails, geolocalização e até mesmo o que o microfone e a câmera captavam.

O advogado de direitos humanos Ahmed Mansoor foi um dos alvos desse ataque. Na época, Mansoor acionou especialistas do Citizen Lab, instituição canadense, e da Lookout, empresa americana que descreveram o programa como **uma das armas cibernéticas mais sofisticadas já descobertas**. Ao examinar o celular de Mansoor, os especialistas encontraram pistas que remetem ao Pegasus, principal programa da NSO.

10. Ainda, segundo a **Forbes**³:

“(…) A NSO é conhecida no mundo da cibersegurança por seu software “Pegasus” e outras ferramentas que podem ser fornecidas de várias maneiras. O software pode capturar tudo em um telefone, incluindo o texto sem formatação de mensagens criptografadas.”

11. O jornal diário espanhol **El País** noticiou em 2020 que o aplicativo de troca de mensagens instantâneas Whatsapp tentou forçar a empresa a revelar os governos que permitiu ‘invadir’ telefones e que:

“(…) A NSO Group é dona do Pegasus, o software espião que supostamente invadiu os celulares do presidente do Parlamento regional da Catalunha, Roger Torrent, e do ex-conselheiro do partido Esquerda Republicana da Catalunha (ERC, independentista) Ernest Maragall, segundo uma investigação do **EL PAÍS** e do *The Guardian*. A intrusão nos telefones dos dirigentes independentistas catalães ocorreu graças a uma falha de segurança do WhatsApp que, entre abril e maio

² NSO Group, a Polêmica Empresa Israelense Que Está Sendo Vinculada a Hackeamento Do WhatsApp.” *BBC News Brasil*, BBC, www.bbc.com/portuguese/geral-48279595

³ REDAÇÃO. FBI investiga uso de spyware israelense para invadir dados de pessoas e governos. Disponível em: <<https://forbes.com.br/negocios/2020/01/fbi-investiga-uso-de-spyware-israelense-para-invadir-dados-de-pessoas-e-governos/>>



de 2019, permitiu que o programa penetrasse nos celulares de cerca de 1.400 pessoas. No caso dos políticos independentistas, será muito complicado conhecer a identidade de quem instalou os sistemas de espionagem em seus telefones, mas é sabido que os serviços de inteligência espanhóis dispõem desse software.

B. Sistema PEGASUS

12. Pegasus, ferramenta que poderia vir a ser adquirida segundo o teor do edital sob exame, é o mais conhecido equipamento de investigação da empresa NSO Group. Esse equipamento trabalha por meio de um conjunto de softwares e hardwares capazes de invadir telefones celulares à distância. É dito ter a capacidade de captar todas as informações presentes no aparelho, e ainda:

“(…)Não há criptografia de ponta a ponta que resista. O Pegasus identifica e recolhe sorrateiramente desde o histórico de conversas do WhatsApp e do Telegram até os lugares por onde o alvo passou, quanto tempo permaneceu em cada um, sua localização exata, além do som e das imagens do ambiente por meio da ativação de microfone e câmera feita remotamente e em tempo real. Não à toa, vem sendo adquirido por governos ao redor do mundo por milhões de dólares como o mais sofisticado sistema de espionagem da atualidade. Segundo pesquisadores canadenses, governos ao redor do mundo estão usando o Pegasus para espionar ativistas, jornalistas, opositores e potenciais inimigos políticos.”⁴

13. O mesmo artigo informa o tamanho do alcance de infecção do potencial *spyware*, ao informar que nem sequer necessitaria de interação do usuário para que este invada as informações presentes no aparelho infectado:

“Um espião digital silencioso em seu bolso’, assim o Pegasus foi definido pelo pesquisador John Scott-Railton, em um relatório produzido pelo laboratório interdisciplinar Citizen Lab, da Universidade de Toronto, no Canadá, pioneiro na busca por evidências do uso do software. Diferentemente de seus concorrentes no mercado da espionagem, o Pegasus pode acessar o telefone do alvo sem que ele precise clicar em um link infectado. Os policiais chamam isso de ‘capacidade zero clique’, o grande trunfo do produto israelense.”

II - DO CABIMENTO E DA LEGITIMIDADE ATIVA

14. O art. 5º, inciso LXXIII da Constituição Federal, confere ao cidadão a prerrogativa de ajuizar uma ação popular para pleitear a anulação ou a declaração de nulidade de atos lesivos ao patrimônio da União, do Distrito Federal, dos Estados, dos Municípios, de entidades autárquicas, de sociedades de economia mista, de sociedades mútuas de seguro nas quais

⁴ A CHEGADA AO BRASIL DO PEGASUS, ESTRELA DO SUBMUNDO DA ESPIONAGEM. Disponível em: <<https://www.aner.org.br/ani-aner-informativo/a-chegada-ao-brasil-do-pegasus-estrela-do-submundo-da-espionagem.html>>



a União represente os segurados ausentes, de empresas públicas, de serviços sociais autônomos, de instituições ou fundações para cuja criação ou custeio o tesouro público haja concorrido ou concorra com mais de cinquenta por cento do patrimônio ou da receita anual, de empresas incorporadas ao patrimônio da União, do Distrito Federal, dos Estados e dos Municípios, e de quaisquer pessoas jurídicas ou entidades subvencionadas pelos cofres públicos.

15. Vê-se que a Constituição de 1988 conferiu especial importância à ação popular, tornando-a um instrumento jurídico disponível a qualquer cidadão para exercer sua cidadania e buscar a guarida do Poder Judiciário, com vistas à proteger o Estado contra atos atentatórios cometidos pelos seus próprios agentes, aos quais é legítimo governar apenas a partir dos ditames e nos limites constitucionais.

16. Assim, a importância da ação popular se revela por meio da participação dos cidadãos nos destinos da coisa pública, facultando-lhes agir como um fiscal em favor do bem comum e da comunidade. É dizer que a verdadeira cidadania resulta no direito de fazer valer as prerrogativas que defluem de um Estado Democrático de Direito e que a ação popular é uma das formas de exercício imediato dessa prerrogativa.

17. Para corroborar o exposto, traz-se o escólio de Hely Lopes Meirelles:

“Ação popular é o meio constitucional posto à disposição de qualquer cidadão para obter a invalidação de atos (...) ilegais e lesivos do patrimônio federal, estadual e municipal (...). (...) Por ela não se amparam direitos individuais próprios, mas, sim, interesses da comunidade. O beneficiário direto e imediato desta ação não é o autor; é o povo, titular do direito subjetivo ao governo honesto. O cidadão promove em nome da coletividade no uso de uma prerrogativa cívica que a constituição lhe outorga. A constituição vigente mantendo o conceito da carta anterior, aumentou sua abrangência, para que o cidadão possa anular ato lesivo (...) à moralidade administrativa. (...) Entender-se, restritamente, que a ação popular só protege o patrimônio público material é relegar os valores espirituais a plano secundário e admitir que a nossa Constituição os desconhece ou julga indignos da tutela jurídica, quando, na realidade, ela própria os coloca sob sua égide (CF, arts. 23, VI, 24, VI, 170, VI, e 225). Essa proteção constitucional não deve ser apenas nominal, mas real, traduzindo-se em meios concretos de defesa, tais como a ação popular para a invalidação de atos lesivos desses valores. Se ao Estado incumbe proteger o patrimônio público, constituído tanto de bens corpóreos como de valores espirituais, de irrecusável lógica é que o cidadão possa compeli-lo, pelos meios processuais, a não lesar esses valores por atos ilegais da Administração.”

18. O § 3º do art. 1º da Lei 4.717/65 exige a prova de que os autores gozam da qualidade de cidadãos, que é feita por meio da apresentação do título eleitoral. Some-se a isso o fato de que o requerente é Senador da República, ocupante de mandato eletivo, de tal modo que, nesta condição, obrigatoriamente está na plenitude do gozo dos seus direitos políticos, fato que comprova a sua condição como cidadão.



19. De tal feita, apresentando o proponente seu título eleitoral, resta comprovada sua legitimidade para a propositura da presente ação.

III - DA COMPETÊNCIA

20. Dispõe o art. 5º da Lei 4.717/65 que “conforme a origem do ato impugnado, é competente para conhecer da ação, processá-la e julgá-la o juiz que, de acordo com a organização judiciária de cada Estado, o for para as causas que interessam à União, ao Distrito Federal, ao Estado ou ao Município.”

21. No presente caso, como o ato lesivo praticado pelo Ministro da Justiça e Segurança Pública foi realizado no âmbito da União, não restam dúvidas de que a competência para apreciar a presente demanda deve ser atribuída à Justiça Federal.

IV - DO DIREITO

A. DA USURPAÇÃO DE COMPETÊNCIA

22. No mérito, cabe apresentar, primeiramente, a problemática sobre a usurpação de competência para investigar e apurar dados sigilosos que se apresenta no caso concreto, entre a Diretoria da Secretaria de Operações Integradas (DINT/SEOPI), do Ministério de Justiça e Segurança Pública e as agências de inteligência brasileiras, notadamente à respeitada ABIN, submetidas às Forças Armadas.

23. A Licitação 03/2021, do Ministério da Justiça e Segurança Pública, que tinha o objetivo de atender as necessidades operacionais da Diretoria de Inteligência da Secretaria de Operações Integradas (DINT/SEOPI). A competência da DINT, estabelecida pelo Decreto nº 9.662, de 1º de janeiro de 2019, é estrita:

À Diretoria de Inteligência compete:

I - assessorar o Secretário de Operações Integradas com informações estratégicas no processo decisório relativo a políticas de segurança pública;

II - planejar, coordenar, integrar, orientar e supervisionar, como agência central do Subsistema de Inteligência de Segurança Pública, as atividades de inteligência de segurança pública em âmbito nacional;

III - subsidiar o Secretário de Operações Integradas na definição da política nacional de inteligência de segurança pública, especialmente quanto à doutrina, à forma de gestão, ao uso dos recursos e às metas de trabalho;

IV - promover, com os órgãos componentes do Sistema Brasileiro de Inteligência, o intercâmbio de dados e conhecimentos, necessários à tomada de decisões administrativas e operacionais por parte da Secretaria de Operações Integradas;

V - propor ações de capacitação relacionadas com a atividade de inteligência de segurança pública, em parceria com a Diretoria de Ensino e Estatística da Secretaria Nacional de Segurança Pública e com outros órgãos e instituições, no País ou no exterior;



VI - desenvolver, acompanhar, avaliar e apoiar projetos relacionados com a atividade de inteligência de segurança pública;

VII - elaborar estudos e pesquisas para o aprimoramento das atividades de inteligência de segurança pública e de enfrentamento ao crime organizado;

24. Apesar de algumas das competências utilizarem palavras vagas e genéricas, não é possível apreender deste rol estrito a competência de obter e analisar dados, de forma que não se justifica o processo licitatório em questão.

25. Tal entendimento é mais evidente quando se tem em vista que existem órgãos competentes para a obtenção e análise de dados pertinentes à segurança pública, em auxílio ao Presidente da República, como é o caso da ABIN.

26. Com efeito, a ABIN foi instituída pela Lei n. 9.883/1.999, com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional. Trata-se de uma **importantíssima instituição de Estado, não de governo**. A competência da agência é determinada no art. 4º:

Art. 4º. À ABIN, além do que lhe prescreve o artigo anterior, compete:
(Vide ADIN nº 6529)

I - planejar e executar ações, inclusive sigilosas, relativas à **obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o Presidente da República;**

II - planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade;

III - avaliar as ameaças, internas e externas, à ordem constitucional;

IV - promover o desenvolvimento de recursos humanos e da doutrina de inteligência, e realizar estudos e pesquisas para o exercício e aprimoramento da atividade de inteligência.

27. No rol de competências da ABIN tem-se claro o objetivo de obter e analisar dados, o que não é possível depreender das competências da DINT. Assim, *in casu* observa-se a total usurpação de competência da ABIN, pela DINT.

28. Fala-se de **usurpação de competência** porque, como já foi amplamente noticiado, há algum tempo observa-se a criação do que popularmente é chamado de **“ABIN paralela”**. Concretamente, é exatamente isso que ocorre.

29. O Subsistema de Inteligência de Segurança Pública (SISP) tem como órgão central a DINT/SEOPI. O atual Governo Federal possui um projeto de reestruturação deste sistema, como inclusive está disposto no parágrafo 3.1.5, do Edital de Licitação 03/2021, de forma que existiria a necessidade de aparelhamento do referido órgão central.



30. É compreensível o aparelhamento de tal órgão para a maior integração ao sistema, aumentando seu desempenho, com o objetivo de uma atuação mais estratégica perante o crime organizado. O cerne da questão, no entanto, é a relação entre tal integração e a aquisição de “Solução de Inteligência em Fontes abertas, Mídias Sociais, Deep e Dark Web”. Sabe-se que **tais softwares possibilitam, em tese, a espionagem, sem deixar rastros, com cruzamento de informações de fontes fechadas, a exemplo do Pegasus**, explicado anteriormente. De que maneira, portanto, **tais ferramentas podem auxiliar o SISP?** Essa questão se impõe e é do interesse de todos os brasileiros.

31. O edital da licitação apresenta a seguinte justificação:

"A aquisição de Solução de Inteligência em Fontes abertas, Mídias Sociais, Deep e Dark Web permitirá um ganho considerável em requisitos de performance e segurança, possibilitando uma maior integração com os sistemas de segurança pública, tornando-os seguros e com maior capacidade de desempenho. É de extrema importância o alinhamento da tecnologia da informação com as demandas da sociedade, visando eficiência e celeridade no acesso à informação, sustentando a função essencial de Segurança Pública, que é dar segurança e tranquilidade à sociedade, através de meios ágeis, de alta-disponibilidade, continuidade e segurança."

32. Por mais que o texto tente criar uma relação de causa e consequência, o **objeto da licitação é extremamente vago, sem qualquer descrição pormenorizada de como tais softwares podem contribuir para a atuação do órgão. Palavras como “segurança”, “desempenho”, “celeridade”, não justificam a escolha específica destes softwares, em detrimento a outras tecnologias.**

33. Ainda, é **relevante indagar as motivações que levaram a não inclusão da ABIN entre as instituições que receberão licenças de uso do novo sistema. Como coordenadora do Sistema Brasileiro de Inteligência, a agência estaria entre as principais interessadas em softwares que possibilitam a obtenção e análise de dados. Contudo, não foi abarcada pelo projeto.**

34. Confirmando-se ainda mais o potencial desenvolvimento de um **órgão paralelo de inteligência, que se distancia da ABIN e se aproxima do Palácio do Planalto**, por razões ainda não esclarecidas, mas que podem ser traçadas, tendo em vista a atuação repressiva, a partir de motivações pessoais do Presidente da República, nos últimos anos.

B. LICITAÇÃO DE OBJETO POTENCIALMENTE ILÍCITO

35. Para viabilizar a eventual atuação dos órgãos de controle, é imprescindível a possibilidade de auditoria do sistema. Tal como apresentado, apesar de nota dizendo o contrário por parte da União após tornarem-se públicas, por meio da grande mídia, as informações referentes



ao objeto da presente ação, está comprovado que o que é buscado em questão é um **equipamento que permitiria potencial acesso secreto, sem controle e sem nenhuma forma de auditoria e controle externo sobre acesso a dados, inclusive pessoais, de cidadãos brasileiros.**

36. O sistema, por sua própria fama de impossibilitar que seja rastreado o acesso, corresponderia à aquisição de equipamento, por parte do Governo Federal, capaz de conceder aos **agentes públicos que o manejarem, em tese, total e irrestrito acesso a dados de qualquer brasileiro que, por exemplo, tiver um celular.** E os cidadãos, **sem que nada em contrário possam fazer, terão apenas que confiar cegamente na ética subjetiva e discricionariedade dos transitórios ocupantes de cargos públicos.** Com efeito, conforme revelado pelo próprio Governo Federal, **nem mesmo a respeitada instituição de Estado ABIN participará do manejo de tão invasivo dispositivo.**

37. **A descrição do objeto da licitação (Solução de Inteligência em Fontes Abertas, Mídias Sociais, Deep e Dark Web), anexa a esta exordial e parcialmente transcrita no início da exposição dos fatos, abre espaço, de modo inequívoco, à potencial contratação de serviços de espionagem** que não podem estar à disposição do Estado sem que haja sindicabilidade.

38. Mesmo que houvesse uma descentralização no uso de tais serviços, franqueando-o a forças de segurança pública e defesa social sem potencial intervenção do Ministério da Justiça e Segurança Pública, não se mitiga a gravidade de sua utilização.

39. A realização da licitação nesses termos causa ainda maior preocupação ao se considerar que o ordenamento jurídico brasileiro não dispõe ainda de regras claras e uniformes para a separação informacional de poderes, tema que vem sendo discutido em países europeus, notadamente na Alemanha.

40. A possibilidade desmesurada de compartilhamento de dados sensíveis de particulares entre diferentes órgãos da Administração Pública, sem qualquer garantia de controle sobre obtenção e transmissão, representa grande perigo a direitos fundamentais previstos na Constituição Federal.

41. Portanto, mesmo que a publicização dada à licitação faça crer que o que se quer prestigiar é a segurança pública, o teor do edital de licitação n. 03/2021 dá ampla margem para a eventual contratação de ferramentas como a Pegasus, cuja nocividade já foi amplamente demonstrada em estudos de inegável seriedade (<https://citizenlab.ca/2018/09/hidden-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>).

42. Os contratos administrativos mantêm a natureza genérica de contratos e permanecem submetidos ao regime do Código Civil para negócios jurídicos. Dessa forma, o que se está a promover é um certame que, ao final, resultará em **contratação de objeto ilícito.**



43. Conforme narrado, o objeto do pregão é classificado como um *malware*, ou seja, um programa que seria, em tese, capaz de controlar e alegadamente espionar os sistemas que o recebem. Dessa forma, enquadrar-se-ia analogamente à prática de espionagem. Embora sem tratamento específico na legislação brasileira, a espionagem é tratada de maneira esparsa na legislação penal, geralmente referenciada à espionagem militar, isto é, ao acesso e apropriação desautorizados de informações e dados atinentes à defesa. Entretanto, os efeitos jurídicos da espionagem não se cingem à esfera do direito penal, podendo também repercutir em outras instâncias do direito, como a civil e a administrativa.

44. Afora os casos específicos e nominais de espionagem, a lei pune o acesso a dados ou os meios de obtenção, conforme o caso. Há que encarar o corpo de leis de modo sistemático; a mera ausência de menção ao termo espionagem não significa que ela não gere repercussões perante nosso ordenamento jurídico. Não obstante, há casos, sim, em que o termo espionagem é cunhado. Isso acontece no Código Penal Militar e na Lei de Segurança Nacional, diplomas legais de incidência relativamente restrita.

45. Dentre os crimes possíveis advindos do uso de tal ferramenta, podemos citar:

INFRAÇÕES PENAIS PRÓPRIAS DE ESPIONAGEM	
DIPLOMA LEGAL	TIPO
CÓDIGO PENAL MILITAR (DECRETO-LEI 1.001/1969)	Art. 143 – consecução de notícia, informação ou documento para fim de espionagem
	Art. 145 – turbação de objeto ou documento
	Art. 146 – penetração com o fim de espionagem
	Art. 147 – desenho ou levantamento de plano ou planta de local militar ou de engenho de guerra



	Art. 325, par. ún. – violação ou divulgação indevida de correspondência ou comunicação
	Art. 359 – informação ou auxílio ao inimigo
	Art. 362 – traição imprópria
	Art. 366 – espionagem
	Art. 367 – penetração de estrangeiro
LEI DE SEGURANÇA NACIONAL (LEI FEDERAL 7.170/ 1983)	Art. 13, par. ún., I e II – manter serviço de espionagem ou praticá-la
LEI DAS ELEIÇÕES (LEI FEDERAL 9.504/1997)	Art. 72, I – acesso indevido a sistemas de dados eleitorais
LEI DE PROPRIEDADE INTELECTUAL (LEI FEDERAL 9.279/1996)	Art. 195, XII – vazamento ou utilização de conhecimentos obtidos por meios ilícitos

46. Dessa forma, **fica demonstrado o potencial caráter ilícito do objeto licitado, uma vez que seu alcance para atividades proibidas é constatado** mediante vários estudos apresentados. Ademais, conforme se lê na descrição do Termo de Referência, há apenas uma descrição vaga da finalidade a que se presta a aquisição, sem qualquer controle ou garantia do modo como será operacionalizado.



47. Além das provisões penais, a espionagem também é tratada, implicitamente, na legislação de crimes de responsabilidade, que, conforme o entendimento predominante, não constituem infrações penais.

48. A Lei de Crimes de Responsabilidade (Lei Federal nº. 1.079, de 10 de abril de 1950) é aplicável ao Presidente da República, aos Ministros de Estado, aos Ministros do Supremo Tribunal Federal e ao Procurador-Geral da República e prevê, como pena, a perda do cargo e a inabilitação, por até cinco anos, para o exercício de função pública. Entre os crimes de responsabilidade contra a existência da União, praticáveis exclusivamente pelo Presidente da República, encontramos o do art. 5º, n. 4, c/c art. 4º, I.

49. Ressalta-se que este crime de responsabilidade, como dito acima, refere-se exclusivamente ao Presidente da República.

C. DO DIREITO DE SIGILO À CORRESPONDÊNCIA E ÀS COMUNICAÇÕES TELEGRÁFICAS, AOS DADOS E ÀS COMUNICAÇÕES TELEFÔNICAS

50. O direito ao sigilo à correspondência e às comunicações telegráficas, aos dados e às comunicações telefônicas é garantido constitucionalmente:

art. 5º. XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

51. Ainda, a Lei n. 9.296/1996, no art. 2º, parágrafo único, afirma que a quebra de sigilo deve descrever com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.

52. O Marco Civil da Internet do Brasil (Lei 12.965/ 2014) vai no mesmo sentido, garantindo, no art. 10, § 2º, que o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer.

53. O Decreto nº 8.771/2016, no art. 11, regulamenta o referido dispositivo, definindo que tais pedidos de autoridades administrativas devem expressamente conter o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados. Ainda, o §3º determina:

§ 3º. Os pedidos de que trata o caput devem especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas, **sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos.** (grifo nosso)

54. Sendo assim, com **respaldo em diversas leis, é ilegal um projeto que possibilite teoricamente a quebra de sigilo de dados, sem a individualização dos alvos, ou**



seja, a especificação dos objetos de investigação. No caso em questão vislumbra-se a compra de um software para “*solução de Inteligência em Fontes abertas, Mídias Sociais, Deep e Dark Web*”, alegadamente capaz de controlar e espionar os sistemas que o recebem.

55. Ainda, a quebra de sigilo e interceptação de informações é regida sempre pela prerrogativa de que se houver outra medida menos gravosa, ela deve ser adotada. Na Lei n. 9.296/1996, no art. 2º, II, é definido que não será admitida a interceptação se a prova puder ser feita por outros meios disponíveis.

56. Nesse sentido, a especialista em weblaw Carolina Christofoletti⁵:

“Chama a atenção, justamente, que a descrição do software seja feita como a de uma “Solução em Fontes Abertas, Mídias Sociais, Deep e Darknet”. Principalmente por que, em termos investigativos, a Deep Web é o único local no qual uma solução como um spyware poderia ser cogitável. Nos demais casos, **a utilização da ferramenta seria tão desproporcional como matar uma mosca com um fuzil.**” (grifei)

57. Tal comparação demonstra a desproporcionalidade da utilização de tais softwares quando se tem o objetivo de aumentar o desempenho e integração entre os sistemas de inteligência, o que indica a existência de outras ferramentas, menos intrusivas, que poderiam cumprir a mesma função.

D. DO PRINCÍPIO DE AUTODETERMINAÇÃO INFORMATIVA

58. A Lei Geral de Proteção de Dados, Lei n. 13.709/2018, define, no art; 4º, § 1º, que o tratamento de dados pessoais para fins de segurança pública e atividades de investigação de infrações penais será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD.

59. Ainda não há uma lei em vigência sobre este tema, apesar de já haver uma comissão de juristas que trabalha no Anteprojeto da chamada “LGPD Penal”. Contudo, como mencionado, o tratamento de dados pelas autoridades públicas deve respeitar os princípios da referida Lei, com destaque para a autodeterminação informativa.

60. A autodeterminação informativa é um conceito importado do direito alemão e consiste na faculdade de o particular determinar e controlar a utilização de seus dados, como decorrência do direito geral de personalidade.

⁵ A hacker tool in the hands of the government: With what criteria? (Portuguese). Disponível em: <<https://www.linkedin.com/pulse/hacker-tool-hands-government-what-criteria-portuguese-christofoletti/?published=t>> Acessado em: 19/05/2021



61. O Tribunal Constitucional Federal Alemão estabeleceu este direito a partir da Decisão do Censo, de 1983, tendo discorrido sobre o tema:

“Quem não consegue entrever com suficiente segurança que as informações a ele concernentes são conhecidas em que contextos de seu ambiente social, e quem não consegue, ainda que grosseiramente, estimar o que sabem os seus parceiros de comunicação, poderá ver-se consideravelmente impedido em sua liberdade de planejar e decidir a sua vida de forma autônoma. Uma ordem social, e o direito que a possibilita, em que os cidadãos não conseguem mais saber em que oportunidade quem, quando, sabe o que sobre as suas pessoas, não é compatível com o direito de autodeterminação informacional.”

62. *In casu*, tem-se a potencial adoção de um **sistema que possibilitaria a espionagem, a partir de total anonimato, não sendo possível o conhecimento dos cidadãos sobre o destino e o uso dos seus dados, em completa violação ao princípio da autodeterminação informativa, garantido pela LGPD.**

E. DA NECESSIDADE DE CONCESSÃO DA MEDIDA LIMINAR

63. Nos termos do § 4º do art. 5º da Lei 4.717/65, na defesa do patrimônio público, cabe a suspensão liminar do ato lesivo que é impugnado.

64. A presença dos requisitos para a concessão é inegável.

65. Por um lado, verifica-se o *fumus boni iuris*, diante do fato de que há lesão flagrante ao patrimônio público, desrespeito à moralidade pública e violação à intimidade e ao sigilo, tal como demonstrado nos tópicos anteriores.

66. O *periculum in mora* se evidencia pelo risco de comprometer gravemente a liberdade individual de todo e qualquer cidadão brasileiro na medida em que o objeto do pregão alegadamente possui a capacidade de invadir qualquer aparelho de comunicação, incluindo sistemas protegidos do Poder Judiciário e demais Poderes.

67. Diante desses elementos, pugna-se pela concessão de medida liminar para suspensão imediata do certame, na fase em que estiver, impedindo a consecução do contrato com a Administração Pública ou, se já feito, anulando o contrato.

V. DOS PEDIDOS

Ante o exposto, requer-se à Vossa Excelência, como medida justa e perfeitamente condizente com os ditames legais e constitucionais:



a) a concessão de liminar, sem oitiva da parte contrária, para que seja imediatamente suspenso o ato do Ministério da Justiça e Segurança Pública correspondente à consecução do Pregão n. 003/2021 da Pasta, suspendendo assim o certame, na fase em que estiver, e impedindo a consecução do contrato com a Administração Pública ou, se já feito, anulando o contrato;

b) o julgamento de procedência da presente demanda para que, ao final, seja anulado o ato descrito no item anterior;

c) seja citada a parte contrária para que, querendo, apresente contestação no prazo legal, sob pena de aplicação dos efeitos da revelia;

d) a intimação do Ministério Público Federal para que, em respeito ao art. 6º, § 4º da Lei n. 4.717/65, acompanhe a ação;

e) a condenação da parte demandada a arcar com custas, despesas judiciais e extrajudiciais, bem como com honorários advocatícios, nos termos do art. 12 da Lei da Ação Popular;

Protesta-se pela produção de todas as provas em direito admitidas.

Dá-se à causa o valor de R\$ 1.000,00 para fins de alçada.

Termos em que pede e aguarda deferimento.

São Paulo, na data do protocolo.

Renato Ribeiro de Almeida
OAB/SP n. 315.430

