EXCELENTÍSSIMO SENHOR MINISTRO BENJAMIN ZYMLER - TRIBUNAL DE CONTAS DA UNIÃO

EMENTA: Denúncia de entidades da sociedade civli. Irregularidades insanáveis no Pregão 3/2021 do Ministério da Justiça e Segurança Pública. Tentativa de contratar empresa para monitorar e gerar relatórios diários de dados em redes de relacionamentos, aplicativos de chat, deepweb. **Inadequação da modalidade de licitação escolhida.** Serviços que não podem ser caracterizados como *comuns*. **Usurpação de competência e violação do princípio da legalidade.** Órgão cujo papel é exclusivamente para formulação e gestão das políticas de segurança pública, sem poder de polícia. Impossibilidade. **Ilicitude do objeto.** Sistema que será usado para perfilamento e vigilantismo. Incompatibilidade com o Estado Democrático de Direito. Possível caracterização de desvio de finalidade. Necessidade de medida cautelar para impedir a homologação e a adjudicação do certame.

Distribuição por dependência ao Processo 014.845/2021-0

ASSOCIAÇÃO DIREITOS HUMANOS EM REDE - CONECTAS DIREITOS HUMANOS, [redacted] (**Docs. 01**), **INSTITUTO IGARAPÉ**, [redacted] (**Docs. 02**), **INSTITUTO SOU DA PAZ**, [redacted] **(Docs. 03), ASSOCIAÇÃO TRANSPARÊNCIA E INTEGRIDADE (TRANSPARÊNCIA INTERNACIONAL)**, [redacted]

[redacted] (**Docs. 04**), por seus procuradores e procuradoras **(Docs. 05)**, com fulcro nos artigos 71 da Constituição Federal, 53 a 55 da Lei 8.443/92, 234 e ss. e 249 e ss. do regimento interno do Tribunal de Contas da União vem oferecer a seguinte

DENÚNCIA

em razão da existência de irregularidades no **PREGÃO ELETRÔNICO Nº 3/2021 do Ministério da Justiça e Segurança Pública** cujo objeto é 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)"*, conforme as razões adiante expostas[1].

1. PRELIMINARES: dos requisitos para a apresentação de denúncia a esta Corte de Contas.

Nos termos do que define o art. 235 do Regimento Interno deste E. Tribunal de Contas da União, importa elucidar de saída o atendimento desta denúncia aos requisitos erigidos em tal diploma, para a apresentação de denúncia.

A presente peça é absolutamente idônea para cumprir a função a que se presta, na medida em que:

[1] Disponível em https://www.gov.br/mj/pt-br/acesso-a-informacao/licitacoes-e-contratosv1/licitacoes-e-contratos-segen/cglic/cpl/copy64_of_pregoes-02_2021, acessado em 20 de maio de 2021.

(i) Refere-se a administrador ou responsável sujeito à sua jurisdição.

A presente denúncia diz respeito a edital público assinado pelo Diretor de Gestão da Secretaria de Gestão e Ensino em Segurança Pública do Ministério da Justiça e Segurança Pública, órgão integrante da Administração Pública Federal Direta e, portanto, sujeita à jurisdição deste Tribunal de Contas da União, nos termos do que definem os artigos 70 e 71 da CF/88.

(ii) Está redigida em linguagem clara e objetiva.

A denúncia está redigida no registro formal da Língua Portuguesa, atendendo aos parâmetros na norma culta, tendo sido empreendido o maior esforço possível para manter o relato sintético e objetivo, procedendo-se inclusive à repartição do argumento em tópicos simples e claros.

(iii) Contém o nome legível do denunciante e seu endereço.

As denunciantes encontram-se devidamente identificadas na primeira página da denúncia, bem como na procuração anexa, contendo não apenas o seu nome, como seus dados de contato (telefônico e eletrônico).

(iv) Está acompanhada de indício concernente à irregularidade ou ilegalidade denunciada.

A farta compilação dos fundamentos de fato e de direito para a presente denúncia encontra-se devidamente elencada ao longo das seções desta peça, acompanhada das devidas comprovações na documentação anexa, quando necessário.

2. RESUMO DO CASO

Trata-se de procedimento licitatório flagrantemente ilegal que, ademais de descumprir e violar as normas básicas da administração pública, compreende lesão ao erário e a direitos fundamentais. Por se evidenciar **urgência**, dado que o procedimento se encontra em tese apto a ser consumado, passa-se a narrativa objetiva dos fatos.

Por meio do pregão eletrônico nº 3/2021, o Ministério da Justiça e Segurança Pública, pretende 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)*" (**Doc. 06**[2]).

O edital[3] foi tornado público em 7 de maio[4] com previsão de abertura das propostas no dia 19/05/2021, às 10h[5]. De saída, dois aspectos levantam preocupação: **i)** a vagueza e amplitude do objeto, que permitiria a aquisição de recursos voltados à indevido controle e violação de garantias fundamentais e **ii)** o fato de para uma solução tão complexa ter sido escolhido o critério "menor preço por item", por meio de pregão eletrônico, dado que evidentemente não se trata de mero recurso "de prateleira".

---

[2] Documentos disponíveis em https://www.gov.br/mj/pt-br/acesso-a-informacao/licitacoes-e-contratosv1/licitacoes-e-contratos-segen/cglic/cpl/copy64_of_pregoes-02_2021,a cessado em 24 de maio de 2021.

[3] https://www.gov.br/mj/pt-br/acesso-a-informacao/licitacoes-e-contratosv1/licitacoes-e-contratos-segen/cglic/cpl/pregao-2-2021-1/edital_completo.pdf

[4] https://www.gov.br/mj/pt-br/acesso-a-informacao/licitacoes-e-contratosv1/licitacoes-e-contratos-segen/cglic/cpl/copy64_of_pregoes-02_2021

[5] https://www.gov.br/mj/pt-br/acesso-a-informacao/licitacoes-e-contratosv1/licitacoes-e-contratos-segen/cglic/cpl/pregao-2-2021-1/publicacao_abertura_dou.pdf

Um olhar atento ao Termo de Referência constante do edital indica se tratar de solução abrangente, que tenha potencial de coletar grande número de informações sobre as pessoas, inclusive oriundas de redes sociais, o que sugere inclusive a possibilidade de exploração de brechas de segurança:

> 2. Classificar as seguintes entidades: pessoas, grupos, companhias, organizações, páginas web, infraestrutura de internet, frases, documentos, arquivos, dentre outras;
>
> 3. Realizar análise de vínculos;
>
> 6. Buscar informações em redes sociais e sites de busca;
>
> 9. Coletar a geolocalização de postagens (local de origem da postagem);
>
> 10. Coletar responsáveis por postagens (postadores);
>
> 11. Coletar dados demográficos do postador (por exemplo, sexo, idade, estado civil);
>
> 18. Permitir pesquisas em mídias e redes sociais (Facebook, Instagram, Twitter, LinkedIn, etc, fontes abertas, blogs, fóruns e sites da Deep e Dark Web);

Não parece se tratar, portanto, de um inocente recurso que permita a mera agregação de informações disponíveis em fontes abertas, mas sim explorar e coletar massivamente dados, inclusive por meio de brechas de segurança, a fim de instituir amplo e generalizado monitoramento. Mas, mesmo assim, as especificações técnicas (Anexo I) têm menos de 1 página.

Consta do **documento de oficialização da demanda (Doc. 07[6])**, que o objetivo é adquirir "softwares e hardwares que possibilitam a pesquisa de dados em redes de relacionamentos, **aplicativos de chat**, deepweb necessário para análise e produção de conhecimento diário", como será visto adiante.

Esse mesmo documento afirma que

> A Plataforma de Inteligência deverá oferecer os recursos mais abrangentes e avançados de **monitoramento de toda a esfera digital**, permitindo pela primeira vez não só a exposição automatizada de alvos conhecidos, mas também a exposição e identificação de ameaças de baixa assinatura" (g.n.).

Como se sabe, a obtenção de dados de "aplicativos de chat" não é possível por meio de "fontes abertas". Ou seja, uma **solução que seja capaz de interceptar essas mensagens vai muito além de mera coleta de dados em meios que sejam públicos**.

Ainda, afirma-se que se busca uma solução abrangente, que permita "*pela primeira vez*" uma ampla possibilidade de monitoramento. Trata-se, portanto, de evidente **recurso inovador, muito mais poderoso do que o monitoramento que já realizado pelos órgãos públicos.**

Note-se que além de 40 licenças a estarem à disposição da SEOPI em seus "Centros Integrados de Inteligência de Segurança Pública", pretende-se a aquisição de mais 209 outras, sendo 100 delas para a Polícia Federal, 3 delas para o Ministério Público Federal e as demais para diversos outros órgãos estaduais. Há órgãos ali listados que sequer integram as forças de segurança, que não têm poder de polícia, como é o caso do BACEN (para

6 https://www.gov.br/mj/pt-br/acesso-a-informacao/licitacoes-e-contratosv1/licitacoes-e-contratos-segen/cglic/cpl/pregao-2-2021-1/sei_mj-10722651-documento-de-oficializacao-da-demanda-in-01_2019.pdf

quem está prevista a entrega de uma licença). E vale verificar, ainda, que para o Ministério Público do Trabalho estão previstas 5 licenças, enquanto para **40 licenças estão previstas para a Secretaria da Segurança Pública de Brasília (órgão que já foi chefiado pelo atual Ministro).**

Há uma desproporcionalidade total entre as licenças previstas para operar o tal sistema.

O cenário, portanto, é muito preocupante: estamos na iminência de permitir a contratação de recursos tecnológicos, de alto valor, cuja utilização é potencialmente lesiva à direitos fundamentais, dentre eles a privacidade e o devido processo legal. Pior, tal contratação vem em procedimento flagrantemente inadequado para o fim que se propõe.

Esse Ministério da Justiça já atuou em outras oportunidades fora dos cânones legais. Exemplo disso é o lamentável episódio dos "dossiês" elaborados no âmbito da própria SEOPI que mobilizou recursos públicos para coletar dados e informações de pessoas por razões meramente ideológicas.

Pode ser viabilizado, por meio do uso de recursos públicos, caso esse pregão seja homologado, a implantação de aparato vigilantista, nitidamente ilegal.

Os fatos ora narrados já ganharam ampla repercussão nacional. Além da contratação em si (diga-se, em cenário de necessária contenção de despesas e de necessidade de se focalizar recursos no enfrentamento da pandemia e suas consequências), chama atenção o contexto de uma via de vigilância "paralela". Inclusive com participação de agentes políticos estranhos à administração pública federal.

O portal O Antagonista publicou matéria em 18/05/2021 intitulada "*Órgão que fez dossiês de inimigos do governo vai comprar sistema que vasculha redes, aplicativos de chat e dark web*"[7] na qual aponta que:

> O Antagonista apurou que essa "solução de inteligência" será capaz de cruzar informações de mais de 15 mil alvos relacionados, com análise de vínculos e geolocalização de postagens, autoria e responsáveis, assim como dados demográficos de quem postou.
>
> (...)
>
> Chama atenção que a Agência Brasileira de Inteligência (Abin), que exerce a função de coordenação do Sistema Brasileiro de Inteligência (Sisbin), não apareça na lista de beneficiados com licenças de uso do novo sistema.
>
> Também é curioso que, depois da própria Polícia Federal (que terá 100 licenças de uso), o órgão mais beneficiado seja a Secretaria de Segurança Pública do Distrito Federal (com 40 licenças), que era comandada pelo delegado Anderson Torres, antes de ele virar ministro da Justiça e da Segurança Pública.
>
> A concorrência deve atrair grandes empresas do setor, como as israelenses NSO Group, Rafael Advanced Defense Systems e Cognyte, além da sul-africana Paterva.

Por sua vez, o UOL[8] explorou as circunstâncias políticas em torno da contratação, que são no mínimo alarmantes:

[7] https://www.oantagonista.com/brasil/exclusivo-orgao-que-fez-dossies-de-inimigos-do-governo-vai-comprar-sistema-que-vasculha-redes-aplicativos-de-chat-e-dark-web/amp/?__twitter_impression=true&s=08

[8] https://noticias.uol.com.br/politica/ultimas-noticias/2021/05/19/briga-entre-militares-e-carlos-bolsonaro-racha-orgaos-de-inteligencia.htm

> "Uma licitação para a aquisição de uma ferramenta de espionagem expôs a disputa entre o alto comando militar e o vereador carioca Carlos Bolsonaro (Republicanos), o filho "02" do presidente da República, Jair Bolsonaro (sem partido).
>
> Diferentemente de editais semelhantes lançados em outras ocasiões, desta vez órgãos oficiais de investigação que seriam beneficiados diretamente pela ferramenta, como o GSI (Gabinete de Segurança Institucional) e a Abin (Agência Brasileira de Inteligência), não estão envolvidos nas tratativas.
>
> (...)
>
> **'Abin paralela'**
>
> Segundo fontes ouvidas pelo UOL sob a condição de não terem seus nomes e cargos revelados, **o político carioca tenta diminuir o poder dos militares na área de inteligência. Para tanto, articulou junto ao novo ministro da Justiça, Anderson Torres, para excluir o GSI da licitação**.
>
> O órgão, que é responsável pela Abin, é chefiado pelo general Augusto Heleno e tem muitos militares em seu quadro. De acordo com as mesmas fontes, o objetivo final de Carlos Bolsonaro é usar as estruturas do Ministério da Justiça e da PF (Polícia Federal) para expandir uma "Abin paralela", na qual tenha grande influência."

Mais adiante, a reportagem ainda aponta:

> Pegasus
>
> A reportagem teve acesso, com exclusividade, às propostas, ainda sob sigilo, de todos os concorrentes do pregão eletrônico. Fontes que integram o Sisbin (Sistema Brasileiro de Inteligência) enfatizaram a participação da NSO Group, dona do Pegasus, no pregão por meio de um revendedor brasileiro, que fez uma proposta ao edital de R$ 60,9 milhões. O valor, porém, ainda poderá ser reajustado para se enquadrar à quantia estabelecida para a aquisição por 12 meses da nova ferramenta.

> As propostas com valores muito superiores ao previsto pelo edital, como é o caso da empresa Synchronet Telecomunicações Ltda., que fez uma oferta de R$ 1,25 bilhão para o fornecimento do serviço, já foram descartadas de antemão.
>
> **Há o entendimento na ala militar de que o Pegasus possibilita a invasão de celulares e computadores sem indicar o responsável pelo acesso —a facilidade é tamanha que um dispositivo pode ser acessado sem precisar ser ativado pelo usuário, o que membros da inteligência chamam de "zero cliques"**.
>
> Fontes ouvidas pelo UOL afirmam que o maior problema é que, se adquirido, o Pegasus permitirá o monitoramento de pessoas e empresas sem decisão judicial. Ou seja: **o uso da ferramenta dependerá apenas do senso ético de quem controlará o sistema**.
>
> Outro ponto de discórdia entre os militares e Carlos Bolsonaro está no fato de que Anderson Torres não se opõe ao armazenamento de dados e informações por estrangeiros, em especial de empresas com sede na Alemanha ou em Israel.
>
> Alegando questões de segurança nacional, equipes do GSI e da Abin, porém, não abrem mão de que informações oriundas de investigações, enriquecidas com os dados de cidadãos e de empresas nacionais, devam ser exclusivamente armazenadas e processadas no Brasil."

Assim, outro ponto de fundada preocupação é a possibilidade de que a ferramenta contratada seja similar ao famigerado sistema "Pegasus" ou, mesmo, a própria solução de propriedade do NSO Group.

Preocupa pelos diversos relatos de utilização de sistemas como esse contra cidadãos comuns, ativistas e pessoas que simplesmente sejam opositoras ao governo da vez. Há inúmeros relatos de abusos na utilização desses tipos de sistema ao redor do mundo.

No México recentemente foram utilizados recursos similares para perseguição de ativistas, o que se tornou um escândalo internacional para o Governo Peña Nieto[9]:

> O escândalo de espionagem que teve como alvo ativistas, jornalistas e investigadores no México se soma à lista de polêmicas do governo do presidente Enrique Peña Nieto e tem consequências negativas para o seu Partido Revolucionário Institucional (PRI), que buscará um novo mandato nas eleições do ano que vem.
>
> Na última polêmica do governo de Peña Nieto, 19 pessoas, dentre jornalistas, advogados, políticos de oposição, ativistas anticorrupção e investigadores da Comissão Interamericana de Direitos Humanos - que buscavam evidências sobre o desaparecimento de 43 estudantes há três anos - tiveram celulares infectados pelo software de espionagem Pegasus.
>
> O programa é desenvolvido pela empresa israelense NSO e visa permitir o acesso aos celulares, incluindo microfone e câmera, a partir de uma mensagem de texto.

No Marrocos, a utilização ilegal do sistema Pegasus foi destacada pela Anistia Internacional, que documentou detalhadamente os abusos[10]:

> A Anistia Internacional descobriu que, pelo menos desde outubro de 2017, os defensores dos direitos humanos de Marrocos têm sido alvo do infame spyware "Pegasus" produzido pela empresa israelita 'NSO Group'. Este relatório revela como esse spyware foi usado para atingir ilegalmente dois defensores de direitos humanos proeminentes do Marrocos, que têm um histórico de enfrentar represálias do estado por falar abertamente sobre os direitos humanos no país. A Anistia

[9] https://valor.globo.com/mundo/noticia/2017/07/14/caso-de-espionagem-no-mexico-abala-o-governo-pena-nieto.ghtml
[10] https://www.amnesty.org/en/latest/research/2019/10/Morocco-Human-Rights-Defenders-Targeted-with-NSO-Groups-Spyware/

> Internacional pode revelar que os dois alvos são Maati Monjib, acadêmico e ativista que trabalha com questões de liberdade de expressão, e Abdessadak El Bouchattaoui, advogado de direitos humanos envolvido na defesa legal de manifestantes em um movimento de justiça social em Hirak El-Rif que ocorreu entre 2016 e 2017.
>
> Essas revelações são particularmente significativas em um contexto em que as autoridades marroquinas estão cada vez mais usando disposições repressivas de códigos penais e leis de segurança para criminalizar e desacreditar os defensores dos direitos humanos e ativistas por exercerem seus direitos à liberdade de expressão, associação e reunião pacífica. Defensores de direitos humanos marroquinos enfrentaram assédio, intimidação e prisão. Este relatório revela que, pelo menos desde 2017, as autoridades estaduais também têm usado o spyware do Grupo NSO como uma ferramenta para reduzir ainda mais o espaço para a realização de trabalhos de direitos humanos, visando defensores de direitos humanos."

Ano passado, tornou-se público que um jornalista estadunidense do New York Times foi alvo de um ataque semelhante vindo da Arábia Saudita, mostrando inclusive o alcance internacional desse tipo de ferramenta[11]:

> Um jornalista do New York Times recebeu um spyware vinculado à Arábia Saudita e incorporado em uma mensagem de texto de 2018 em seu celular - o primeiro jornalista americano conhecido por ter sido alvo de tal malware no que parece ser uma ameaça global crescente para jornalistas, dissidentes e humanos ativistas de direitos humanos, de acordo com um novo relatório.

[11] https://www.washingtonpost.com/national-security/a-new-york-times-journalist-was-targeted-by-spyware-linked-to-saudi-arabia-according-to-report/2020/01/28/f603f36c-41dc-11ea-b5fc-eefa848cde99_story.html

> O jornalista, Ben Hubbard, soube da tentativa de hackear seu telefone em outubro de 2018, enquanto cobria uma história sobre um dissidente saudita no Canadá visado pelo mesmo spyware Pegasus, de acordo com o Citizen Lab da Escola Munk da Universidade de Toronto, que escreveu o relatório.
>
> O malware foi criado por uma empresa israelense, NSO Group, que é o foco de um escrutínio intensificado sobre o suposto uso de seus produtos por governos autoritários para atacar oponentes, disse o relatório.

Por fim, há relatos[12] de investigações do FBI estadunidense sobre o uso de ferramentas desse tipo para investigação não apenas de pessoas privadas como também de governos, o que sugere que nem mesmo autoridades e órgãos públicos estão a salvo de ataques do tipo:

> ***FBI investiga uso de spyware israelense para invadir dados de pessoas e governos***
>
> O FBI está investigando a participação da empresa israelense fabricante de criadora de spyware NSO Group Technologies em possíveis invasões de empresas e cidadãos norte-americanos, bem como a suspeita de coleta de dados de governos, segundo quatro pessoas familiarizadas com o inquérito.
>
> A investigação estava em andamento em 2017, quando funcionários do FBI tentavam descobrir se a NSO obteve de hackers norte-americanos qualquer código necessário para infectar smartphones, disse uma pessoa entrevistada pelo FBI à época e de novo em 2019.

12 https://forbes.com.br/negocios/2020/01/fbi-investiga-uso-de-spyware-israelense-para-invadir-dados-de-pessoas-e-governos/

Fazendo coro ao alegado, encerramos o relato mencionando centros de pesquisa internacionais muito respeitados como a *Red en Defensa de los Derechos Digitales* (R3D), sediada no México[13] e a *CitzenLab*[14] sediada no Canadá possuem farto material sobre o tema.

Por outro lado, não passou despercebida a nota do Ministério da Justiça e Segurança Pública que, em tom anomalamente agressivo[15], tachou de "mentirosas" reportagens dos portais O Antagonista e UOL. A leitura atenta da nota não trouxe nenhum elemento adicional que afaste as preocupações levantadas: o fato de a licitação ter sido iniciada em 2020 e a afirmação genérica de que não se pretende adquirir a ferramenta "Pegasus" infelizmente não infirmam o ora alegado.

A recente difusão epidêmica de sistemas de coleta de informação tão abrangentes e agressivos se mostra especialmente graves, já que a coletividade - inclusive autoridades públicas e companhias - poderão ser monitoradas, devassadas e seus dados comprometidos independentemente de ordem judicial ou ulterior responsabilização dos agentes perpetradores.

Em suma, estamos diante de contratação ilegal, por via inadequada, de sistema potencialmente lesivo à coletividade, que permitirá coleta indiscriminada e indevida de informações, inclusive podendo servir a interesses políticos escusos.

É por essa razão que as peticionárias vêm diante desse e. Tribunal de Contas da União requerer a imediata suspensão do certame.

---

[13] https://r3d.mx/tag/pegasus/
[14] https://citizenlab.ca/tag/pegasus/
[15] https://www.gov.br/mj/pt-br/assuntos/noticias/reportagens-do-201cuol201d-e-201co-antagonista201d-mentem-sobre-licitacao-do-ministerio-da-justica-e-seguranca-publica

3. DAS IRREGULARIDADES DO PROCESSO LICITATÓRIO

3.1 Da inadequação da modalidade pregão

O objeto da licitação é claramente um programa/sistema/software para monitoramento de redes sociais e produção de informações.

O que o Edital chama de "Solução de Inteligência em Fontes abertas, Mídias Sociais, Deep e Dark Web", na verdade é um **serviço em Tecnologia da Informação** (um sistema que vai percorrer diferentes plataformas reunindo dados e informações sobre pessoas).

Este Tribunal de Contas tem jurisprudência consolidada sobre esse tipo de serviço, que culminou com a Nota Técnica TCU 02/2008, sobre o uso do Pregão para aquisição de bens e serviços de Tecnologia de Informação, que compilou os seguintes entendimentos:

> **- Entendimento I.** A licitação de bens e serviços de tecnologia da informação considerados comuns, ou seja, aqueles que possuam padrões de desempenho e de qualidade objetivamente definidos pelo edital, com base em especificações usuais no mercado, deve ser obrigatoriamente realizada pela modalidade Pregão, preferencialmente na forma eletrônica.
>
> **- Entendimento II.** Devido à padronização existente no mercado, os bens e serviços de tecnologia da informação geralmente atendem a protocolos, métodos e técnicas pré-estabelecidos e conhecidos e a padrões de desempenho e qualidade que podem ser objetivamente definidos por meio de especificações usuais no mercado. Logo, via de regra, esses bens e serviços devem ser considerados comuns para fins de utilização da modalidade Pregão.

Fora do que deve ser considerado *"software de prateleira"*, portanto (em que há uma padronização dos bens e serviços pelo mercado),

há necessidade de se seguir o previsto no §4º do art. 45 da Lei nº 8.666/1993, para que seja possível a comparação de fatores técnicos (o que exige uma licitação que contemple a análise técnica).

É isso que está previsto também no art. 9º do Decreto 7.174/2010, que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal:

> **Art. 9°** (...)
>
> **§2°** Será considerado comum o bem ou serviço cuja especificação estabelecer padrão objetivo de desempenho e qualidade e for capaz de ser atendida por vários fornecedores, ainda que existam outras soluções disponíveis no mercado.
>
> (...)
>
> **§4°** A licitação do tipo técnica e preço será utilizada exclusivamente para bens e serviços de informática e automação de natureza predominantemente intelectual, justificadamente, assim considerados quando a especificação do objeto evidenciar que os bens ou serviços demandados requerem individualização ou inovação tecnológica, **e possam apresentar diferentes metodologias, tecnologias e níveis de qualidade e desempenho**, sendo necessário avaliar as vantagens e desvantagens de cada solução.

Os *softwares* objeto do edital claramente não são serviços "comuns", demandando licitação pela modalidade de técnica e preço.

Em primeiro lugar, note-se que para aquisição de uma ferramenta

de segurança que terá o poder de interferir na esfera de privacidade dos cidadãos, não pode conter termos tão genéricos como os que constam do edital em questão.

Não se pode verificar, pelas questões técnicas apresentadas, se o software/sistema será seguro o suficiente para evitar que a empresa contratada monitore, por exemplo, as atividades que estarão sendo realizadas pelas forças de segurança.

A aquisição de um programa com as funcionalidades prometidas, que representa uma ferramenta estratégica e sensível por parte da administração pública, especialmente se destinada a atividades de inteligência e segurança pública, não pode ser feita sem análise técnica.

Realizá-la a partir apenas do critério de preço representa inadequação flagrante.

O tema é estratégico e sensível o suficiente para que a aquisição considere a análise de critérios técnicos, que neste caso deveriam abranger parâmetros de segurança da informação e boas práticas de sistemas de informação. Isto colocaria em grau superior de proteção a confiabilidade, segurança e integridade do programa a ser adquirido e os dados e informações tratados a partir de seu funcionamento. A compra realizada desta maneira representa enorme risco à segurança da informação das atividades empreendidas pelos órgãos da Administração Federal envolvidos (já que não atentar para a confiabilidade do código do sistema a ser adquirido, por exemplo, pode significar imensa vulnerabilidade que permita um hacker ver o que o governo está fazendo com ele).

E essa é até uma questão lógica: se esse tipo de tecnologia estivesse à disposição do mercado, de forma generalizada e padronizada, certamente já não seria mais útil para o fim a que se destina, relacionado à segurança pública (pois a burla a esse tipo de ferramenta já seria por demais conhecida)[16].

E com a alteração de políticas de extração de dados de redes sociais do Facebook, Instagram e Twitter, por exemplo, retirando de suas APIs grande parte de seu *data stream*, se tornou raro no mercado a oferta de *softwares* capazes de extrair dados conforme especificação presente no edital e que cumpram as especificações técnicas descritas no ANEXO I do edital. **Cada empresa terá, portanto, uma metodologia, uma tecnologia e qualidade de desempenho distintas, a exigir uma necessária análise técnica que não é possível pela via do pregão.**

3.2 Da usurpação de competência e da violação do princípio da legalidade

Outra questão que salta aos olhos, apontada pelas reportagens acima referidas, é a **incompetência do órgão do Ministério da Justiça para a aquisição e usufruto da tecnologia ora em discussão**, parecendo haver usurpação da competência da Agência Brasileira de Inteligência (ABIN), sujeita às Forças Armadas.

O instrumento convocatório aponta como **beneficiária direta da aquisição** a **Diretoria de Inteligência da Secretaria de Operações**

[16] "A aquisição está vinculada ao Programa de Combate ao Crime Organizado (PACCO), projeto estratégico do Ministério da Justiça e Segurança Pública que tem por objeto o apoio aos entes federados na repressão ao crime organizado," afirma o secretário de Operações Integradas, Alfredo Carrijo. Disponível em https://www.gov.br/mj/pt-br/assuntos/noticias/reportagens-do-201cuol201d-e-201co-antagonista201d-mentem-sobre-licitacao-do-ministerio-da-justica-e-seguranca-publica, acessado em 22 de maio de 2021.

Integradas. A competência desta diretoria está definida no Decreto n. 9.662 de 1º de janeiro de 2019, onde se lê:

> 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;

Não é razoável o entendimento de que o *software* em questão (que vai monitorar redes sociais e fornecer informações sobre cidadãos) pode servir a órgão cujo papel está ligado a **aspectos institucionais da formulação e gestão das políticas de segurança pública**. O órgão não possui legitimidade para funcionar investido do poder de polícia do Estado, e portanto, não tem legitimidade para contratar esse tipo de serviço para atender às "suas necessidades".

As polícias e, subsidiariamente, a ABIN, ligada às Forças Armadas, esses sim constituem órgãos integrantes da Administração Pública que, por sua natureza, desenvolvem atividades investigativas e de inteligência, fazendo jus a esse tipo de solução.

A dissociação entre o que Edital 3/2021 visa adquirir e as competências da DINT/SEOPI fica ainda mais evidente se confrontados com a competência atribuída à ABIN pela Lei n. 9.883/1999:

> 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.

Diferentemente da competência apontada para a DINT/SEOPI, constante no Decreto 9.662/2019, o artigo acima é explícito ao incluir, dentre as competências da ABIN a obtenção e análise de dados. Esse contraste evidencia que a aquisição das referidas "soluções" para o órgão do Ministério da Justiça representa flagrante **usurpação** da competência da ABIN que está, essa sim, investida do Poder de Polícia do Estado, para agir nas situações excepcionais de suspensão do direito à privacidade, **nos limites estritos impostos pela autoridade judiciária** e sob o controle próximo do Ministério Público, a quem incumbe o controle externo da atividade policial.

A DINT/SEOPI não foi imbuída pela Lei do poder de polícia do Estado, restando evidente que suas competências não justificam a aquisição de tão específica e perigosa ferramenta tecnológica, demonstrando flagrante irregularidade no certame questionado.

Importante ressaltar que pela força do princípio da legalidade, sob cuja autoridade inexorável deve operar toda a Administração Pública, não é possível fazer uma interpretação extensiva de um tal rol de competências, notadamente, quando a interpretação resulta em autorizar atividades que implicam na invasão à esfera privada dos administrados, como parece ser o caso do monitoramento de redes sociais e mensagens em *chats* privados.

O sentido do princípio da legalidade para os cidadãos é de garantir a liberdade para fazer tudo aquilo que não seja restrito por lei. Para a Administração Pública o princípio funciona em sentido inverso, justamente para defender os indivíduos de arroubos autoritários do Estado. A Administração Pública só pode agir na estrita medida do que a lei permite fazê-lo.

E vale lembrar também que **esse Ministério da Justiça vem de um histórico de diversos atos de perfilamento e monitoramento da sociedade civil**, fatos levados ao Supremo Tribunal Federal e tidos como ilegais. Como será visto adiante, há fortes indícios de que há **desvio de finalidade** que justifica essa usurpação de competência, com o objetivo da criação de uma "ABIN paralela", como foi mencionado nas reportagens.

3.3 Da ilicitude do objeto

3.3.1 Perfilamento e vigilantismo pela Administração Pública: comportamento incompatível com o Estado Democrático de Direito.

Por óbvio, o objeto de qualquer licitação tem que ser lícito.

A intimidade e vida privada dos indivíduos são protegidos de maneira autônoma pela Constituição Federal, notadamente pelo seu art. 5º, inciso X. Esses valores existenciais da pessoa humana são definidos como *"uma esfera íntima da pessoa, na qual a conduta do sujeito ou sua família não influencia sobre os demais e os demais podem influenciar sobre ela"*[17] e derivam dos princípios da legalidade (art. 5º, II, CF), da inviolabilidade do direito à liberdade (art. 5º, caput, CF) e da dignidade da pessoa humana (art. 1º, CF), além das manifestações concretas desta por meio da expressão do pensamento (art. 5º, IV, CF), inviolabilidade da liberdade de consciência e da crença (art. 5º, VI, CF), dentre outras.

No âmbito infraconstitucional, diversos instrumentos jurídicos visam materializar a proteção da intimidade, da vida privada, honra e imagem dos cidadãos, mormente a Lei nº 12.737/2012 (Lei Carolina Dieckmann), a Lei nº

[17] LORENZETTI, Ricardo Luis. Fundamentos do direito privado. Trad. Vera Maria Jacob de Fradera. São Paulo: RT, 1998, p. 492.

12.965/2014 (Marco Civil da Internet) ou a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados).

Esses direitos são tão caros aos institutos democráticos que carregam substancioso respaldo internacional. Em consequência, diversas declarações, pactos e convenções internacionais sobre os direitos humanos protegem, de maneira independente, o direito à intimidade e à vida privada. Cita-se, nesse sentido, o art. 12 da Declaração Universal de Direitos Humanos, o art. 5º da Declaração Universal dos Direitos Humanos, o art. 17 do Pacto das Nações Unidas sobre Direitos Civis e Políticos, o art. 11 da Convenção Americana de 1969 sobre os Direitos do Homem e o art. 8º da Convenção Europeia de 1950 sobre os Direitos do Homem.

O direito à intimidade e à vida privada são indissociáveis do Estado Democrático de Direito. **A coleta discricionária de dados pessoais, para fins de perfilamento da população, apenas se sustenta em um Estado repressivo**, que promove recolhimento de informações privadas para promoção de medidas discricionárias que desrespeitem direitos fundamentais.

A interferência que se busca com a licitação em questão remonta ao nefasto período ditatorial militar que se iniciou em 1964, no qual vigorava o antigo Serviço Nacional de Informações (SNI)[18]. À época, o SNI armazenava dados pessoais dos indivíduos, especialmente opositores políticos. Vejamos ensinamento do Ministro LUÍS ROBERTO BARROSO:

> Inicialmente, tais dados [informações sobre a vida privada dos cidadãos], muitas vezes obtidos de forma ilegal, forneciam a matéria-prima que alimentava a perseguição política, mesmo

[18] LIMA, Jesus Costa. Comentários às súmulas do Superior Tribunal de Justiça. 2. ed. Brasília Jurídica, 1993. v. 1, p. 38.

> quando não havia qualquer imputação formal de violação da ordem jurídica. Mais à frente, na crescente patologia das ditaduras desgastadas, o uso indevido de informações comprava o silêncio e a adesão dos dissidentes do próprio regime, sob a ameaça de escândalos familiares e de publicidade de fatos da vida privada. Logo cedo, a ideia de um 'serviço de inteligência' voltado, elevadamente, para a segurança do Estado esvaiu-se em tropicalismos diversos. Envolvendo-se na política ordinária, os órgãos de segurança mergulharam em terreno pantanoso, operando frequentemente nas fronteiras da marginalidade. A chamada 'comunidade de informações' passou a constituir um poder paralelo e agressivo, que, por vezes, sobrepunha-se ao poder político institucional, valendo-se de meios ilícitos para fins condenáveis[19].

O sistema constitucional brasileiro opõe-se firmemente a essas práticas pelo Estado. **O direito à intimidade e privacidade dos jurisdicionados é fundamento de justificação e estruturação do Estado Democrático de Direito**.

Conforme apontado por JOSÉ AFONSO DA SILVA:

> A tarefa fundamental do Estado democrático de Direito consiste em superar as desigualdades sociais e regionais e instaurar um regime democrático que realize a justiça social.[20]

Assim, o Estado que se diz democrático e de direito impõe a participação efetiva e operante do povo na coisa pública; para além da formação das instituições representativas[21].

Nesse sentido, o conceito de Estado democrático de direito apenas se

[19] BARROSO, Luís Roberto. O direito constitucional e a efetividade de suas normas, 6. ed. atualizada. Rio de Janeiro: Renovar, 2002.
[20] SILVA, José Afonso da. *Curso Direito Constitucional Positivo*. São Paulo: Malheiros, 1994, p.110.
[21] SILVA, José Afonso Da. O Estado Democrático de Direito. Revista Dir. adm, Rio de Janeiro, 173: 15-34. Jul/set 1988.

realiza a partir do controle do poder estatal baseado na separação de poderes e na adoção dos direitos de liberdade. Essa noção é revisitada muito antes da construção teórica de democracia nos moldes atuais, eis que cunhada a partir do "Estado de direito" – conhecido como primeiro Estado jurídico –, expressado pela materialização das revoluções espirituais e racionalistas do século XVIII protagonizadas pela burguesia europeia[22].

Ao mesmo tempo, é reconhecido a todos os países o exercício da defesa nacional, inclusive por meio do monitoramento de pessoas, coleta e análise de dados, e tratamento de informações. Nessa esteira, a atividade de inteligência brasileira foi criada, a partir do exercício e ações especializadas, voltadas para *"a produção e difusão de conhecimentos, com vistas ao assessoramento das autoridades governamentais nos respectivos níveis e áreas de atribuição, para o planejamento, a execução, o acompanhamento e a avaliação das políticas de Estado"*.

Essas ações de vigilância e inteligência apenas são protegidas pela legalidade **quando pautadas nos princípios e mandamentos constitucionais, observadas também as leis ordinárias**. Conforme bem pontuado pela **Ministra Carmen Lúcia no julgamento da ADPF 722**:

> A República não admite catacumbas, a democracia não se compadece com segredos, a não ser para se lembrar de situações que precisamos ter como superadas (...) Direitos fundamentais não são concessões estatais, são garantias aos seres humanos conquistadas antes e para além do Estado, e seu objetivo é

[22] BONAVIDES, Paulo. Do Estado Liberal ao Estado Social. – 8ª ed. – São Paulo: Maleiros Editores, 2004.

possibilitar o sossego pessoal e a dignidade individual[23].

Não pode ser considerada legítima a atuação de órgãos estatais que, sob o pretexto de cuidar da atividade de monitoramento, inteligência ou vigilância, investiguem, sem observar o devido processo legal, cidadãos brasileiros.

A vigilância e monitoramento de pessoas devem observar os princípios constitucionais pertinentes, sob pena de colocar-se em risco a própria democracia brasileira. É necessário que a máquina pública seja utilizada para neutralizar ameaças reais à segurança do país. E ainda mais imperativo é o reconhecimento de que as hipóteses de flexibilização do direito à vida privada e intimidade são excepcionais, **eis que se trata de um direito constitucionalmente garantido.**

Nesse sentido, nenhuma instância estatal – nem os serviços prestados pelo Sistema Brasileiro de Inteligência, responsáveis por operações de monitoramento – pode escusar-se de controle de legalidade, interno e externo. Por isso mesmo o parágrafo único do art. 3º Lei 9.883/1999 estabelece que o objetivo do Sistema se relaciona com a salvaguarda e a segurança da sociedade e do Estado (§2º, art.1 da Lei 9.883/1999), com **irrestrita** observância dos direitos e garantias individuais, fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado.

É nesse sentido que o Supremo Tribunal Federal, no âmbito da ADPF 722, asseverou:

[23] ADPF 722 MC, Relator(a): CÁRMEN LÚCIA, Tribunal Pleno, julgado em 20/08/2020, PROCESSO ELETRÔNICO DJe-255 DIVULG 21-10-2020 PUBLIC 22-10-2020)

> O serviço de inteligência do Estado para segurança pública, para a segurança nacional e para a garantia de cumprimento eficiente dos deveres do Estado é necessário, como antes lembrado por este Supremo Tribunal e é tema mais que sensível. Não pode ser desempenhado fora de estritos limites constitucionais e legais, sob pena de comprometer a democracia em sua instância mais central, que é a de garantia dos direitos fundamentais.
>
> Por isso é certo que órgãos de inteligência de qualquer nível hierárquico de qualquer dos poderes do Estado submetem-se também ao crivo do Poder Judiciário porque podem incorrer em desbordamentos legais. E, note-se, até mesmo atos do Judiciário são examinados e decididos, em sua validade constitucional e legal à luz do direito, como se teve há pouco na arguição de descumprimento de preceito fundamental 572[24].

Ainda naquela oportunidade, o STF prelecionou:

> Direitos fundamentais não podem ser objeto de ameaça ou lesão, nos termos constitucionalmente estampados. Nem o Judiciário atua para reparar direitos, senão quando não há mais via jurídica adequada para impedir o dano. O que se busca é que lesões a direitos fundamentais não ocorram, não persistam, não possam ser praticados. O Estado não pode ser infrator. Menos ainda em afronta a direitos fundamentais, que é sua função garantir e proteger. No Estado de direito tem o Poder Judiciário o dever de impedir, quando convocado, ameaça ou lesão a direito.

Desse modo, a proteção à vida privada deve balizar os atos administrativos. A atuação do Poder Público deve ser **transparente**, **norteada pela legalidade, e garantidora de direitos**. O monitoramento não é, **e não deve ser**, a regra geral do Poder Público. As bases de um Estado

[24] ADPF 722 MC, Relator(a): CÁRMEN LÚCIA, Tribunal Pleno, julgado em 20/08/2020, PROCESSO ELETRÔNICO DJe-255 DIVULG 21-10-2020 PUBLIC 22-10-2020)

Democrático de Direito não são a vigilância, o perfilamento de cidadãos, a invasão da privacidade - ao contrário, **as bases da legalidade estão fincadas na proteção de direitos fundamentais e a garantia da intimidade e vida privada dos jurisdicionados**.

E é justamente por isso que não se pode admitir a efetivação da referida compra intentada pela Administração Pública.

A definição do objeto da licitação é mantido em **termos convenientemente vagos**, tornando quase impossível, por exemplo, precisar que propriedades seriam demandadas dessas "soluções" em mídias sociais, *deep* e *dark web*, e para quais finalidades elas precisam estar aptas a operar.

Ainda no edital, o órgão oferece a seguinte justificativa para a aquisição de tais "soluções":

> 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.

Assim como na descrição do objeto da licitação, a justificativa oferecida para a aquisição é repleta de expressões vagas, cujo emprego pouco ajuda a compreender **1)** quais as propriedades específicas buscadas nas "soluções" que se objetiva adquirir e **2)** que finalidades estão incluídas

em expressões vagas como “ganho em requisitos de performance e segurança”, “maior capacidade de desempenho”, “eficiência e celeridade”.

Ora, sabe-se que *softwares* da natureza descrita no instrumento convocatório constituem ferramentas potencialmente destinadas à realização de serviços de espionagem e vigilância de indivíduos em suas redes sociais.

A descrição das funcionalidades enviadas aos licitantes é reveladora em um dos esclarecimentos solicitados por uma das empresas por meio do sistema de pregão eletrônico no site Compras.Net, do Governo Federal.

Na oportunidade, em esclarecimento enviado no dia 17 de maio de 2021, às 17:28, o licitante indagou o pregoeiro a respeito da extensão das funcionalidades pretendidas pelo órgão. A descrição é, a um só tempo, preocupante e evidenciadora do grau em que a presente licitação extrapola a legalidade:

> **Esclarecimento** 17/05/2021 17:28:57
>
> Pedido de Esclarecimento 5 Prezados, boa noite. Segue pedidos de esclarecimentos referente ao PE 03/2021. São eles: 1) Item 6. **Buscar informações em redes sociais e sites de busca; Item 10. Coletar responsáveis por postagens (postadores); Item 11. Coletar dados demográficos do postador (por exemplo, sexo. idade, estado civil); Item 18. Permitir pesquisas em mídias e redes sociais (Facebook, Instagram, Twitter, LinkedIn, etc, fontes abertas, blogs, fóruns e sites da Deep e Dark Web)**; Q: Pelo exposto, entendemos que deverá ser entregue módulo ou ferramenta adequada para monitoramento em redes sociais, a fim de realizar pesquisas avançadas em tais fontes, obtendo assim melhores resultados. Está correto nosso entendimento? 2) Item 9. **Coletar a**

> **geolocalização de postagens (local de origem da postagem); Item 11. Coletar dados demográficos do postador (por exemplo, sexo, idade, estado civil);** Q: Entendemos que, independentemente da solução existente no mercado, todas terão dificuldades de pleno atendimento aos itens da forma que está escrito. Nem mesmo a solução Maltego, um dos maiores fabricantes do seguimento, já que poucas fontes de coleta detêm informações como local de origem da postagem, idade e estado civil, por exemplo. Portanto, entendemos que a ferramenta fornecida deve possuir a funcionalidade desde que exista a informação na fonte e esteja disponível para coleta. Está correto nosso entendimento?[25]

Os esclarecimentos são necessários porque **o Anexo I, que são as especificações técnicas, tem menos de 1 página...**

Mais revelador da verdadeira intenção dessa contratação, é o DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA (que explicita a necessidade da contratação por trás da licitação) (**Doc. 07**).

Ali está afirmado que a ferramenta a ser contratada deverá **possibilitar a pesquisa de dados em aplicativos de chat**, com análise e produção de **conhecimento diário**.

[25] BRASIL. Compras Gov. Esclarecimentos enviados pelos licitantes anteriormente ao início do pregão. Disponível em: http://comprasnet.gov.br/livre/Pregao/avisos1.asp?prgCod=933821&Origem=Avisos&Tipo=E. Acesso em 20 de mai 2021.

IDENTIFICAÇÃO DA DEMANDA

Nome do Projeto: Solução de Inteligência em Fontes abertas, Mídias Sociais, Deep e Dark Web.

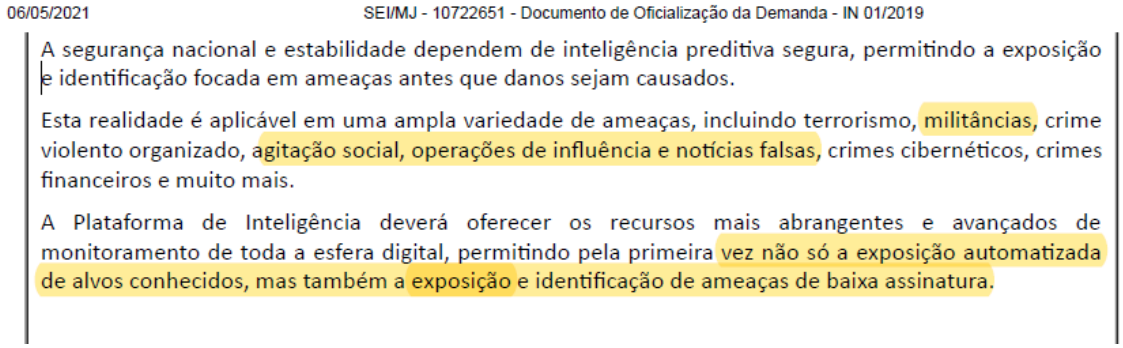
Trata-se de solução formada por softwares e hardwares que possibilitam a pesquisa de dados em redes de relacionamentos, aplicativos de chat, deepweb necessário para análise e produção de conhecimento diário realizado no Centro Integrado de Inteligência de Segurança Pública Nacional - CIISPN e nos Centros Integrados de Inteligência de Segurança Pública Regionais - CIISPRs.

Na era da globalização e anonimato, agências de inteligência e serviços de segurança no mundo todo enfrentam um cenário de riscos complexos.

https://sei.mj.gov.br/sei/controlador.php?acao=documento_imprimir_web&acao_origem=arvore_visualizar&id_documento=12439856&infra_siste... 1/6

Aplicativos de chats não são dados públicos. São dados que dependem de invasão da esfera privada, o que nos termos da Constituição e da Lei, só poderiam ser realizados a partir de autorização judicial. E se é algo que só pode ser feito a partir da existência de uma investigação, esse monitoramento não pode ser diário, como o documento referência menciona, sob pena de não ser ferramenta para contribuir com uma investigação criminal existente, mas de se tornar uma **ferramenta de investigação especulativa**, o que é proibido no ordenamento jurídico brasileiro.

E a intenção de perfilamento e vigilantismo, bem como de monitorar cidadãos em suas redes sociais ficam evidentes na identificação da demanda:



06/05/2021 SEI/MJ - 10722651 - Documento de Oficialização da Demanda - IN 01/2019

A segurança nacional e estabilidade dependem de inteligência preditiva segura, permitindo a exposição e identificação focada em ameaças antes que danos sejam causados.

Esta realidade é aplicável em uma ampla variedade de ameaças, incluindo terrorismo, militâncias, crime violento organizado, agitação social, operações de influência e notícias falsas, crimes cibernéticos, crimes financeiros e muito mais.

A Plataforma de Inteligência deverá oferecer os recursos mais abrangentes e avançados de monitoramento de toda a esfera digital, permitindo pela primeira vez não só a exposição automatizada de alvos conhecidos, mas também a exposição e identificação de ameaças de baixa assinatura.

O Ministério da Justiça classifica como "ameaças" (ao lado de terrorismo ou crimes violentos), a atividade de *militância*, *operações de influência* e *notías falsas*. Ora, o que são esses conceitos? Nenhum deles está definido como crimes ou ilícitos.

Numa lógica bem própria de governos autoritários, o Ministério da Justiça usa expressões vagas, que podem servir para investigar a sociedade civil, num arroubo antidemocrático que lembra bastante a doutrina de segurança nacional.

O fundamento dessa doutrina era a noção de guerra total, isto é, uma noção de conflito ilimitado, tanto temporalmente - na medida em que é permanente - quanto no que diz respeito à identificação dos inimigos, porque envolve todos os setores da sociedade. Deixa-se de tratar somente da defesa contra ameaças externas, **voltando o Estado e seu aparato repressivo contra seus próprios cidadãos e cidadãs[26]. É o que temos aqui.**

A potencial adoção de um sistema que possibilitaria a coleta de dados **sensíveis e privados** dos cidadãos de forma anônima (pela via da espionagem), sem dar conhecimento sobre o destino e o uso dos seus dados, está em completa violação ao princípio da autodeterminação informativa, que é garantido pela Lei Geral de Proteção de Dados.

E permitir a aquisição de *software* voltado para a espionagem de cidadãos sem justificativa robusta e por órgão cujas atribuições rotineiras

[26] TIBOLA, Ana Paula Lima. **A Escola Superior de Guerra e a Doutrina de Segurança Nacional (1949-1966).** Dissertação. Disponível em: <http://www.funag.gov.br/ipri/btd/index.php/10-dissertacoes/3800-a-escola-superior-de-guerra-e-a-doutrina-de-seguranca-nacional-1949-1966> Acesso em: 25 mar 2021.

não envolvem o monitoramento ou tratamento e análise de dados é uma afronta grave a direitos fundamentais.

Pior: esse é um precedente que, dentro da conjuntura atual brasileira, oferece perigo à própria estabilidade democrática, eis que salta aos olhos a sistematicidade do vigilantismo e do monitoramento ilegal perpetrado pela Administração Pública Federal nos últimos tempos.

Há pouquíssimo tempo foi noticiado que esse Ministério da Justiça e Segurança Pública teria formulado dossiê com nomes, fotografias e endereços de redes sociais de 579 servidores federais e estaduais de segurança e três professores universitários integrantes do movimento antifascista, poucos dias depois da divulgação, no dia 5 de junho, de um manifesto intitulado *"Policiais antifascismo em defesa da democracia popular"*, subscrito por 503 servidores da área de segurança, aposentados e na ativa, incluindo policiais civis e militares, penais, rodoviários, peritos criminais, papiloscopistas, escrivães, bombeiros e guardas municipais[27].

Além disso e ao mesmo tempo, foi noticiado a utilização, pelo Poder Público, da tecnologia de inteligência artificial Córtex, que usa a leitura de placas de veículos por milhares de câmeras viárias espalhadas por rodovias, pontes, túneis, ruas e avenidas país afora para rastrear alvos móveis em tempo real e acessar, em poucos segundos, diversos bancos de dados com informações sigilosas e sensíveis de cidadãos e empresas, como a Rais, a Relação Anual de Informações Sociais, do Ministério da Economia. Assim, a poucos cliques, oficiais podem ter acesso a dados cadastrais e trabalhistas

[27] Cf: <https://noticias.uol.com.br/politica/ultimas-noticias/2020/08/18/uol-explica-o-que-e-quem-fez-e-quem-atinge-o-dossie-antifascista.htm>

que todas as empresas têm sobre seus funcionários, incluindo RG, CPF, endereço, dependentes, salário e cargo[28].

Não procede, portanto, no escopo da legalidade e da probidade administrativa, que a DINT/SEOPI licite tecnologia **que permita o monitoramento das redes, a violação do direito ao sigilo de dados de maneira geral, sem ordem judicial, sem individualização dos alvos e sem a especificação dos objetos de investigação**.

O comportamento desse Ministério da Justiça é sistemático e temerário, violando frontalmente dispositivos constitucionais, o que deve conduzir à atuação enérgica e imediata deste Tribunal de Contas.

3.4 Do possível desvio de finalidade.

Ainda que o objeto fosse lícito (o que se afirma apenas para efeito de argumentação), as reportagens mencionadas no preâmbulo desta denúncia sugerem que se trata de uma fachada para contratar um produto ilícito.

Segundo verificaram pelo menos 2 fontes distintas, o produto a ser contratado iria além daquilo que está descrito no Edital.

O fato do Anexo I – Especificações Técnicas ser absolutamente vago e estar descrito em pouco menos de uma página (para assentar a parte técnica de objeto aparentemente complexo), pode significar que as reportagens efetivamente apuraram corretamente e o que se pretende é a construção de uma Abin paralela a partir do Ministério da Justiça para perfilamento, vigilantismo e perseguição de opositores do atual governo.

[28] Cf: <https://theintercept.com/2020/09/21/governo-vigilancia-cortex/>

Como destacado pelo Ministro Luiz Fux em voto condutor na Ação Direta de Inconstitucionalidade n. 5.468 (DJe de 1.8.2017)

> o desvio de finalidade tem como referência conceitual a ideia de deturpação do dever-poder atribuído a determinado agente público que, embora atue aparentemente dentro dos limites de sua atribuição institucional, mobiliza a sua atuação à finalidade não imposta, ou não desejada pela ordem jurídica, ou pelo interesse público[29].

Esse é o mesmo posicionamento da doutrina especializada, que entende o desvio de finalidade como um vício de ato administrativo, demonstrado na ação estatal voltada à satisfação de finalidade alheia à natureza do ato, eis que o agente busca finalidade incompatível com o interesse público (Celso Antônio Bandeira de Mello, Curso de Direito Administrativo, cit., 29a ed., p. 410). Uma das manifestações mais típicas do desvio de finalidade é a utilização dos poderes públicos para benefício próprio ou em prejuízo de inimigos políticos.

No caso em apreço, o Ministério da Justiça tenta adquirir, por meio licitatório, *software* voltado à espionagem de cidadãos, sem qualquer justificativa pertinente e inobservando as regras jurídicas que pautam a atividade de vigilância no país.

Conforme detalhado no tópico anterior, as ações de monitoramento, quando indiscriminadas, não são acomodadas pelo Estado Democrático de Direito. Todas as atividades de vigilância, análise de dados e monitoramento - que, a propósito, são atribuídas pelo sistema jurídico ao Sistema Brasileiro de Inteligência - **apenas se justificam quando imprescindível à segurança**

[29] ADI 5468, Relator(a): LUIZ FUX, Tribunal Pleno, julgado em 30/06/2016, PROCESSO ELETRÔNICO DJe-169 DIVULG 01-08-2017 PUBLIC 02-08-2017

da sociedade e do Estado, devendo, em qualquer hipótese, a teor do parágrafo único do art. 3º Lei 9.883/1999, observar, de maneira **irrestrita**, os direitos e garantias individuais, a fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado.

A utilização da máquina estatal, com aporte substancial de dinheiro público, para fins manifestamente ilegais - vigiar cidadãos e monitorar comportamentos -, é inaceitável, contrastando com o interesse público. A finalidade do ato, que deve ser dirigida para a construção do bem comum, passa a ser desviada, permeando interesses individuais, escusos e ocultos. É a clara configuração do desvio de finalidade.

Note-se que, conforme assevera DANIEL WUNDER HACHEM, "*por mais paradoxal que possa parecer, o interesse público serve para legitimar e, simultaneamente, para limitar o exercício do poder*"[30]. Ou seja, o Poder Público apenas age legitimamente quando a sua atuação está alinhada com o interesse público, pois este elemento condiciona o agir da Administração, dando-lhe a tônica e a finalidade, e estabelecendo uma condição negativa de validade dos atos administrativos.

E a doutrina mais especializada - dentre eles DANIEL WUNDER HACHEM, ENEIDA DESIREE SALGADO, JUAREZ FREITAS e ROMEU FELIPE BACELLAR FILHO[31] - assinala que a fundamentação jurídica para o princípio da supremacia do interesse público está no artigo 3º do texto constitucional. Em outras palavras: o interesse público consiste, nos ditames constitucionais, em construir uma sociedade livre, justa e solidária; garantir o desenvolvimento nacional; erradicar a pobreza e a marginalização e reduzir as desigualdades

[30] HACHEM, Daniel Wunder. A dupla noção jurídica de interesse público em direito administrativo. A&C – Revista de Direito Administrativo & Constitucional, Belo Horizonte, a. 11, n. 44, p. 59-110, abr./jun. 2011a.
[31] idem.

sociais e regionais e promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação. **Ou, de maneira mais clara: o interesse público é à realização dos direitos fundamentais protegidos pela Constituição da República**.

Com efeito, o ordenamento jurídico pátrio não permite que a atuação dos órgãos públicos desborde os limites impostos pela legalidade; **em verdade, o que se impõe é que os atos públicos observem, de maneira irrestrita, os direitos e garantias individuais, a fidelidade às instituições e os princípios éticos que regem os interesses e a segurança do Estado.**

Atuar de maneira diversa - adquirindo objeto ilícito com fins a desrespeitar direitos e garantias - significa atropelar o interesse público; desviar à finalidade da Administração.

4. O PEDIDO

Em face de todo o exposto, requerem a **prioridade de tramitação**, nos termos do art. 159, V, do Regimento Interno deste E. Tribunal de Contas, em razão dos fatos graves relatados.

Requerem seja determinado **cautelarmente ao Ministério da Justiça e Segurança Pública a imediata suspensão do Pregão Eletrônico nº 3/2021**, impedindo a homologação e a adjudicação do objeto em andamento.

Requer, ainda, seja instaurado procedimento para averiguação da denúncia ora formulada, que ao final deverá ser acolhida pelo Exmo. Sr. Relator, com posterior submissão ao Plenário determinando-se:

▪ a imediata **SUSPENSÃO** do Pregão Eletrônico nº 3/2021, em razão da violação aos princípios que norteiam os procedimentos licitatórios e do evidente prejuízo à democracia e ao erário;

▪ o acolhimento de todos os fundamentos e o provimento para consequente **REVOGAÇÃO** do Pregão Eletrônico nº 3/2021, em razão dos vícios insanáveis apresentados nesta denúncia.

Nesses termos,

pedem e esperam deferimento.

São Paulo, 24 de maio de 2021

JULIANA VIEIRA DOS SANTOS
OAB/SP 183.122

GABRIEL DE CARVALHO SAMPAIO
OAB/SP 252.259

LUCAS MORAES SANTOS
OAB/DF n. 49.849

RODRIGO FILIPPI DORNELLES
OAB/SP 329.849