

Atividade estatal de inteligência: legitimidade, controle e o PL 6.423

Autor(a): Vitor Soliano

Publicado em: 12 de julho de 2026

Publicação: conjur_import

Link JurisTube: <https://juristube.com.br/colunistas/vitor-soliano/atividade-estatal-de-inteligencia-legitimidade-controle-e-o-pl-6423>

Fonte original:

<https://conjur.com.br/2026-jul-12/atividade-estatal-de-inteligencia-legitimidade-controle-e-o-pl-6-423-25-2>

Identificador citável: juristube.com.br/colunistas/vitor-soliano/atividade-estatal-de-inteligencia-legitimidade-controle-e-o-pl-6423#ep-ac09f91d

Resumo

Atividade de inteligência, função estatal permanente e estratégica, também tem fundamento na adequada persecução dos interesses da sociedade

Texto integral

A atividade de inteligência, função estatal permanente e estratégica, encontra fundamento não apenas na preservação da soberania nacional e da ordem pública, mas na adequada persecução dos interesses da sociedade, no dever de estruturação de políticas públicas estrategicamente maduras e efetivas, baseadas em dados e informações confiáveis. Não está adstrita, portanto, às ações policiais e investigativas estrito sensu, espalhando-se para contextos relativamente recentes, como os atinentes a práticas potencialmente prejudiciais levadas a efeito por meio das redes sociais, com o uso pouco transparente de algoritmos e impulsionamento. A concentração do poder tecnológico — e de infraestrutura — nas mãos dos grandes conglomerados representa potencial risco para toda a sociedade, em especial aos mais vulneráveis e suscetíveis a manipulações, enredamentos e influência em sua esfera de decisão e autonomia. A compreensão desse cenário é condicionante de uma legislação eficiente e funcional sobre o tema, e deve nortear as discussões sobre o assunto — o que, conforme se verá ao longo do presente, não se aperfeiçoou, ainda, na redação do Projeto de Lei 6.423/2025, voltado justamente a disciplinar os aspectos gerais da Inteligência no Estado brasileiro. Atividade estatal de inteligência: razão de ser, fundamentos e legitimidade A atividade em foco somente pode ser legitimamente exercida sob o viés democrático, da garantia dos direitos fundamentais, e conforme a lógica do sistema constitucional de controle — tanto de legalidade estrita quanto de juridicidade/legitimidade democrática. Imprescindível, portanto, a criação de mecanismos de controle confiáveis, perenes e desvincilhados do governo de ocasião. A distribuição difusa das instâncias de accountability — a atuarem como verdadeiro sistema — deve ser, portanto, prioridade: em se tratando de ação potencialmente invasiva da esfera de intimidade do cidadão, que se dá conceitualmente de forma sub-reptícia e velada, os cuidados com o controle devem ser especialmente considerados. A sua legitimidade repousa no equilíbrio entre eficácia operacional e conformidade com os valores da legalidade, respeito aos direitos fundamentais, proporcionalidade, estrita necessidade. Conforme lição de Cepik [1], condicionam tal legitimidade: 1. um marco legal estrito sobre as operações de coleta de dados e contrainteligência, com limites

claros; 2. mecanismos e controle externo robusto, com o fortalecimento da fiscalização e do controle institucional (Legislativo, Judiciário, Executivo e MP) sobre todas as agências de segurança; e 3. estabelecimento de uma integridade analítica, traduzida na capacidade de gerar produtos analíticos de qualidade, imunes à politização e aos interesses privados, com neutralidade institucional. Segundo o autor, o conceito representa garantia de que a análise de inteligência seja tecnicamente precisa, profissionalmente ética e politicamente neutra, estando na base do equilíbrio entre democracia, segurança e desenvolvimento. Instrumentais de suma importância são os códigos de ética e a profissionalização da atividade, de modo a proporcionar constante escrutínio público e técnico. Fundamental, ainda, o conceito de vigilância recursiva — capacidade dos sistemas de vigilância viabilizarem seu próprio escrutínio posterior, a partir de ‘pegadas’ que levem à “decodificação” do sistema [2] —, que vem fundamentado a expansão dos limites de controle pelo Judiciário e Política Federal ao investigar rastros digitais deixados por ferramentas eletrônicas. Foi o que se deu, exemplificativamente, com os arquivos do Serviço Nacional de Informações (SNI) da ditadura militar, utilizados como matéria-prima pela Comissão Nacional da Verdade (2011-2014), e que permitiram a decodificação do sistema repressivo décadas depois. Mais recentemente, a técnica foi empregada no caso do software de geolocalização First Mile pela Abin: os registros digitais deixados pelo monitoramento de 33.000 ativistas e políticos tornaram-se as evidências empregadas na investigação da própria agência, em momento posterior. Por fim, de se manter como norte, sempre, os objetivos da inteligência estatal: 1. Assessoramento de autoridades na análise e difusão de conhecimento; 2. Defesa das instituições democráticas, da ordem constitucional e do Estado de Direito; 3. Identificação de ameaças à soberania e aos direitos fundamentais, e de oportunidades; 4. Salvaguarda da sociedade, com a proteção de conhecimentos sensíveis; 5. Garantia da efetividade e legitimidade das políticas públicas. Limites da atividade de inteligência: controle e direitos fundamentais A atividade de inteligência deve ser desenvolvida em estrita consonância com a legalidade, necessidade e proporcionalidade, além do respeito aos direitos fundamentais. Seu controle judicial apresenta atualmente limites estruturais, políticos e operacionais, determinantes de sua natureza comumente reativa, descrita pela doutrina como ‘alarme de incêndio’, em razão de somente ocorrer depois de consumada a ofensa à ordem jurídica/democrática [3]. Embora a Abin não tenha poder de polícia ou autorização legal para interceptar comunicações, a falta de legislação específica que regule detalhadamente as operações de coleta de dados e contrainteligência dificulta o controle judicial — que muitas vezes se fundamenta em princípios genéricos, com potencial prejuízo à segurança jurídica e previsibilidade. Não obstante, o STF vem fixando balizas importantes, tais como a proibição do monitoramento ideológico, com consequente determinação de suspensão da produção de relatórios sobre opositores do governo que atuavam dentro da legalidade [4]. A lógica a ser seguida tem como cerne, invariavelmente, os direitos fundamentais, em especial a privacidade, intimidade e proteção de dados. PL 6.423/25: vulnerabilidades e pontos de aprimoramento A ausência de disciplina legal exauriente compromete a legitimidade, legalidade e juridicidade da atividade de inteligência, inclusive por carência de ferramentas de previsibilidade, limites, controle e segurança jurídica. Nesse sentido, louvável a iniciativa consubstanciada no PL ora em comento. Não se pode deixar de consignar, porém, alguns pontos dignos de atenção — e revisão — no projeto. Considere-se, de plano, a abrangência da pretensão, que foca desde operações sigilosas até acesso a bases de dados, uso de inteligência artificial, big data e compartilhamento de informações. A falta de precisão técnica na definição das operações de inteligência, descritas de forma aberta e vaga, exemplificativamente, como as voltadas à “obtenção de dados negados” (artigo 3º, I) e à “influência legítima sobre pessoas, organizações e processos decisórios” (artigo 12), não se coaduna com o

sistema constitucional pátrio. Realmente, influenciar 'legitimamente' pessoas, organizações e processos implica em uma miríade praticamente infinita de iniciativas, a colocarem em risco a autonomia, livre consciência e convencimento cidadãos, inclusive em termos políticos. Da mesma forma, a locução “ produção de inteligência preventiva, antecipatória e oportun a” afigura-se carregada de subjetividade, com exagerada elasticidade, a dar azo a distorções e instrumentalizações (artigo 5º, §5º). O artigo 8º autoriza o acesso, por profissionais de inteligência, e independentemente de autorização judicial, a dados cadastrais mantidos por órgãos públicos, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito. A facilidade de acesso, com exclusão da avaliação judicial, vulnera a garantia à proteção de dados pessoais. Similar ameaça consta do artigo 11, segundo o qual empresas de telecomunicações, provedores de internet e empresas de transporte devem manter registros de conexão, metadados de tráfego, identificação de usuários e dados de viagens por até cinco anos (período bastante prolongado, considerada a natureza das informações e a ilegitimidade de seu armazenamento genérico e imotivado) — os quais ficarão à disposição dos órgãos de inteligência, mediante requisição formal (sem maiores controles) — com potencial facilitação de estratégias de monitoramento cidadão. O artigo 13 possibilita — temerariamente, ao nosso ver —, de emprego de técnicas e meios sigilosos, como acompanhamento e monitoramento de alvos, recrutamento e controle de fontes humanas, comunicação sigilosa, dissimulação, infiltração de inteligência, captação ambiental de sinais eletromagnéticos, ópticos ou acústicos, e meios técnicos e cibernéticos, bastando mero “ plano específico validado por superior hierárquico”. A exigência de autorização judicial para o uso de táticas tais está adstrita a ‘meios excepcionais’, definidos como ferramentas de monitoramento remoto de terminais de comunicações pessoais; e o afastamento dos sigilos financeiro, bancário e fiscal . Tal estratégia enfraquece a accountability . O artigo 20, parágrafo único, traz a excepcionalidade da transparência dos contratos de aquisição e utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais – em mais um avanço em direção à relativização, ou inviabilização, do controle, inclusive social, em dissonância com a lógica regente da LAI (transparência como regra). O afastamento dos órgãos de controle e da própria sociedade do escrutínio sobre tais atos representa sério risco à privacidade e proteção de dados: conforme análise da Transparência Brasil, em 2024, de 61 contratos de tecnologia de vigilância firmados por secretarias de segurança da Bahia, Paraná, Rio de Janeiro e São Paulo (a maioria para aquisição de ferramentas de acesso intrusivo a dispositivos móveis), apenas 28% traziam cláusula com referência direta à LGPD [5] . O artigo 27 autoriza genericamente a ocultação de identidade para a realização de atividades destinadas à produção de conhecimentos, inclusive em ambiente cibernético. A falta de parâmetros objetivos, aliada, uma vez mais, à carência de meios de controle efetivos, coloca em inconstitucional vulnerabilidade os direitos fundamentais. O dispositivo deveria prever, ao menos, restrições fáticas — como ação profissional oficial, legítima e de interesse público — com, idealmente, prévia autorização judicial. Outro ponto digno de atenção: a possibilidade, trazida pelo artigo 39, que altera a LAI, de classificação de informações como ultrassecretas, pelo prazo de 25 anos, prorrogáveis por mais 25, pelo diretor-geral da Abin. Atualmente, essa prerrogativa é exclusiva do presidente e vice-presidente da República, ministros de Estado, comandantes das Forças Armadas e chefes de missões diplomáticas e consulares permanentes no exterior, representando o alargamento ameaça à transparência e controle social, tônicas da democracia e da ordem constitucional, mormente em atividade por natureza velada, como a de inteligência. Para além desses aspectos, o dispositivo gera menor sujeição da agência ao escrutínio do Executivo, com risco de politização da atividade, subtraída da avaliação dos quadros

técnicos da administração. Digna de crítica, por fim, a ausência de estruturação técnica da CCAI, com perda de oportunidade do projeto, que poderia valer-se da inclusão do tema na ordem do dia para prever carreira estruturada, estável, com garantias indispensáveis à independência do seu quadro. É mais um dos aspectos relacionados à vasta gama de prerrogativas desacompanhadas dos respectivos mecanismos de contenção (inclusive social) e critérios seguros de proporcionalidade e necessidade, além de garantia, aos afetados, de acessar, corrigir ou contestar o uso de seus dados. O diploma perpetua, assim, traços autocráticos herdados da era militar, em que a garantia da ‘segurança nacional’ era invocada rotineiramente a justificar abusos e ofensas aos direitos e garantias individuais. Considerações finais A construção do PL 6.423/25, proposto pela Comissão Mista de Controle da Atividades de Inteligência do Congresso Nacional após envolvimento de entidades como a União dos Profissionais de Inteligência de Estado da ABI, não obstante corporifique resposta a demanda social por clara e mais profunda disciplina legal da atividade de inteligência, não se acha ainda maduro para aprovação, sofrendo de vícios e inconsistências a demandarem aprofundamento das discussões. Nesse sentido, absolutamente necessário o envolvimento da sociedade civil, da academia, de especialistas e órgãos de controle, de modo a trazer para o campo da disciplina legitimidade, transparência, controle social e accountability efetiva. Somente então, poderemos ficar (um pouco mais) tranquilos quanto à juridicidade do exercício de tão sensível função estatal, mormente em tempos de protagonismo da internet e redes sociais. [1] CEPIK, Marco. Intelligence and security in Brazil: a historical and institutional overview. *International Journal of Intelligence, Security, and Public Affairs*, v. 23, n. 2, p. 145–165, 2021. Disponível aqui . [2] MELGAÇO, Lucas. Recursive surveillance and the persistence of authoritarian surveillance in Brazil. *Surveillance & Society*, v. 23, n. 1, p. 140–144, 2025. DOI: 10.24908/ss.v23i1.18986. Disponível aqui . [3] MCCUBBINS; SCHWARTZ, 1984 apud CEPIK, 2021, p. 9. [4] Como no caso do Caso do “Dossiê Antifascista”, apreciado no âmbito da ADPF 722. O governo vinha então monitorando 579 servidores públicos da área de segurança (níveis federal e estadual) identificados como membros do “Movimento Policiais Antifascismo”, quatro professores universitários “influenciadores de opinião” e intelectuais. O STF, em agosto de 2020, fixou balizas fundamentais para a inteligência democrática, proibiu o monitoramento ideológico ou de convicções políticas. [5] TRANSPARÊNCIA INTERNACIONAL BRASIL. Proteção de dados e tecnologias de vigilância para segurança pública. Brasília: Transparência Internacional Brasil, 2025. Disponível aqui .

Como citar este documento

As citações abaixo seguem os padrões ABNT NBR 6023:2018, APA 7ª edição, Chicago Author-Date (17ª ed.) e BibTeX (LaTeX). Copie o formato exigido pelo periódico ou gerenciador bibliográfico (Zotero, Mendeley, EndNote).

ABNT (NBR 6023:2018)

SOLIANO, Vitor. Atividade estatal de inteligência: legitimidade, controle e o PL 6.423. conjur_import, 12 jul. 2026. Disponível em:
<https://conjur.com.br/2026-jul-12/atividade-estatal-de-inteligencia-legitimidade-controle-e-o-pl-6-423-25-2>.
Acesso via: JurisTube — Acervo Digital de Direito. Disponível em: <https://juristube.com.br/colonistas/vitor-soliano/atividade-estatal-de-inteligencia-legitimidade-controle-e-o-pl-6-423>. Acesso em: 30 set. 2026.

APA 7ª edição

Soliano, V. (2026, July 12). Atividade estatal de inteligência: legitimidade, controle e o PL 6.423. *conjur_import*.
<https://conjur.com.br/2026-jul-12/atividade-estatal-de-inteligencia-legitimidade-controle-e-o-pl-6-423-25-2>

Chicago Author-Date (17ª ed.)

SOLIANO, Vitor. 2026. "Atividade estatal de inteligência: legitimidade, controle e o PL 6.423." *conjur_import*, July 12.
<https://conjur.com.br/2026-jul-12/atividade-estatal-de-inteligencia-legitimidade-controle-e-o-pl-6-423-25-2>

BibTeX

```
@article{vitor-soliano-atividade-estatal-de-intelig-ncia-legiti-2026,  
author = {Soliano, Vitor},  
title = {Atividade estatal de inteligência: legitimidade, controle e o PL 6.423},  
journal = {conjur_import},  
year = {2026},  
url = {https://conjur.com.br/2026-jul-12/atividade-estatal-de-inteligencia-legitimidade-controle-e-o-pl-6-423-25-2},  
urldate = {2026-07-12}  
}
```



Licença de Uso — CC BY-NC-SA 4.0

Este conteúdo está licenciado sob a licença Creative Commons Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional (CC BY-NC-SA 4.0). O uso para fins acadêmicos e educacionais é permitido, desde que citada a fonte original (JurisTube) conforme as normas técnicas indicadas neste documento.

Termos completos:
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.pt-br>