WHITE PAPER

Fundamentos para o Controle da Inteligência no Brasil

Proposta de marco legal para um sistema de controle parlamentar, judicial, especializado e social

Conrado Klöckner

2026

Legiscraft

Legiscraft

Sobre o Legiscraft

O Legiscraft é um laboratório de políticas públicas dedicado ao desenvolvimento de arranjos normativos para desafios emergentes.

Autores colaboradores

Débora Coward Fogliatto · Gabriel Oliveira Bohm · Isadora Zorzi · Luiz Eduardo Antonello · Renato Maciel Damiani · Samuel Alfredo Forneck · Vitória Battisti da Silva

Revisores internos

Samuel Alfredo Forneck · Vitória Battisti da Silva

Revisores externos

André Ramiro (Universidade de Hamburgo) · Pedro Saliba (Data Privacy Brasil) · Vinicius Silva (Data Privacy Brasil)

Como referenciar este documento

Klöckner, Conrado. 2026. *Fundamentos para o Controle da Inteligência no Brasil: proposta de marco legal para um sistema de controle parlamentar, judicial, especializado e social*. White paper. Porto Alegre: Legiscraft.

director@legiscraft.org · legiscraft.org

Principais achados

- O déficit de controle da inteligência no Brasil é estrutural.
- O arranjo vigente entrega mera aparência de controle, sendo estreito, fragmentado e predominantemente reativo.
- Um controle externo estritamente parlamentar nunca será suficiente.
- Um controle prévio em medidas de alto risco é indispensável, mas pode ser capturado se não incluir contraditório independente.
- A criação de uma autoridade especializada com capacidade de realizar monitoramento contínuo é fundamental para enfrentar a assimetria informacional.
- Capacidades intrusivas opacas ou incompatíveis com o ordenamento jurídico devem ser identificadas antes da contratação das tecnologias.
- O controle social é indispensável, mas não pode ser a principal via de apuração de irregularidades.
- A recente crise de legitimidade das atividades de inteligência abriu uma janela de oportunidade histórica para uma reforma robusta.
- A PEC 18/2025 e o pacote da CCAI contêm avanços pontuais, mas incapazes de alcançar as causas de fundo, havendo risco de que sejam consolidados como uma reforma cosmética.
- O pacote da CCAI pode ser útil se for promovido como uma etapa de transição, preparando terreno para uma reforma estrutural.

Sumário executivo

As capacidades intrusivas do sistema de inteligência cresceram rapidamente, sem que houvesse a constituição de mecanismos proporcionais de fiscalização. No Brasil, o sistema de controle, concentrado no parlamento, é limitado ao plano federal, predominantemente reativo e incapaz de realizar monitoramento contínuo. O resultado é um quadro de **descontrole estrutural** onde há muita opacidade, pouco escrutínio e baixa capacidade de responsabilização. Um problema crítico que resulta da combinação entre legado autoritário de sigilo, baixa saliência política do tema e um arranjo institucional que segue estreito, fragmentado e dependente do próprio ator controlado.

Esse diagnóstico se projeta sobre um momento histórico especialmente sensível. A crise da chamada "Abin Paralela", somada às investigações sobre a tentativa recente de golpe de Estado, retirou o tema do plano abstrato e expôs, de forma aguda, os riscos de manter atividades de inteligência em espaço de exceção, com controles frágeis e baixa auditabilidade. Em meio à crise de legitimidade do sistema, aumenta o custo político da inércia e surge uma **janela de oportunidade para reformas**. Esse cenário, porém, guarda riscos previsíveis, como a provável reação corporativa, a inércia pró-sigilo, a baixa prioridade pública do tema e a tentação de aprovar soluções de fachada.

A **proposta** apresentada neste *white paper* envolve a construção de um sistema contínuo, escalonado e distribuído de controle, com núcleo parlamentar, judicial, especializado e social, tendo como referência as melhores práticas internacionais. Em seu cerne, está o estabelecimento de um mecanismo de **controle judicial prévio** e a criação de um **novo ator** especializado, independente e vinculado ao Parlamento — a Autoridade Nacional de Controle das Atividades de Inteligência.

A proposta também reforça o **controle parlamentar**, substituindo a excepcionalidade pela rotina e a dependência política por fluxos mais sólidos de supervisão, integrando mecanismos específicos para proteger a captura por maiorias ocasionais. Além disso, estabelece procedimentos na fase de **contratação de tecnologias**, passando a exigir relatórios de impacto antes mesmo de o Estado internalizar capacidades potencialmente intrusivas. Para fins de **controle social**, a proposta ainda institui um sistema robusto para proteger denunciantes e o dever de notificação posterior de pessoas vigiadas, derivado do sistema alemão.

Por fim, o documento avalia a PEC 18/2025 e o pacote elaborado no âmbito da CCAI, hoje postas como **alternativas de reforma** do setor. A conclusão é que, embora ambos possam produzir avanços pontuais, nenhum enfrenta com densidade suficiente os vetores centrais do problema. Isso não impede, contudo, de reconhecer eventual utilidade do pacote da CCAI, desde que ele seja compreendido não como resposta final, mas como etapa de transição — como piso inicial para uma reforma mais robusta. À luz do diagnóstico produzido, o pacote integrado aqui proposto permanece como a formulação mais consistente, por ser o único que procura enfrentar de modo combinado o escopo insuficiente do controle, sua baixa densidade, a dependência do próprio controlado, a opacidade operacional e a fragmentação institucional.

Sumário

1 Introdução

Enquanto o vigia bebe da ubiquidade e dos encantos da inteligência artificial, alcançando **níveis quase distópicos de intrusão**, o seu controlador perambula confuso, maltrapilho e empoeirado, preso no século XX. Um descompasso crônico que revela um problema democrático de primeira ordem: com a digitalização da vida social, a capacidade estatal de coletar, correlacionar e explorar dados cresceu muito mais rapidamente do que os mecanismos de contenção e responsabilização de abusos, criando uma **hipertrofia que desequilibra o sistema de freios e contrapesos** e põe em risco não só a qualidade das atividades de inteligência[1], mas a própria continuidade democrática (Parsons 2018; Broeders et al. 2019; Zuboff 2019; Vieth e Wetzling 2019; Parlamento Europeu 2023, Klöckner e Joia 2025).

É desse descompasso que parte este *white paper*. No Brasil, a expansão das capacidades de inteligência, sem correspondente fortalecimento do controle externo, produziu um quadro de **descontrole estrutural**. O diagnóstico, a tese e as proposições legislativas que compõem este trabalho se organizam como resposta a esse problema. O foco no controle **externo** é estratégico, pois em atividades marcadas por sigilo e potencial intrusivo, é ele que pode ter força real para conter abusos e, por tabela, induzir o funcionamento adequado do controle interno.

[1] Para os fins deste *white paper*, "atividades de inteligência" são compreendidas como atividades administrativas de assessoramento preparatório à tomada de decisão, distinguindo-se da investigação criminal, que é voltada à apuração de infrações penais determinadas. O recorte adotado limita-se àquelas atividades que, em razão de seus alvos ou das técnicas empregadas, apresentam maior risco para direitos fundamentais — isto é, aquelas via de regra desenvolvidas por órgãos de inteligência de Estado, militar ou policial. O conteúdo exato desse recorte é desenvolvido ao longo do texto e, em termos normativos, encontra correspondência no **art. 5º** do primeiro anteprojeto de lei.

O caso do **Pegasus**, *spyware* capaz de ativar câmeras de smartphones sem um único clique, é um marco simbólico, tendo demonstrado que o risco não é retórico. Diversas democracias testemunharam o monitoramento abusivo de jornalistas, opositores e críticos da sociedade civil, gerando graves crises institucionais e de legitimidade:

- na **Espanha**, o caso revelou o monitoramento de parlamentares, líderes políticos, advogados e ativistas ligados ao movimento catalão, expondo o potencial de uso da vigilância contra atores centrais da oposição política e da sociedade civil (Scott-Railton et al. 2022);
- na **Polônia**, o spyware foi utilizado contra figuras da oposição, tendo gerado a abertura de comissão parlamentar de inquérito e tornado visível o risco de captura político-partidária de capacidades intrusivas (Gera 2024);
- no **México**, as revelações mostraram que jornalistas estavam entre os alvos, evidenciando a especial vulnerabilidade de quem exerce funções de crítica e fiscalização do poder (Lakhani 2021);
- na **Índia**, as alegações envolveram monitoramento abusivo de opositores, jornalistas e ativistas, tendo a Suprema Corte precisado determinar investigação independente (Dhillon e Safi 2021).

Também no Brasil, esse debate deixou de ser abstrato. A crise conhecida como **"Abin Paralela"** revelou, segundo a Polícia Federal, o uso sistemático de estruturas e ferramentas de inteligência para monitoramento ilegal de autoridades públicas (Brasil, PF 2025). Em paralelo, o Supremo Tribunal Federal passou a discutir, na **ADPF 1143**, os limites constitucionais do uso, por órgãos públicos, de ferramentas invasivas de monitoramento digital (Brasil, STF 2024). Na mesma linha, as investigações sobre a recente **tentativa de golpe de Estado** apontaram para a

participação da então diretora de inteligência do Ministério da Justiça e de integrantes das forças especiais do Exército brasileiro (Brasil, STF 2025), o que obriga a colocar no centro da agenda o perigo de se manter as atividades de inteligência em espaço de exceção, livre de escrutínio. Em um mundo em que o Pegasus é possível, **qualquer eleição pode ser a última**.

O presente trabalho, fruto dessa preocupação, foi produzido pelo Legiscraft, um laboratório de políticas públicas voltado à tradução de problemas complexos e emergentes em desenho normativo. Para tal, o laboratório se aprofunda no **problema concreto**, construindo a solução a partir dele, sem caminhos pré-definidos: identifica as suas causas estruturais, reconstrói os incentivos dos atores relevantes, analisa riscos e oportunidades do ambiente político e só então estrutura uma proposta regulatória integrada. Esse percurso é especialmente importante para **evitar** que uma janela de oportunidade legislativa produza **reformas cosméticas**, incapazes de tocar nos alicerces que perpetuam o problema.

Tratar do controle da inteligência, nesse sentido, é especialmente desafiador, pois incide sobre uma atividade marcada por **sigilo** estrutural, **pressões políticas** permanentes, **assimetria extrema de informação** e **rápida mutação tecnológica**. Sem um desenho sólido, o controlador vai saber menos, chegar depois e depender daquilo que o próprio controlado ou um *whistleblower* decidirem revelar — uma combinação fatal que tende a produzir deferência ou captura, reduzindo o controle a mera formalidade (Hillebrand 2019; Defty 2020).

Essa dificuldade se agrava ainda mais porque a inteligência contemporânea já não se concentra em uma única agência, nem em um único plano institucional: ela **opera em rede**, envolvendo atores federais, estaduais, privados e parceiros internacionais e distribuindo-se entre diferentes modalidades — inteligência de Estado, militar, policial, fiscal e financeira. Uma complexidade que torna

insuficientes controles baseados apenas em recortes orgânicos ou em supervisão estritamente macro-política (Gill 2020; Moses 2022).

No **Brasil**, o controle externo se resume a uma **comissão parlamentar** sem estrutura, com atuação guiada por escândalos pontuais, desprovida de procedimentos regulares de supervisão e limitada a atores federais. Não há mecanismos *ex ante* ou monitoramento contínuo e não há controle sobre a inteligência produzida pelos estados. Trata-se de um arranjo que desconsidera, em diversos níveis, as complexidades desse tipo de controle, resultando em **baixíssima capacidade de escrutínio** e na alta dependência de vazamentos.

Um **controle eficaz**, por contraste, precisa ser desenhado à altura da complexidade do objeto que supervisiona. Na inteligência, ele só deixa de ser simbólico quando estabelece uma **rede institucional** de atores independentes, sem assimetria de informação, com **capacidade formal e material** de realizar monitoramento contínuo, autorizar atividades intrusivas e responsabilizar quem exceder o seu mandato (Klöckner e Joia 2025). Além disso, um sistema eficaz precisa construir canais seguros para que **denunciantes** — que devem ser a última *ratio* da *accountability*, e não a única — possam acionar as instituições sem depender de vazamentos disruptivos (Gill 2022; Kniep et al. 2024).

Dito isso, a **tese central** deste paper é que, no Brasil, o **problema do descontrole é estrutural**, e sua solução arquitetônica **não pode ser salva por remendos** normativos. Hoje, o controle é limitado em escopo, frágil em densidade, pouco independente, escasso em meios e fragmentado entre instâncias que não se reforçam adequadamente. O resultado é um arranjo em que a opacidade operacional é a regra, a responsabilização é rara e a legitimidade democrática da atividade segue instável.

O documento se desenvolve em três **fases**. A primeira é **diagnóstica**: reconstrói o problema, identifica suas causas e explicita por que o descontrole da inteligência no Brasil é estrutural. A segunda é **propositiva**: apresenta o pacote regulatório integrado elaborado pelo Legiscraft, sua arquitetura institucional e sua teoria da mudança. A terceira é **de viabilidade**: examina riscos, oportunidades, *stakeholders* e alternativas hoje em disputa, para avaliar as condições políticas de avanço da proposta e situá-la em relação às demais opções presentes na agenda do setor.

2 Diagnóstico

2.1 Problema e suas causas

Ausência de capacidade efetiva de controle das atividades de inteligência no Brasil não decorre de uma falha isolada, mas de uma cadeia causal em camadas. Em sua base, está uma causa de natureza histórico-cultural: o **legado autoritário de sigilo e deferência institucional**, que sobreviveu à redemocratização e dificultou a consolidação da inteligência como tema ordinário de escrutínio democrático (Figueiredo 2005; Rocha 2013).

Dessa herança decorre uma segunda camada, de natureza político-cultural: a **baixa saliência política** e a ainda limitada maturidade pública do tema (Gonçalves e Bedritichuk 2024). Esse fenômeno também se explica, em larga medida, pelo sigilo, alta tecnicidade e baixo retorno eleitoral da matéria, o que acaba por afastar agentes políticos do tema. Neste último caso, trata-se de característica que não é singular ao caso brasileiro, atingido todo o modelo de controle concentrado na esfera parlamentar (Born e Leigh 2005; Jasutis 2021; Hansén 2023).

Sobre esse terreno é que se estabelecem as **causas de natureza institucional-normativa** — isto é, aquelas que podem efetivamente ser atacadas por meio de mudanças legislativas e, por isso, são o **foco das propostas** deste *white paper*. São elas: a opacidade operacional, a indeterminação do que deve ser objeto de controle, o escopo limitado do escrutínio e a falta de independência, recursos e articulação do sistema de controle como um todo.

A **Figura 1**, a seguir, organiza esse diagnóstico na forma de uma árvore do problema. Ela também distingue, entre as causas e efeitos, aquelas sobre as quais a proposta legislativa trazida por este trabalho incide de modo direto ou indireto.

Figura 1. Árvore do problema e impacto da proposta

No Brasil, o controle externo da inteligência permanece desregulado. O que existe, de forma concreta, é a **Resolução nº 2/2013-CN**, que cria um órgão

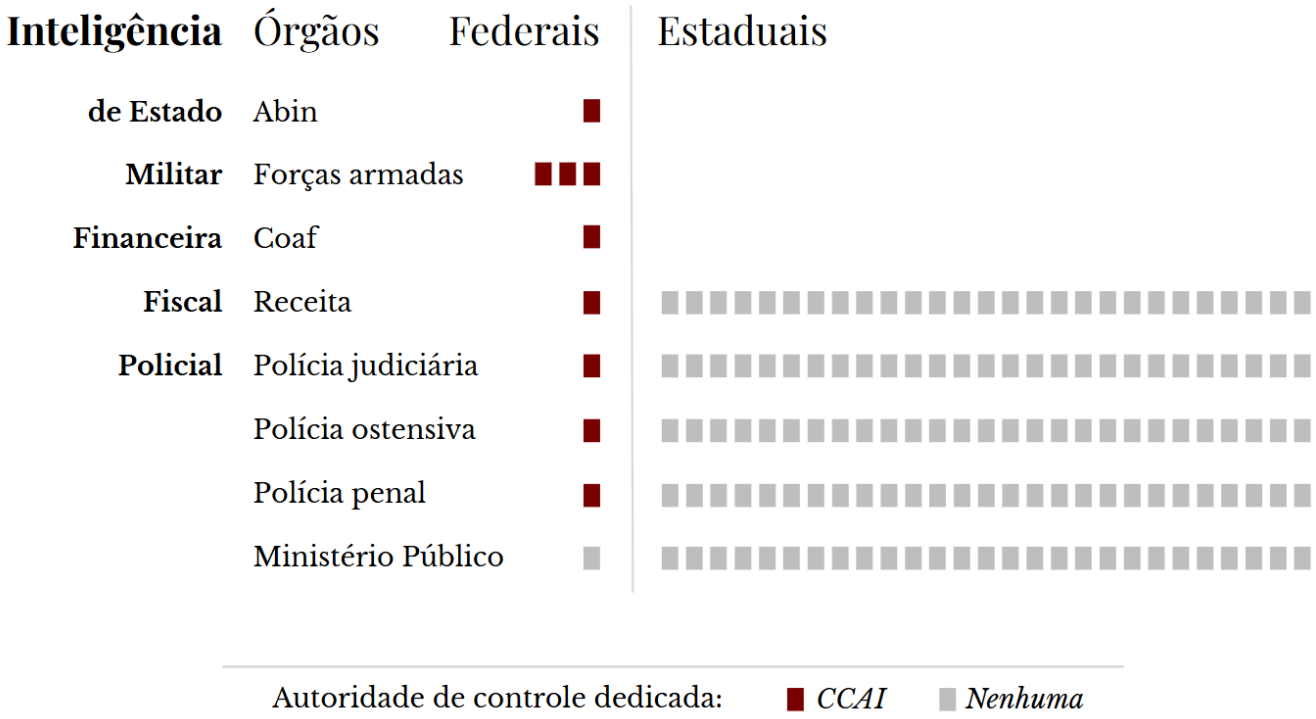
parlamentar especializado, bastante limitado, em nível federal: a Comissão Mista de Controle das Atividades de Inteligência (**CCAI**). Fora disso, o ordenamento não estruturou qualquer sistema de controle que discipline tratamento de dados, trilhas de autorização, requisitos de auditabilidade ou fluxos de articulação interinstitucional, o que gera **opacidade operacional das atividades controladas**.

Uma evidência sólida do nível de opacidade do sistema brasileiro foi trazida pelo Relatório de Gestão Correcional da Abin (2026) para o exercício de 2025. No texto inédito, é informado que até 2022 o controle interno sequer era uma atividade estruturada, dependendo de esforços e habilidade individuais[2]. Ou seja, 9 anos de funcionamento da CCAI não resultaram sequer na criação de uma unidade correicional estruturada no principal órgão de inteligência do país. Se há uma variável *proxy* capaz de condensar a ineficácia do sistema atual, é esta.

Além de solitária, a CCAI tem um **escopo bastante limitado**. Seu escrutínio se limita à administração pública federal (Brasil 2013, art. 2º), deixando de fora, por exemplo, toda a atividade de inteligência produzida pelas **polícias e receitas estaduais** — só aqui, são mais de cem órgãos sem controle dedicado, conforme se verifica na **Figura 2**.

[2] O mesmo relatório, vale destacar, registra avanços recentes relevantes: em 2024, a corregedoria passou a ser considerada unidade com "competência, estrutura e recursos (...) para atuação independente" (Abin 2026). O ponto aqui, por óbvio, não é negar a evolução recente, mas mostrar que ela é tardia e que, sem pressão estável de controle externo, segue dependente da prioridade atribuída pelo próprio órgão controlado, podendo os avanços serem desarticulados a qualquer momento.

Figura 2. Órgãos de inteligência com controle externo dedicado



Em tese, nada impede que as assembleias legislativas instituam comissões locais — embora não se tenha notícia de algo nesse sentido e não haja incentivo normativo para que isso ocorra. Também fica fora dessa cobertura o Ministério Público (MP), que, uma vez consolidada sua atuação em investigações de natureza penal, passou a ser produtor de inteligência policial (Brasil, CNMP 2024).[3]

A limitação do escopo de controle não é apenas em termos de alcance institucional, mas também em profundidade. O modelo de controle parlamentar brasileiro não foi estruturado para realizar autorizações *ex ante* em caso concreto

[3] Na Resolução nº 292/2024, do Conselho Nacional do Ministério Público, que trata da política de inteligência do órgão, fica claro que aquilo que é referido como inteligência *ministerial* é, na prática, um misto de inteligência institucional tradicional, realizada por todos os Poderes, e inteligência policial, dada sua nova função de investigador (Brasil, CNMP 2024).

nem para manter monitoramento contínuo. O controle existente, assim, é ao mesmo tempo federalmente restrito e **predominantemente posterior**, deixando fora parcelas relevantes da atividade.

Outros órgãos de controle, como o judiciário, o MP e os tribunais de contas, até podem incidir sobre a atividade de inteligência, mas o fazem apenas de modo incidental, fragmentário e não dedicado, como pode ser observado no inquérito da "Abin Paralela" (Brasil, PF 2025), na investigação do sistema Cortex (Brasil, MPF 2022) e na contestação de uma licitação de ferramenta de OSINT (Brasil, TCU 2021). São atuações que surgem apenas quando há algum ponto de contato com competências gerais de controle, sendo incapazes de substituir um arranjo contínuo, especializado e vocacionado à supervisão da inteligência enquanto tal.

No caso do **MP**, cabe destacar, o judiciário decidiu que seu mandato não alcança as atividades de **inteligência policial** (Brasil, STJ 2016). Em qualquer cenário, o fato de a instituição ter se transformado também em produtora de inteligência, afasta-o da posição institucionalmente neutra necessária para figurar como protagonista do controle externo. Em uma reforma, antes de se avaliar se o MP deve fazer controle externo da inteligência, deve-se decidir se ele seguirá acumulando funções policiais — no quadro de incentivos, não é lógico nem eficaz que exerça ambas as atividades.

Outro elemento promotor do descontrole é a **indeterminação do objeto fiscalizado**. Hoje, "atividade de inteligência" abarca um conjunto excessivamente amplo e heterogêneo de práticas, sem destaque para o que exatamente exige escrutínio reforçado. Sequer há, por exemplo, uma definição normativa do que se qualifica como medida intrusiva, o que dificulta enormemente a criação de gatilhos, prioridades e graus diferenciados de supervisão (Ramiro 2025).

Soma-se a isso a **falta de independência do controlador**. O parlamento, por sua natureza intrinsecamente política, tende a reproduzir maiorias governistas e dinâmicas de coalizão. Em matéria de inteligência, ele só ganharia densidade real se estivesse acompanhado de garantias institucionais que permitissem atuação autônoma por minorias — algo que não se observa na CCAI. Também por isso, a participação de outros atores, de natureza politicamente contramajoritária, como o Judiciário e um órgão técnico especializado, é tão importante.

A falta de independência é agravada pela **insuficiência de meios**. Mesmo dentro do espaço estreito que formalmente cobre, a CCAI não dispõe de uma base de recursos humanos e materiais compatíveis com a magnitude da tarefa (Gonçalves e Bedritichuk 2024). É preciso capacidade própria para reduzir assimetrias informacionais, examinar documentos sensíveis, compreender técnicas operacionais e sustentar supervisão regular. Sem *staff* especializado, apoio analítico contínuo, softwares dedicados e fluxos seguros, isso é impraticável.

Por fim, há a **fragmentação sistêmica do controle**. A CCAI opera de forma solitária e desarticulada, mas não por opção — inexiste no Brasil uma rede de controle. Isso é grave, pois cada ator, por sua natureza, tem limitações intrínsecas: o Legislativo costuma ser governista e ter foco eleitoral; o judiciário é inerte; órgãos especializados têm menos legitimação pública; a sociedade civil, por sua vez, tem limitado acesso à informação. Por isso, a diversidade de atores com funções complementares e eventualmente coincidentes é fundamental. Ela permite que "a fraqueza de um ator [possa] ser suplantada pela força de outro, de modo que haja caminhos possíveis em caso de omissão" (Klöckner e Joia 2025, 14)

2.2 Riscos e oportunidades

A passagem do diagnóstico à proposta exige uma etapa intermediária de avaliação estratégica. Antes de discutir o desenho de uma reforma, é preciso compreender em que medida o contexto atual oferece condições para seu avanço — e em que medida tende a bloqueá-la, diluí-la ou desviá-la. O **Quadro 1**, a seguir, identifica os riscos e oportunidades relevantes que moldam essa janela de mudança.

Quadro 1. Riscos e oportunidades para uma reforma estrutural

Oportunidades	Riscos
Fatores políticos	
Crise de legitimidade O desgaste recente da atividade de inteligência, em especial a associação pública entre segmentos militares, golpismo e uso politizado da inteligência na Abin, cria uma janela favorável para reformas apresentadas como resposta de reconstrução institucional	**Inércia pró-sigilo** Em temas ligados à segurança, a tendência do sistema político e burocrático é preservar arranjos opacos, mesmo sem defesa aberta do *status quo*, sobretudo quando a alternativa exige confrontar estruturas historicamente blindadas
Conflitos de competência A persistência de atritos e zonas cinzentas entre investigação criminal e inteligência, bem como entre diferentes ramos da inteligência (de Estado, militar, policial, financeira e fiscal) cria ambiente favorável a uma reorganização	**Passivos ocultos** Abrir a "caixa preta" pode trazer custos políticos, jurídicos e reputacionais, incentivando resistência de atores beneficiados pela opacidade ou responsáveis pela baixa qualidade do controle

Convergências parciais Há incentivos possivelmente convergentes, ainda que distintos, entre atores que podem ganhar mais poder (Congresso, Judiciário, ANPD) e outros que buscam conviver com maior segurança jurídica (gestores e servidores de órgãos de inteligência)	**Baixa prioridade pública** Ainda que o tema ganhe visibilidade em momentos de crise, ele continua competindo em desvantagem com agendas de maior potencial eleitoral, o que reduz o incentivo de lideranças para investir capital político em reforma estrutural
Fatores discursivos	
Demanda por regulação tecnológica A maior densidade do debate sobre vigilância, privacidade, proteção de dados e *accountability* tecnológica torna mais inteligível a necessidade de controle e aumenta a pressão pública por regulação	**Narrativa de engessamento** A linguagem de urgência, risco e excepcionalidade pode deslocar a discussão do controle democrático para o medo de que qualquer escrutínio possa implicar perda de capacidade operacional
Fatores econômicos	
Mercado da conformidade A expansão de padrões regulatórios mais exigentes em governança tecnológica e auditabilidade pode favorecer fornecedores e consultorias interessadas em operar em ambiente mais estável e reputacionalmente seguro	**Mercado da opacidade** Fornecedores e intermediários cuja vantagem competitiva dependa de caixa-preta técnica, assimetria informacional e informalidade contratual tendem a ver a reforma como ameaça a seus interesses

O quadro sugere que a **janela de reforma é real, mas instável**. As oportunidades decorrem, sobretudo, de uma combinação incomum entre desgaste reputacional recente, maior inteligibilidade pública do problema e incentivos parciais à

reorganização institucional. Ao mesmo tempo, os riscos não se concentram em uma oposição frontal e homogênea, mas em mecanismos mais difusos de bloqueio: inércia burocrática, baixa prioridade política, medo de exposição de passivos ocultos e narrativas que tendem a apresentar qualquer aumento de controle como ameaça à capacidade operacional.

São duas as implicações estratégicas. A primeira é que a proposta deve contemplar não apenas uma **agenda** de contenção democrática, mas também a promoção de **segurança jurídica** para a atuação de servidores e gestores e a reconstrução pública da **legitimidade**. A segunda é que seu desenho deve ser suficientemente robusto para enfrentar a opacidade existente **sem inviabilizar as atividades**. É a partir desse terreno — promissor, mas atravessado por ambiguidades — que se pode passar, então, à formulação da proposta.

3 Proposta

A proposta legislativa a seguir estrutura o controle das atividades de inteligência como um sistema contínuo, escalonado e institucionalmente distribuído. A **íntegra** das proposições normativas está nos **apêndices**.

Este capítulo divide-se em **três seções**. A primeira, de **detalhamento**, expõe os elementos centrais do modelo: estrutura, instâncias de controle e regime de tratamento de dados. A segunda trata da **arquitetura legislativa**, explicando a distribuição do sistema entre uma proposta de emenda à Constituição (PEC), dois projetos de lei (PL) e um projeto de resolução do Congresso Nacional (PRN). A terceira, por fim, apresenta a **teoria da mudança** que fundamenta a proposta, articulando diagnóstico, mecanismos institucionais e efeitos esperados.

3.1 Detalhamento

3.1.1 Estrutura

Rede de controladores

O modelo proposto estrutura o controle das atividades de inteligência como uma rede de controladores, e não como atribuição concentrada em um único órgão. A premissa é simples: nenhuma instituição, isoladamente, reúne legitimidade democrática, capacidade técnica, competência processual, especialização regulatória e abertura social suficientes para controlar, sozinha, uma atividade marcada por sigilo estrutural, assimetria informacional e elevada complexidade tecnológica. Por isso, o sistema distribui funções entre instâncias distintas, organizadas de forma complementar, conforme consta na **Figura 3**.

Figura 3. Rede de controladores

Um novo órgão

A única peça nova dessa rede é a Autoridade Nacional de Controle das Atividades de Inteligência (Ancai), órgão de controle especializado, vinculado ao Congresso Nacional, com função de controle especializado e intervenção judicial.

Considerando que se trata de órgão novo, antes de avançar para a arquitetura do controle, convém explicitar a lógica de sua criação e os critérios que orientam o seu desenho institucional.

A literatura especializada converge no diagnóstico de que o controle na era digital precisa de **alta *expertise*** e capacidade de **monitoramento contínuo**, o que invariavelmente demanda uma autoridade especializada (Broeders et al. 2019; Gill 2020; Cahane 2021). Não por acaso, diversos países já contam com instituições dessa natureza, como o *Investigatory Powers Commissioner's Office* (IPCO), no Reino Unido, a *Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* (CTIVD), nos Países Baixos, e o *Tilsynet med Efterretningstjenesterne* (TET), na Dinamarca.

No caso da Ancai, a principal referência para sua formulação foi a autoridade francesa a *Commission Nationale de Contrôle des Techniques de Renseignement* (**CNCTR**). O diferencial dessa autoridade é a prerrogativa de participar como um **terceiro *de facto* no processo** de autorização das atividades de inteligência — elemento considerado como fundamental para a arquitetura aqui proposta, conforme detalhado na **seção** que trata do controle judicial.

Foi também por essa razão que se descartou a utilização do **TCU** como órgão central desse arranjo. Sua vocação institucional é a da auditoria e do controle externo clássico, não a de interveniente permanente em processos judiciais. Mesmo abstraindo essa dimensão processual, permanece um segundo desencaixe: o controle da inteligência exige monitoramento contínuo, com capacidade para acompanhar fluxos, sistemas e conformidade ao longo do tempo, e não apenas ciclos de fiscalização baseados em achados posteriores.

Em termos de formato institucional, por sua vez, **CNJ** e **CNMP** oferecem **referências** úteis, pois demonstram ser possível reunir os atributos essenciais ao

controle especializado — autonomia funcional, administrativa e orçamentária, estabilidade institucional e posição clara no sistema de freios e contrapesos — sem converter o órgão em um poder hipertrofiado ou dotado de iniciativa legislativa ampla. No desenho aqui proposto, essa lógica é reforçada por sua **vinculação ao Legislativo**, que deve aprovar os seus **diretores**. As indicações do colegiado foram articuladas de modo a representar a diversidade política e garantir a base técnica: são 8 pelas lideranças parlamentares, 3 pela ANPD e 2 pela OAB.

O desafio, portanto, é de calibração. Um órgão como a Ancai deve ter blindagem suficiente para assegurar independência real e capacidade técnica, mas sem elevar desnecessariamente o custo político de sua criação nem concentrar poder em excesso. O desenho busca responder a esse problema combinando três dimensões: **força técnica**, para produzir controle qualificado e contínuo; **capacidade processual**, para participar do controle judicial e acionar o Judiciário quando necessário; e **integração democrática**, para operar como órgão auxiliar do Parlamento, com prestação de contas e ancoragem republicana.

3.1.2 Instâncias

Controle parlamentar

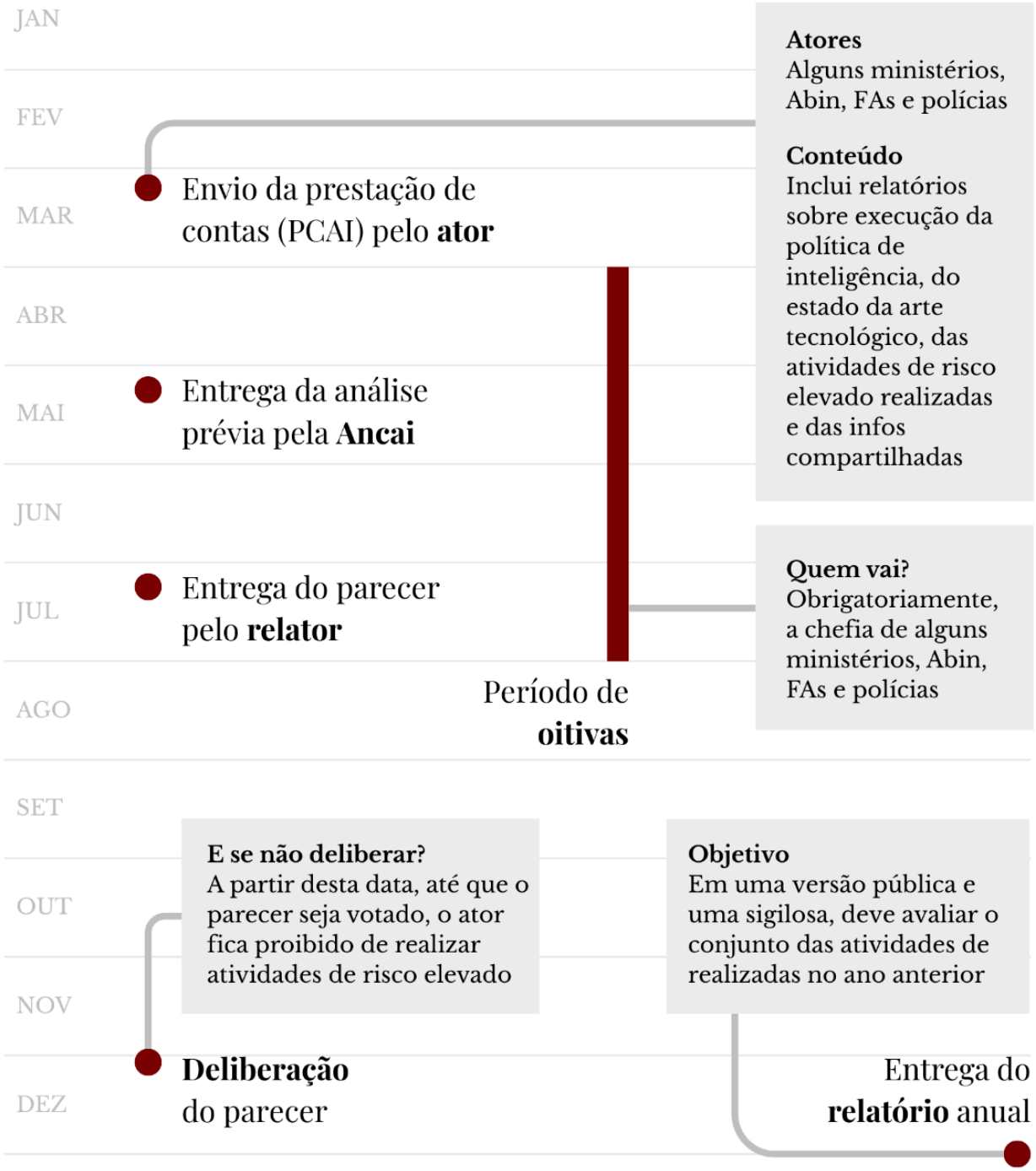
A pedra fundamental de um sistema republicano é a exigência de uma **política de inteligência**. Sem ela, falta o parâmetro elementar para distinguir mandato legítimo de desvio de finalidade. Por isso, a proposta exige que **cada ente** federativo tenha sua própria política de inteligência, aprovada **em lei** (e não mais por decreto), devendo seratualizada a cada quatro anos e estruturada em **horizontes de 4, 10 e 20 anos**, de modo que induza planejamento de longo prazo compatível com a complexidade dos desafios contemporâneos.

O segundo passo é a **sabatina de autoridades estratégicas** na cadeia de inteligência, isto é, aquelas que concentram maior poder sobre funções intrusivas. A proposta, por isso, amplia o rol de cargos sujeitos à aprovação prévia após arguição pública, abrangendo, além do diretor-geral da **Abin**, chefes de centro de inteligência das **Forças Armadas** e dirigentes das unidades **policiais** especializadas em inteligência. Propõe-se, também, que as sabatinas deixem a Comissão de Relações Exteriores e passem à CCAI, de modo a concentrar no foro especializado as funções de direção, acompanhamento e responsabilização da atividade.

No controle posterior, propõe-se uma prestação de contas regular, em dois níveis distintos. O primeiro é o nível macro, tradicional, ligado ao controle externo clássico das finanças públicas. Aqui, a proposta exige que o **parecer prévio** sobre as contas anuais do chefe do Executivo contenha seção específica sobre atividades de inteligência. O segundo é o nível da fiscalização operacional, voltado à atividade em si, realizado por instâncias específicas de controle e centrado na Prestação de Contas das Atividades de Inteligência (**PCAI**).

Essa PCAI é composta por quatro documentos: o Relatório de Execução da Política (REP), o Relatório de Estado Tecnológico (RET), o Relatório de Atividades de Risco Elevado (RAR) e o Relatório de Compartilhamento de Informações (RCI). Devem encaminhá-la anualmente os atores assim discriminados na **Figura 4**, **independentemente de solicitação**.

Figura 4. Fluxo anual e padronizado da CCAI



O conteúdo é desenhado para permitir fiscalização real: o REP conecta estrutura, estratégias, histórico de atuação, indicadores e despesas à política aprovada; o RET expõe *softwares*, bases de dados e equipamentos usados; o RAR permite escrutínio sobre medidas mais gravosas; e o RCI revela a circulação institucional das informações produzidas.

Além dos documentos acima, a Casa Civil fica obrigada a entregar um quarto: o **Relatório de Soberania Nacional**. Sua função é acrescentar ao controle uma dimensão muitas vezes negligenciada: a dependência tecnológica. Seu conteúdo deve indicar o grau de exposição do país a tecnologias estrangeiras utilizadas na atividade, os principais obstáculos à redução dessa dependência e as medidas adotadas, em curso e necessárias para superá-la no curto, médio e longo prazo.

Para que esse controle não dependa da boa vontade das maiorias de ocasião, o processo precisa ser **orgânico e automático**. A proposta, por isso, estabelece envio anual obrigatório da PCAI, distribuição automática da relatoria no âmbito da comissão, remessa imediata à Ancai para análise preliminar e prazos improrrogáveis para cada etapa, vedando expedientes que favoreçam paralisação ou captura do procedimento. A ideia é simples: controle parlamentar que depende de impulso eventual tende a ser seletivo e vulnerável tanto à conveniência política quanto à pressão externa.

A mesma lógica vale para as **oitivas de autoridades**. Para reduzir pressões políticas e evitar que o escrutínio seja acionado apenas em contextos de crise ou conflito, a proposta pressupõe rotinas periódicas de comparecimento e prestação de esclarecimentos pelas autoridades centrais da área, conforme recomendam Gonçalves e Bedritichuk (2024), que trabalham diretamente com a Comissão.

Em paralelo, a proposta ainda dá ao parlamentar titular das comissões especializadas **prerrogativa própria para acessar informações**, sem depender de

anuência do colegiado ou de qualquer outra autoridade, evitando a captura do órgão. Com isso, fecha-se o ciclo de legitimação política da inteligência: o Parlamento fixa direção, legitima as chefias, recebe prestação de contas, acompanha a execução e dispõe de meios permanentes para avaliar o sistema.

Escrutínio de contratos

Melhor que resolver uma crise, é evitar que ela aconteça. Por isso, o Estado deve avaliar, desde a contratação, quais capacidades são compatíveis com o mandato dos atores de inteligência, em que condições elas serão usadas e com que grau de auditabilidade. Por isso, o modelo proposto trata a **contratação de soluções** tecnológicas como um ponto sensível de controle *ex ante*.

A premissa é simples: tecnologias opacas, não auditáveis ou incompatíveis com a legislação brasileira tendem a produzir, mais adiante, custos muito maiores de fiscalização, contenção e reparação. O controle da inteligência, assim, não deve começar apenas no momento da autorização judicial ou da auditoria operacional, mas já no desenho do **edital**, na escolha do fornecedor e na definição das salvaguardas que acompanharão a implementação da ferramenta.

A proposta cria, para esse fim, uma dupla camada documental. De um lado, o Relatório de Impacto de Vigilância (**RIV**), produzido pelo próprio ator de inteligência contratante, voltado ao tipo de tecnologia ou serviço objeto do edital. De outro, o Relatório de Impacto à Proteção de Dados Pessoais (**RIPD**), elaborado pelo potencial contratado, voltado à solução concreta que pretende oferecer. O primeiro examina riscos sistêmicos e institucionais associados ao uso da capacidade tecnológica; o segundo detalha os processos de tratamento de dados pessoais e as medidas de mitigação adotadas no produto ou serviço específico.

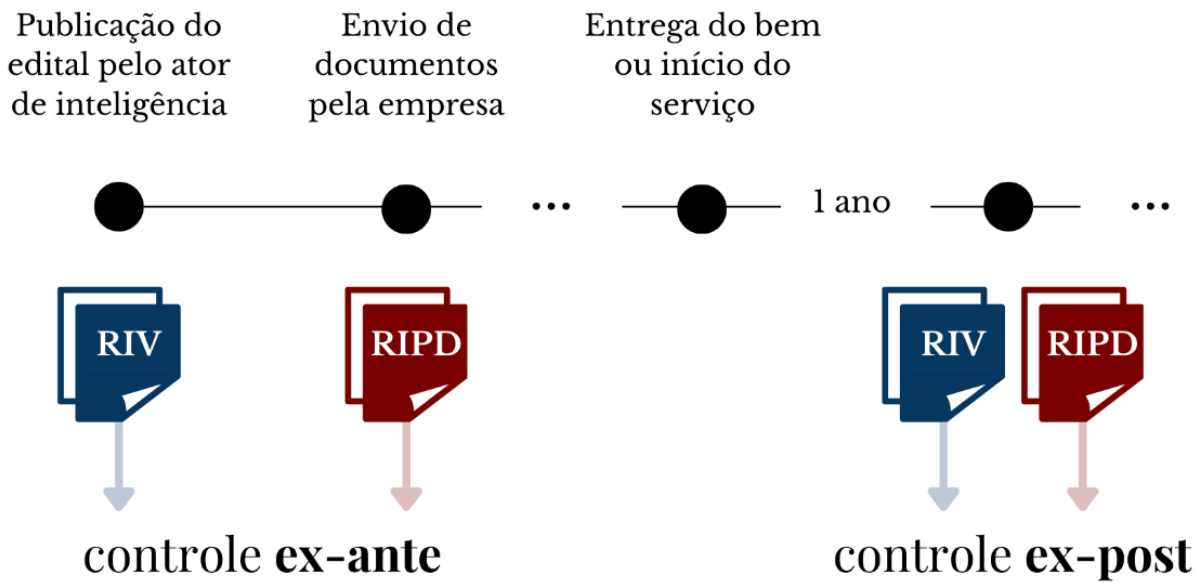
As diferenças entre eles seguem detalhadas na **Figura 5**.

Figura 5. RIV e RIPD – Diferenças

	RIV **Relatório de Impacto de Vigilância**	RIPD **Relatório de Impacto à Proteção de Dados Pessoais**
Quem produz	ator de inteligência	empresa contratada
Destinatária	Ancai	ANPD
Objeto	tipo de tecnologia (abstrato)	modelo (concreto)
Objetivo	avaliar os riscos sociais gerais associados ao uso	avaliar riscos à exposição de dados pessoais
Momento da entrega	no edital; 1 ano após início do contrato; e quando requerido pela destinatária	idem
Conteúdo mínimo	descrição técnica fluxos de dados base legal finalidade específica demonstração da necessidade análise de riscos medidas para mitigar riscos condições de implementação	processos de tratamento medidas para mitigar riscos

A **lógica é complementar**: o RIV pergunta se o Estado deve incorporar determinada capacidade e o RIPD, se a solução concreta proposta atende aos parâmetros legais e técnicos exigidos. Em conjunto, os dois relatórios permitem que o controle especializado incida tanto sobre a capacidade abstrata que se pretende adquirir quanto sobre o modelo concreto que se pretende contratar. Os documentos devem ser apresentados conforme a **Figura 6**.

Figura 6. RIV e RIPD – Fluxo de envio



A repartição institucional acompanha essa lógica. A **Ancai** deve ser cientificada da juntada do RIV, e a **ANPD**, da juntada do RIPD. Além disso, cada uma pode exigir, a qualquer tempo, a apresentação de novo relatório em sua esfera de competência. O arranjo reforça a ideia de especialização complementar: a Ancai

examina a conformidade sistêmica, operacional e estratégica da tecnologia com o regime jurídico da inteligência; a ANPD, os riscos e salvaguardas ligados ao tratamento de dados pessoais. Não se trata de duplicação, mas de divisão racional do escrutínio.

Essa engenharia se completa com um **cadastro unificado de contratos** cujo objeto esteja relacionado a atividades de risco elevado. Os atores de inteligência deverão inserir nesse cadastro, mantido pela Ancai, informações como finalidade, unidades usuárias, íntegra dos instrumentos licitatórios e contratos, despesas associadas e os RIVs e RIPDs correspondentes. O objetivo é elevar a rastreabilidade das contratações e permitir que o controle parlamentar e especializado acompanhe, de forma comparada e contínua, quais capacidades tecnológicas estão sendo incorporadas ao sistema de inteligência.

Por fim, o modelo reconhece que o problema não se limita à legalidade formal da contratação. Em alguns casos, a própria origem da tecnologia, a localização do tratamento de dados e a dependência de **soluções estrangeiras** podem gerar riscos à soberania nacional e à efetividade do controle. Por isso, o desenho normativo exige detalhamento específico quando a tecnologia for desenvolvida por organização estrangeira ou implicar operações de tratamento de dados fora do território nacional, inclusive com justificativa para a não adoção de solução nacional e análise dos riscos para a auditabilidade pelo controle brasileiro.

Autorização judicial

Dada a direção política e garantida a conformidade das soluções tecnológicas, o controle chega ao **caso concreto**: a operação específica, o alvo determinado e a

técnica efetivamente empregada. Há, portanto, uma lógica de proteção por camadas: política, ferramentas, uso.

Ao adotar um sistema de autorização externa, comum em democracias consolidadas, tem-se como premissa que, nas hipóteses de maior risco, a inteligência não pode atuar apenas com base em confiança institucional. Para resolver isso, o sistema adotado **segue o modelo francês**, que introduz no processo de autorização, além do requerente e do juízo, uma terceira instituição, independente e externa à estrutura de poder do requerente — no nosso caso, a Ancai.

Tal demanda parte do entendimento de que um dos maiores limites à eficácia do controle judicial tradicional, presente em sistemas como o dos EUA e do Reino Unido é a **baixa densidade dialética** do procedimento. Em ambos os casos, a iniciativa parte do Executivo e a decisão judicial é tomada sem a oitiva de outra parte que possa tensionar pela conformidade legal.

Nos **EUA**, o requerimento é formulado por agente federal, com aprovação prévia apenas do *Attorney General*, que não tem status de controlador externo, sendo após submetido diretamente ao juiz[4]. No **Reino Unido**, a situação se repete, havendo submissão ao *Judicial Commissioner*, após aval do *Secretary of State*, que não representa uma camada de controle externo[5].

[4] United States Code, title 50, sec. 1804(a): "Each application for an order approving electronic surveillance under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 1803 of this title. Each application shall require the approval of the Attorney General..."; sec. 1805(a): "Upon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order...". (Estados Unidos 2025)

[5] Investigatory Powers Act 2016, sec. 19(1): "The main duty of the Judicial Commissioner to whom a decision to issue a warrant is referred under this Chapter is to review the Secretary of State's conclusions as to the following matters..."; Explanatory Notes, para. 77: "The decision of the Secretary of State to issue the warrant must then be approved by a Judicial Commissioner before the warrant can be issued." (Reino Unido 2016)

O risco desse modelo é a conversão do controle em **chancela quase automática**. Em procedimentos marcados por sigilo, sem contraditório institucional e sem a intervenção de um terceiro independente, o julgador tende a decidir dentro de um circuito fechado de informação, o que favorece a deferência e esvazia a densidade do controle. Não por acaso, a corte estadunidense aprovou mais de 99,97% dos cerca de 33 mil pedidos feitos entre 1979 e 2012. (Clarke 2014). Por isso, esse sistema é qualificado na literatura como ***rubber stamp*** – indicando que se trata de um mero carimbo legitimador.

A **França** foge dessa lógica, e o faz aproveitando a estrutura de sua autoridade especializada — justamente o que se pretende construir no modelo brasileiro. Por lá, a autorização do *Premier ministre* é concedida **após análise da CNCTR** e, se deferida apesar de parecer desfavorável, a autoridade aciona o controle judicial (*Conseil d'État*)[6], o que introduz uma camada com dialética externa, evitando o fenômeno do *rubber stamp*.

Para delimitar o que deve passar por esse escrutínio reforçado, criou-se a categoria das **atividades de inteligência de risco elevado** (IREs). Nela, estão compreendidos os casos em que o risco se torna mais intenso em razão das pessoas que têm como alvo ou das técnicas que são empregadas, conforme detalhado na **Figura 7.**

[6] Code de la sécurité intérieure, art. L. 821-1: "La mise en œuvre sur le territoire national des techniques de recueil de renseignement (...) est soumise à autorisation préalable du Premier ministre, délivrée après avis de la Commission nationale de contrôle des techniques de renseignement"; "Lorsque l'autorisation est délivrée après un avis défavorable de la Commission nationale de contrôle des techniques de renseignement, le Conseil d'État est immédiatement saisi...".

Figura 7. Atividades de inteligência de risco elevado

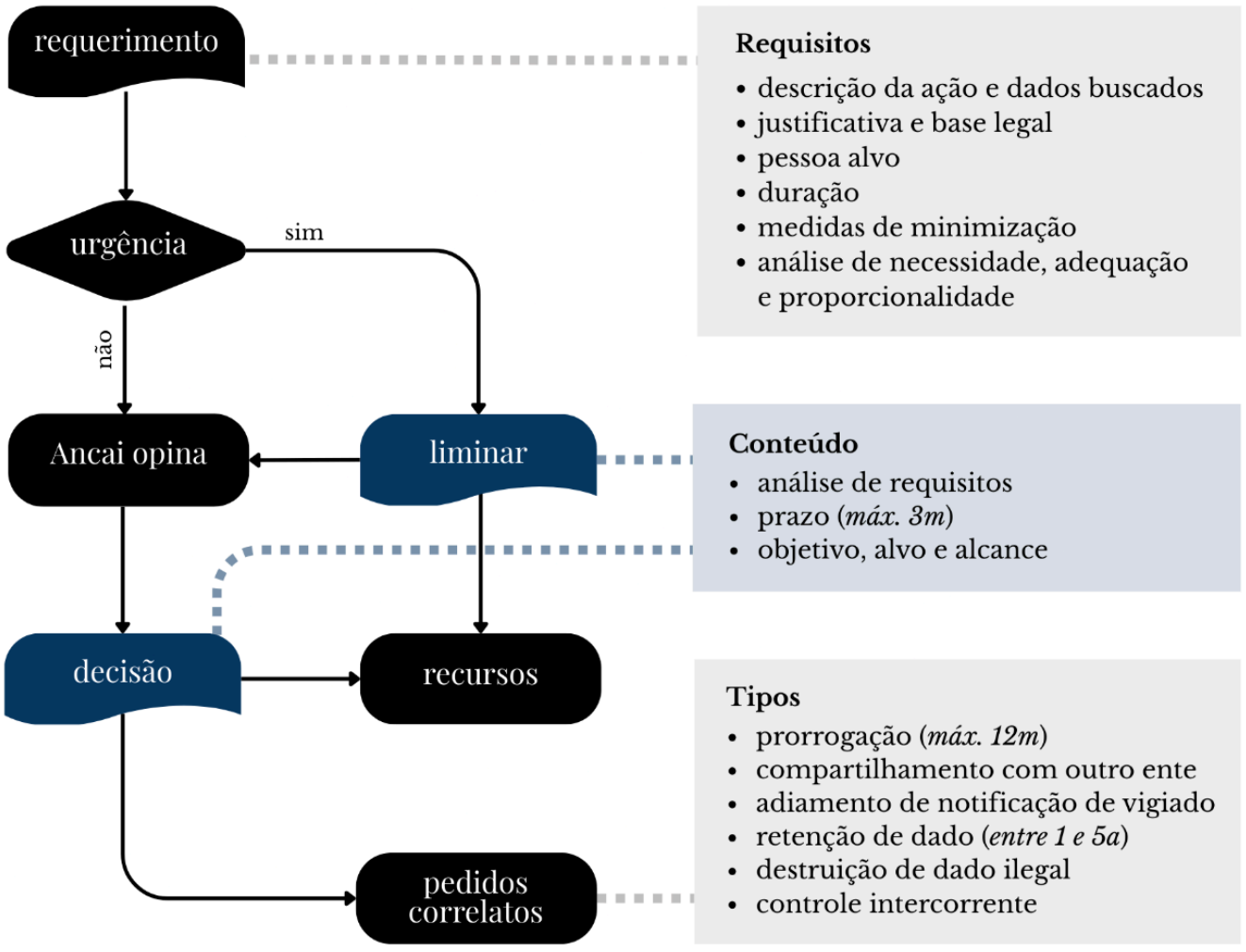
Importa notar que a criação da categoria das IREs não equivale à outorga geral de poderes a qualquer ator de inteligência. Seu papel é definir o universo de hipóteses submetidas ao regime reforçado de controle. A pergunta sobre quais técnicas e alvos podem ser mobilizados por cada órgão ou entidade permanece remetida à sua **lei específica** de regência.

Uma vez delimitadas, em lei específica, as técnicas e os alvos que podem ser mobilizados por cada ator, o procedimento adotado para a submissão do pedido é o da **dupla autorização**. A inspiração é o modelo inglês (*double lock*), que prevê uma primeira autorização pelo controle interno, em nível ministerial, e uma segunda, externa, por autoridade judicial especializada. Em relação ao caso inglês, porém, há uma diferença crucial: aqui, a segunda fase não é unilateral, havendo previsão de dialética pela Ancai, na forma da **Figura 8**.

Figura 8. Sistema de dupla autorização, com exemplo

Na proposta, os pedidos são analisados por **órgão colegiado especializado**, composto por membros com mandato fixo e único, sendo as partes processuais restritas ao representante do ator de inteligência e à Ancai. A dinâmica processual está sumarizada na **Figura 9**, tendo o Código de Processo Civil como regra subsidiária.

Figura 9. Procedimento judicial



Quanto ao **prazo padrão do mandato**, optou-se por três meses por se tratar de marco compatível com referências centrais do direito comparado: o modelo alemão, que fixa esse teto no regime ordinário de autorização, e o modelo norte-americano, que adota, como regra geral, o prazo de noventa dias[7].

O controle judicial, ressalte-se, não se esgota na autorização da medida ou em sua prorrogação. Ele também incide sobre atos supervenientes relacionados aos dados coletados, como a **retenção** por período superior, o **compartilhamento** de dados com outro ente ou país e o adiamento da **notificação do vigiado**[8].

Além disso, o sistema cria um canal seguro para o controle intercorrente pela Ancai, que pode provocar o Judiciário para requerer a **destruição de dado** obtido ou retido ilegalmente e a suspensão, limitação ou cancelamento de atividades que tenham **extrapolado o mandado** concedido.

Monitoramento contínuo

O controle da inteligência não pode se esgotar na autorização judicial e na revisão posterior. Entre uma e outra, é necessário um órgão que seja capaz de acompanhar a execução concreta da atividade, verificar a aderência ao mandado, detectar desvios em tempo útil e agir antes que a ilegalidade se consolide. No modelo proposto, essa função cabe à **Ancai**, que atua não apenas no acompanhamento de medidas autorizadas, mas também na apuração de denúncias, realização de auditorias e assessoramento técnico ao Parlamento.

[7] § 10(5) "In den Fällen der §§ 3 und 5 ist die Anordnung auf höchstens drei Monate zu befristen [...]" (Alemanha 2001); 50 U.S.C. § 1805(d)(1) "An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less [...]" (Estados Unidos 2025)
[8] A notificação do vigiado é instrumento de controle social examinada em seção própria.

Para poder preencher a lacuna entre o filtro de entrada e a responsabilização tardia, a Ancai não pode depender de pedidos de informação. Em matéria de inteligência, controle efetivo exige **acesso direto, irrestrito e autônomo** a dados, sistemas, logs, equipamentos e instalações. Se o controlador depende de solicitação prévia, intermediação do controlado ou seleção daquilo que lhe será mostrado, a assimetria informacional já venceu o controle antes mesmo de ele começar. Por isso, a proposta segue o **modelo dinamarquês** de acesso[9], assegurando à Ancai acesso pleno, inclusive em tempo real.

Controle social

A história mostra que os **grandes avanços no controle** da inteligência nasceram de fora das instituições formais. Como observam Gill (2022) e Kniep et al. (2024), eles tendem a emergir pela pressão externa: escândalos, denúncias, mobilização pública, jornalismo investigativo, litigância e crítica acadêmica. É por isso que o controle social merece, nesse campo, deferência máxima. Não porque seja o arranjo ideal, mas porque, durante muito tempo, foi o único capaz de romper zonas de opacidade que os mecanismos formais de supervisão não conseguiam atravessar.

Tal protagonismo **revela por si uma insuficiência estrutural**: o controle social ocupou esse lugar porque, em muitos contextos, os mecanismos institucionais disponíveis eram fracos, descontínuos ou simbólicos. A proposta aqui apresentada busca justamente alterar esse quadro, construindo instâncias com capacidade real.

[9] A autoridade especializada dinamarquesa (TET) atua como órgão independente de controle externo e não se limita a requisitar informações ao controlado. A lei lhe garante acesso, a qualquer tempo e sem ordem judicial, aos locais de administração dos tratamentos, aos pontos de acesso aos dados e aos meios técnicos empregados. Isso inclui a possibilidade de consultar registros e conhecer diretamente as informações no próprio local de armazenamento (Dinamarca 2013a; Dinamarca 2013b).

Se esse desenho se mostrar viável, o controle social poderá deixar de operar como substituto precário da institucionalidade e passará a ocupar o lugar que lhe é mais próprio: o de última *ratio*, acionada apenas para **expor falhas residuais**.

Isso não significa supor que os novos mecanismos não falharão. Provavelmente falharão. A diferença é que, se implementados, falharão dentro da margem de erro do que há de melhor nos *benchmarks* contemporâneos. Ainda assim, nenhuma arquitetura de controle é completa sem uma dimensão social robusta — não apenas para reagir às brechas que persistem, mas também (e especialmente) para **dar legitimidade direta** ao sistema que só faz sentido existir se for nos proteger.

No modelo proposto, essa dimensão social se organiza em **quatro pilares**.

O primeiro é o da **participação política**, por meio da criação do **Conselho Nacional** de Controle das Atividades de Inteligência, órgão consultivo da Ancai. Sua função é propor diretrizes estratégicas, produzir relatórios anuais de avaliação da política e dos órgãos de controle, sugerir ações à Ancai, elaborar estudos, promover debates e audiências públicas e difundir conhecimento sobre o controle da inteligência. Sua composição busca assegurar pluralidade, com representantes do CNJ, do CNMP, da OAB, da Federação Nacional dos Jornalistas, de entidades voltadas à proteção de denunciantes e vítimas da violência estatal, de organizações de proteção de dados, de instituições científicas e do setor empresarial nacional ligado à área.

O segundo pilar é o da **transparência**, que alimenta especialmente esse trabalho deliberativo e crítico: ANPD, tribunais de contas, CCAI e Ancai devem produzir relatórios anuais sobre suas atividades de controle da inteligência, contando sempre com uma versão pública, permitindo que o debate social não dependa apenas de crises, vazamentos ou revelações extraordinárias, mas também de fluxos institucionais regulares de informação.

O terceiro pilar é estruturado por meio de um **sistema seguro de denúncias**, centrado na Ancai. A proposta não trata a denúncia como mecanismo residual de baixa confiança, mas como válvula institucional indispensável em um campo em que a opacidade, por definição, dificulta a reação tempestiva das instâncias formais. Por isso, a Ancai recebe e apura denúncias, adota medidas de proteção e concentra, sob sigilo reforçado, os elementos de identificação do denunciante. A regra é a denúncia institucional protegida.

A proposta admite, ainda, em caráter excepcional, a **denúncia pública** por servidor quando já tiver havido denúncia formal e inexistir qualquer encaminhamento apto a demonstrar que existe uma reação institucional adequada, conforme recomendam os **Princípios de Tshwane**[10]. Servidores precisam dispor de canais seguros para relatar ilegalidades sem medo de prisão, destruição de carreira ou outras formas de retaliação, devendo-se autorizar uma rota excepcional de exteriorização quando os canais internos forem ineficazes.

O quarto pilar, por fim, é o da **notificação do vigiado**, que consagra a construção de um sistema de inteligência à serviço da democracia. A inspiração aqui vem do **modelo alemão**, que estabelece o dever de comunicação posterior à pessoa que foi alvo uma vez encerrada a medida[11]. Na arquitetura proposta, esse dever se

[10] Os Princípios de Tshwane são um conjunto de diretrizes internacionais elaboradas por especialistas e organizações da sociedade civil para definir quando o sigilo por segurança nacional é legítimo e quando deve ceder à transparência e à responsabilização. Eles também estabelecem parâmetros para a proteção de denunciantes que revelem ilegalidades, abusos ou violações graves de direitos humanos. (Open Society Justice Initiative 2013)

[11] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10), § 12(1): "Beschränkungsmaßnahmen nach § 3 sind dem Betroffenen nach ihrer Einstellung mitzuteilen. Die Mitteilung unterbleibt, solange eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann (...) Erfolgt die nach Satz 2 zurückgestellte Mitteilung nicht binnen zwölf Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der Zustimmung der G10-Kommission." (Alemanha 2001)

materializa quando a pessoa foi objeto de atividade de risco elevado, sendo dever do ator de inteligência repassar-lhe, em até 12 meses, as seguintes informações:

- número do processo que autorizou a atividade;
- juízo responsável pela autorização;
- ator de inteligência responsável pela medida;
- tipo de técnica de coleta utilizada (sem revelar método);
- período em que a coleta ocorreu;
- tipo e alcance das informações que foram obtidas;
- prazo de retenção dos dados coletados.

A proposta admite que a notificação do vigiado seja **adiada**, mas apenas por decisão judicial e em hipóteses restritas: quando sua realização comprometer operações em curso, afetar gravemente a segurança nacional ou expuser terceiros a risco grave. Se o adiamento ultrapassar um ano, passa a exigir renovações periódicas; se superar cinco anos, além da renovação quinquenal, depende também de manifestação unânime do conselho diretor da Ancai.

A **dispensa** da notificação, por sua vez, é ainda mais excepcional, seguindo graduação também usada pelo direito alemão. Só pode ser deferida quando, passados cinco anos do encerramento da medida, a razão que justificaria o adiamento continuar presente por prazo indeterminável, os dados já tiverem sido apagados por todos os atores que a eles tiveram acesso e houver manifestação favorável, também unânime, da direção da Ancai.

3.1.3 Regime de tratamento de dados

A arquitetura proposta só se mantém em pé se houver regras de tratamento de dados voltadas especificamente para a inteligência. Sem elas, o sistema perde auditabilidade, põe em risco grave a soberania nacional e a segurança das operações e, ainda, abre espaço para coletas massivas desnecessárias e desproporcionais às finalidades legais da atividade.

O primeiro passo é afastar a **lógica de excepcionalidade difusa** que historicamente cercou o tema e afirmar que, também aqui, coleta, análise, retenção e circulação de dados devem obedecer a finalidade, necessidade, minimização, temporalidade e auditabilidade.

Nesse desenho, estende-se à **ANPD** o dever de zelar pelas novas regras de tratamento, nos mesmos termos (com algumas adaptações) do que já faz no âmbito da LGPD: acompanhar contratações, auditar, expedir recomendações, requer explicações e, se for preciso, aplicar sanções.

A proposta estabelece, entre outros **parâmetros estruturais**:

- **separação entre inteligência e investigação** criminal, vedando integração automática de bases e compartilhamento fora das hipóteses legais;
- **auditabilidade** desde a concepção, com rastreabilidade integral em *log* inviolável, cadeia de custódia e destruição imediata de dado obtido ou retido ilegalmente;
- **privacidade** desde a concepção e por padrão, vedando a vigilância indiscriminada e garantindo o escrutínio de toda a nova solução tecnológica adotada;

- **revisão humana** prévia em qualquer ação que restrinja direitos ou transforme alguém em alvo de atividade de inteligência;
- **retenção mínima** e temporalmente limitada, rompendo com a naturalização da retenção e a convertendo-a em novo momento de justificação e controle — dado coletado não é, por isso só, dado legitimamente acumulável.

No caso da retenção, estabelece os seguintes **prazos**:

- *logs* de softwares dos atores de inteligência: 30 anos;
- dados pessoais, como regra geral: 10 anos;
- dados obtidos em atividades de inteligência de risco elevado:
    - regra geral: **exclusão imediata** quando do fim do mandado;
    - exceção: mediante justificativa expressa e segundo escalonamento progressivo de controle:
        a. até 1 ano, basta comunicação ao juízo;
        b. entre 1 e 5 anos, exige-se autorização anual;
        c. acima de 5 anos, autorização quinquenal e manifestação favorável unânime da Ancai.

Buscou-se no direito comparado as referências para a definição dos prazos, conforme exemplos que seguem. A legislação aplicável ao serviço de inteligência interna da Alemanha admite para certas categorias de dados pessoais retenção de

até dez anos, com revisão periódica[12]. No regime estadunidense, dados pessoais de estrangeiros obtidos por inteligência de sinais não podem, em regra, ser mantidos por mais de cinco anos, salvo decisão excepcional em sentido diverso[13].

No âmbito do **compartilhamento** a proposta é mais rígida, acabando com a possibilidade de circulação difusa e pouco rastreável de informações entre órgãos. Ela submete o compartilhamento a hipóteses legais expressas e adota a lógica de **controle na origem**. Isso significa que o ator que produziu o dado controla seu compartilhamento, sua classificação de sigilo e qualquer alteração posterior desse regime, sendo vedada a retransmissão sem sua anuência.

Ao mesmo tempo, a circulação passa a ser cercada por exigências de **minimização** e **traçabilidade**, com registro de data, finalidade e responsáveis pelo envio e recebimento. Além disso, fica determinado o dever, antes de qualquer compartilhamento, de anonimização ou pseudonimização de elementos capazes de identificar **fontes humanas** — um dado que não deve ser revelado nem mesmo por ordem judicial ou requisição de autoridade de controle.

Com isso, a proposta substitui a lógica informal do "compartilha-se porque é útil" por uma lógica jurídica mais densa: compartilha-se apenas quando há base legal, finalidade delimitada, lastro documental e responsabilidade claramente atribuída. No caso específico dos dados obtidos em atividades de alto risco, o **compartilhamento entre atores** deve seguir requisitos mais rígidos, conforme exposto na **Figura 10**.

[12] BVerfSchG, § 12 Abs. 3: "[...] Gespeicherte personenbezogene Daten über Bestrebungen nach § 3 Absatz 1 Nummer 1, 3 und 4 sind spätestens zehn Jahre nach dem Zeitpunkt der letzten gespeicherten relevanten Information zu löschen [...]" (Alemanha 2024).
[13] PPD-28, Section 4(a)(i): "[...] Information for which no such determination has been made shall not be retained for more than 5 years [...]" (Estados Unidos 2014).

Figura 10. Requisitos para compartilhamento entre atores de inteligência

outro ator é	requisitos para compartilhar
do mesmo ente	ciência do juízo
de outro ente	autorização judicial
estrangeiro	autorização judicial + análise de risco de compartilhamento internacional favorável + análise de legalidade do meio de obtenção do dado (se Brasil estiver recebendo) em todos os casos é necessário termo de cooperação

Essa racionalidade se adensa ainda mais no **compartilhamento internacional.** Aqui, a proposta não se contenta com cláusulas genéricas de cooperação: ela exige **análise de risco específica**, seguindo o **modelo holandês**[14]. Por meio dela, a Ancai deve aferir se o país destinatário oferece **salvaguardas institucionais** compatíveis com a proteção de direitos, considerando, entre outros elementos, a qualidade do

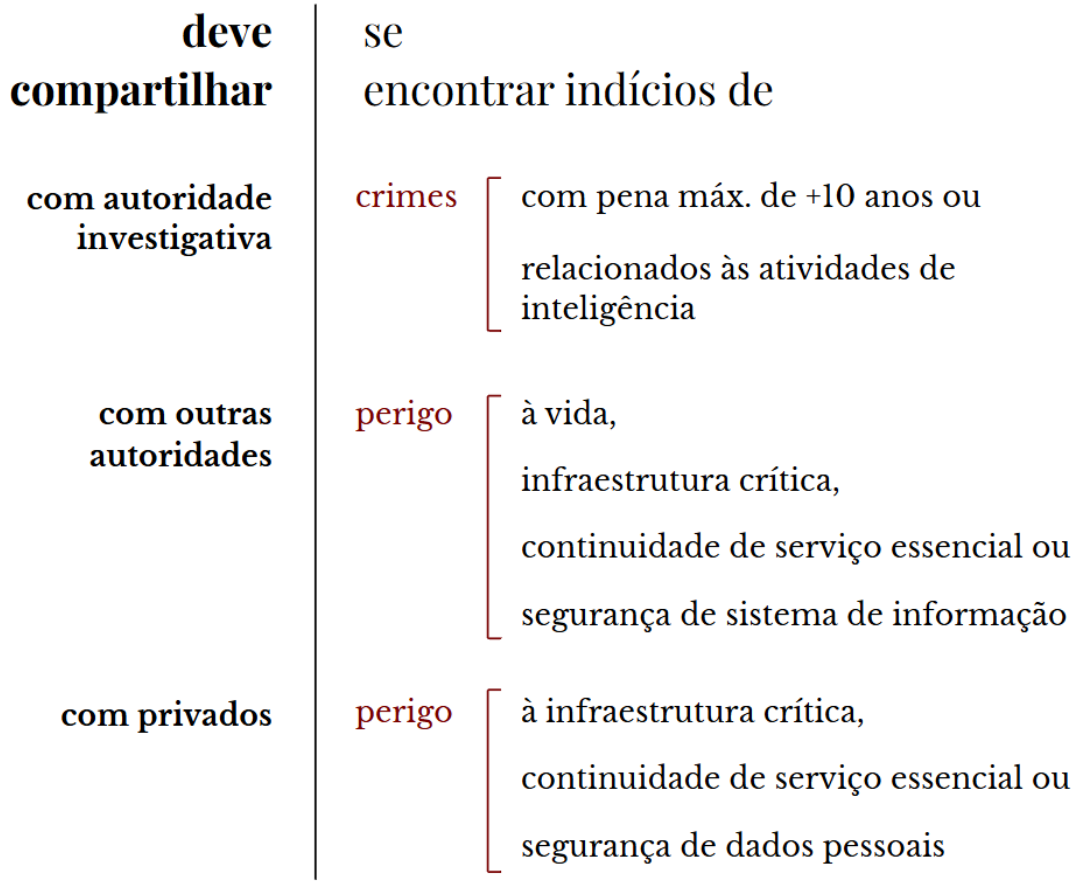
[14] A lei holandesa exige uma análise prévia antes que se estabeleça cooperação com serviço de inteligência estrangeiro. Essa avaliação é feita pelo próprio serviço de inteligência interessado em cooperar e considera, entre outros fatores, a inserção democrática do órgão parceiro, o respeito a direitos humanos, sua confiabilidade, seus poderes legais e o nível de proteção de dados oferecido. A relação de cooperação só pode ser firmada após autorização ministerial (Países Baixos 2017). No modelo aqui proposto, sugere-se acolher o ideia, mas mudar o responsável pela avaliação. Em vez de cada ator fazer a sua, concentra-se na Ancai, evitando retrabalho, duplicidade analítica e o enviesamento.

controle externo da inteligência, a existência de mecanismos de prevenção à tortura, proteção ao jornalismo, proteção de testemunhas e proteção de denunciantes. Além disso, o termo de cooperação só será admissível se assegurar acesso total das autoridades de controle externo de ambos os países aos dados compartilhados. Busca-se garantir que o compartilhamento internacional deixe de ser simples questão diplomática ou operacional e passe a ser também tema de **soberania**, **auditabilidade** e confiança institucional recíproca.

A proposta também enfrenta uma dúvida procedimental hoje desregulamentada: quando uma informação crítica deve ser **comunicada a terceiros?** Para evitar que essa decisão fique entregue à improvisação, o modelo cria hipóteses expressas de dever de informar, acionadas quando surgirem **indícios de criminalidade grave** ou **perigos extremos** a bens especialmente sensíveis, conforme sintetizado pela **Figura 11**. A vertente relativa aos crimes dialoga com a experiência alemã, que obriga o compartilhamento com a persecução penal quando houver base factual para suspeita de crime com pena máxima de ao menos dez anos[15].

[15] Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (BVerfSchG), § 21(1)–(2): “Das Bundesamt für Verfassungsschutz übermittelt personenbezogene Daten an eine zuständige inländische Strafverfolgungsbehörde, wenn bestimmte Tatsachen den Verdacht einer besonders schweren Straftat begründen (...)”; “Eine besonders schwere Straftat (...) ist eine Straftat, die im Höchstmaß mit Freiheitsstrafe bedroht ist von 1. mindestens zehn Jahren (...) (Alemanha 1990)

Figura 11. Hipóteses de dever de informação do ator de inteligência



Por fim, propõe-se a vedação do compartilhamento por meio de **aplicativos de mensagens instantâneas** ofertados ao público geral ou sob controle efetivo de pessoa jurídica estrangeira (WhatsApp e Telegram cairiam por qualquer desses critérios). Trata-se de regra que dialoga diretamente com a agenda contemporânea de soberania digital e segurança da informação. Nesse sentido, o

Brasil está avançando: já temos o **msg gov**, um aplicativo de mensageria segura, com criptografia de Estado, desenvolvido pela própria Abin (2025).

3.2 Arquitetura legislativa

O desenho adotado foi estruturado por meio de três tipos de proposição legislativa, já que o problema opera em planos normativos distintos e seu tratamento por um único instrumento produziria mais ruído do que coerência. O pacote é composto por: uma Proposta de Emenda à Constituição (PEC), dois Projetos de Lei (PLs) e um Projeto de Resolução do Congresso Nacional (PRN).

A **PEC** concentra os ajustes de freios e contrapesos e o rearranjo de competências, o que inclui: a competência legislativa da União para editar normas gerais sobre inteligência, a criação da Ancai e os fundamentos do controle judicial — incluindo atores e partes do processo.

Os **PLs** concentram os conceitos, as definições de atividade de risco elevado, os deveres gerais dos atores, o procedimento judicial, o sistema de denúncias, o dever de notificação do vigiado, o tratamento de dados e as alterações de competência da ANPD. A parte da ANPD, especificamente, é de iniciativa legislativa privativa do chefe do Poder Executivo. Por isso, dividiu-se o PL em dois, mantendo-se no segundo apenas este item.

Por fim, o **PRN** trata daquilo que é próprio da esfera legislativa: a reestruturação da CCAI, com seus novos fluxos, deveres e adequações de prerrogativas, e o funcionamento da Ancai.

3.3 Teoria da mudança

A teoria da mudança desta proposta parte da premissa de que o controle da inteligência no Brasil não será transformado por ajustes marginais, sendo dependente, em qualquer caso, da criação de um sistema de **controle judicial** prévio e de uma **autoridade especializada** (Ancai). Com esses dois vetores estabelecidos no texto constitucional, deve haver pressão normativa para a **mudança do restante do sistema**.

O controle judicial exigirá a delimitação normativa do que é inteligência controlada, dos critérios para requerer e autorizar medidas sensíveis e do procedimento adequado para tanto. A instituição da Ancai, por sua vez, implicará a acumulação de capacidade técnica e redução paulatina da assimetria informacional. Ao longo do tempo, isso tende a aumentar o nível de auditabilidade do sistema, a responsabilização por abusos e fortalecer, por reação, os controles internos, reduzindo a sensação de que a atividade opera em regime de exceção e ampliando sua legitimidade democrática.

No **curto prazo**, o efeito esperado é um **choque de formalização**. As atividades de inteligência tendem a operar em ritmo menor, com aumento do custo decisório, pois procedimentos, sistemas, controles e competências ainda estarão em fase de construção. Essa etapa envolve adaptação legal, elaboração de protocolos, treinamento, início de organização dos novos controladores e revisão de rotinas antes pouco formalizadas. Não se deve esperar fluidez imediata. O mais provável é uma fase de arrumação da casa, acompanhada de **discursos políticos de travamento**, que precisarão ser enfrentados como parte normal de uma transição institucional dessa escala.

Não se assume, aqui, como pressuposto decisivo, a **cooperação** espontânea dos órgãos controlados. Se não houver adesão procedimental mínima, a tendência é outra: paralisação de atividades, responsabilização ou perda de espaço institucional. A teoria da mudança, portanto, não depende de boa vontade generalizada, mas da combinação entre novo eixo constitucional de controle e custo crescente da não adaptação.

No **médio prazo**, a principal marca da mudança tende a ser a **apropriação institucional** dos novos espaços de controle. A CCAI deve ganhar mais protagonismo no debate estratégico do Congresso; a Ancai e a ANPD começam a consolidar sua presença; o controle judicial passa a operar de modo menos excepcional e mais estruturado; e surgem os primeiros casos de responsabilização produzidos por controle institucional, e não por vazamento. É também nessa etapa que o controle interno tende a reagir mais fortemente, por medo de sanção, revisão ou exposição. Como consequência, os **conflitos aumentam antes de diminuir**. Só no **longo prazo** deve ocorrer maior **estabilização** do sistema, com rotinas mais claras, menor dependência de informalidade, maior celeridade nos processos de autorização, mais **previsibilidade** procedimental e maior profissionalização tanto da inteligência quanto de seu controle.

Em síntese, a teoria da mudança da proposta pode ser resumida assim: ao constitucionalizar o controle judicial das atividades de inteligência de alto risco e instituir uma autoridade especializada, independente e com acesso pleno, o Brasil aumenta o custo da opacidade e reduz o custo da *accountability*. Esse deslocamento não produz efeitos instantâneos; ele primeiro desacelera, formaliza e reorganiza. Depois, redistribui poder e induz responsabilização. Só mais tarde tende a estabilizar uma inteligência menos opaca, mais controlável e mais legítima como função de Estado.

4 Viabilidade

4.1 *Stakeholders* e incentivos

A viabilidade de uma reforma do controle da inteligência depende da forma como ela redistribui poder, custos, proteção e visibilidade entre os atores relevantes. Por isso, o quadro a seguir mapeia os principais *stakeholders* com capacidade de **apoiar, moldar, retardar ou resistir** à proposta, bem como os incentivos que tendem a orientá-los.

Os **atores** foram selecionados por sua posição no processo decisório ou por serem diretamente afetados pelo redesenho institucional pretendido:

- Congresso Nacional e Presidência da República são, por definição, os **tomadores de decisão**, os centros indispensáveis de qualquer mudança legislativa dessa natureza;
- os órgãos de inteligência, civis e militares, aparecem porque são os **destinatários** mais imediatos da reforma e, justamente por isso, tendem a querer influenciar o seu desenho;
- Ministério Público e tribunais de contas entram porque a proposta tende a **reduzir seu protagonismo** implícito ou potencial;
- em sentido inverso, Poder Judiciário e ANPD figuram como atores com possibilidade de **ganho institucional**, à medida que a reforma tende a lhes atribuir funções mais estruturadas;

- os atores **privados** (fornecedores de tecnologia e consultorias) foram incluídos porque seus modelos de negócio podem ser diretamente afetados por exigências de auditabilidade, rastreabilidade e governança;
- por fim, a **sociedade civil**, em especial academia, imprensa e organizações de direitos, permanece como ator indispensável porque acompanha historicamente esse debate, influencia sua inteligibilidade pública e pode ampliar ou reduzir sua saliência política.

Quadro 1. Principais *stakeholders* e incentivos em disputa

Stakeholder	Pode apoiar pois	Pode resistir pois
Congresso Nacional	(1) a reforma reforça a centralidade fiscalizatória do Legislativo sobre uma atividade historicamente pouco escrutinada, aumentando margem de barganha institucional; (2) a CCAI se projeta como um centro decisivo do debate político estratégico; (3) lideranças de maioria e minoria podem ver valor adicional nos novos instrumentos de supervisão	(1) parte da base do governo pode temer elevação do custo político para o Executivo em exercício; (2) a inércia institucional se impõe mesmo sem coalizão explícita, o que fica reforçado em temas que envolvem a fiscalização de setores que exercem o monopólio da violência; (3) mesmo diante de escândalos, para evitar conflitos, lideranças podem advogar por reformas de fachada

Stakeholder	Pode apoiar pois	Pode resistir pois
Governo Federal	(1) a reforma pode gerar coordenação, previsibilidade, segurança jurídica e redução do risco de crises futuras; (2) Gabinete da Presidência e Casa Civil podem enxergar valor em reorganizar o sistema e reconstruir legitimidade; (3) o MJSP pode perceber ganho em padronização e maior clareza para a inteligência policial; (4) MD e GSI podem ver na reforma uma oportunidade de dissociar a inteligência militar da sombra do golpismo e reafirmá-la como função de Estado compatível com lealdade constitucional	(1) a proposta reduz opacidade sobre estruturas que hoje operam sem controle externo, havendo receio das consequência políticas decorrente das ilegalidades estruturais que devem aparecer; (2) MD e GSI podem repercutir com força as sensibilidades da inteligência militar, intocada desde a redemocratização; (3) o MJSP pode entender que o custo procedimental para a inteligência policial supera o ganho de segurança jurídica; (4) o governo, em sua arena interna de acomodação entre custos políticos concorrentes, favorece soluções mais cautelosas ou diluídas
Inteligência civil	regras mais claras, maior delimitação do objeto controlado e procedimentos mais densos podem trazer legitimidade, previsibilidade e segurança jurídica, o que pode ser especialmente relevante para: (1) a Abin, como instituição, cuja exposição política e midiática minou...	a reforma aumenta trilhas documentais e reduz zonas de informalidade, o que (1) causa temor em servidores que utilizam a estrutura do Estado para finalidade ilegal; (2) pode ser percebido como fonte de custo procedimental, perda de discricionariedade e maior risco de responsabilização retrospectiva; (3) pode gerar receio de que controles mais...

Stakeholder	Pode apoiar pois	Pode resistir pois
	...sua legitimidade pública, impactando diretamente suas possibilidades de se firmar como órgão de Estado forte e estratégico; (2) para servidores que temem por seguir trabalhando em ambientes desregrados, ficando expostos a ameaças e responsabilização futura	...densos se convertam em disputa corporativa, vazamento ou uso político da supervisão
Inteligência militar	parte do setor pode enxergar a reforma como oportunidade de profissionalização, clarificação institucional e reconstrução de legitimidade — especialmente relevante após o reforço público da associação entre segmentos militares, golpismo e uso politizado da inteligência	(1) o campo é historicamente resguardado de escrutínio fino, podendo uma reforma ser percebida como erosão desse espaço privilegiado de exceção; (2) pode haver resistência ao significado político implícito de reconhecer que o modelo atual é insuficiente
Ministério Público	a reforma o desonera de uma função institucionalmente dissonante, tecnicamente difícil e politicamente custosa — embora o controle da inteligência não integre sua função...	(1) a proposta reduz protagonismo potencial, limitando espaço de intervenção em certas frentes; (2) aumenta a visibilidade sobre suas próprias atividades de inteligência, hoje sem escrutínio estruturado

Stakeholder	Pode apoiar pois	Pode resistir pois
	...constitucional, recai frequentemente sobre o MP a expectativa difusa de que fiscalize esse campo, em especial porque controla a investigação criminal e o imaginário público tende a confundir investigação com inteligência	
Tribunais de contas	a reforma o desonera de uma função institucionalmente dissonante, tecnicamente difícil e politicamente custosa — embora a Constituição dê a função de controle operacional, sua estrutura não tem vocação para monitoramento granular, sendo voltada a controle financeiro e política em nível macro	(1) podem ler a reforma como redução simbólica de protagonismo; (2) podem interpretá-la como afirmação de inadequação institucional em um tema que poderia, em tese, ser ampliado no futuro para sua esfera
Poder Judiciário	a reforma amplia seu poder sobre um campo em que hoje sua intervenção é limitada e pouco estruturada, aumentando sua barganha institucional	(1) a proposta pode elevar carga procedimental; (2) pode gerar atrito com outros centros institucionais

Stakeholder	Pode apoiar pois	Pode resistir pois
ANPD	(1) a reforma amplia seu protagonismo no controle especializado da dimensão informacional; (2) reforça sua centralidade institucional em matéria sensível e de alta relevância pública	(1) a expansão de competências pode vir associada a aumento de encargos, complexidade institucional e tensão com atores poderosos; (2) pode não haver contrapartida clara de estrutura, recursos e delimitação funcional
Fornecedores de tecnologia	(1) a reforma pode funcionar como fonte de selo reputacional positivo para alguns produtos, diferenciando empresas associadas a soluções auditáveis daquelas marcadas por vínculos com usos autoritários de vigilância; (2) podem enxergar possibilidade de crescimento na compra de suas soluções caso essas atividades sejam mais legitimadas	(1) exigências de auditabilidade, rastreabilidade, documentação e verificabilidade independente podem exigir redesign de produtos; (2) soluções cujo valor comercial dependa de baixa transparência podem ficar inviabilizadas; (3) a padronização séria e transparência real ao controle diminui o valor capturado por intermediários que prosperam em ambientes pouco inteligíveis e institucionalmente cinzentos
Consultorias	podem enxergar oportunidade em nichos de compliance, adequação regulatória, auditoria, governança informacional, revisão procedimental e implementação técnica do novo modelo	a padronização séria e transparência real ao controle diminui o valor capturado por intermediários que prosperam em ambientes pouco inteligíveis e institucionalmente cinzentos

Stakeholder	Pode apoiar pois	Pode resistir pois
Sociedade civil	academia, imprensa e entidades de defesa da privacidade, da liberdade de expressão e de direitos humanos defendem accountability, redução de opacidade, proteção de direitos e ampliação do controle democrático	podem surgir grupos que atuem como proxy de atores insatisfeitos com o aumento de accountability, buscando revestir interesses de preservação da opacidade com narrativas de que mudanças seriam um risco à segurança

4.2 Alternativas regulatórias

O ponto de partida da análise de alternativas é a compreensão de que o problema em exame não admite soluções de fachada sem risco de agravamento institucional. Em matéria de inteligência, uma **reforma que simula controle** sem efetivamente alterar opacidade, incentivos e capacidade de supervisão pode ser pior do que a manutenção do arranjo atual. Ao revestir a atividade de aparência de legalidade e *accountability* sem criar mecanismos reais de escrutínio, esse tipo de reforma engana a população, desmobiliza a pressão por mudança estrutural e legitima, sob nova roupagem, práticas potencialmente ilegais ou abusivas.

Para fins de comparação, foram consideradas as duas principais respostas institucionais hoje em circulação no debate brasileiro. A primeira é representada pelas emendas feitas na **PEC 18/2025**, que inserem o debate da inteligência em uma proposta originalmente voltada à segurança pública. A segunda é um **pacote**

elaborado pela própria CCAI para instituir um marco legal da inteligência e qualificar o controle parlamentar.

4.2.1 Emendas à PEC 18/2025

A PEC 18/2025 não surgiu como resposta específica ao problema do controle da inteligência. Seu objeto original era a **segurança pública**. As disposições sobre inteligência apareceram depois, como "**penduricalhos**" agregados ao texto ao longo da tramitação. Esse ponto importa porque ajuda a explicar parte de suas limitações: o tratamento da inteligência não nasce de um esforço concentrado de reconstrução da arquitetura de controle, mas de acréscimos inseridos em uma proposta concebida para outro centro de gravidade institucional.

As emendas à PEC têm o mérito de introduzir o tema no plano constitucional e de reconhecer, ainda que de modo parcial, a necessidade de um maior controle, havendo inclusive proposta de controle judicial prévio. Isso, porém, não basta para qualificá-la como resposta adequada ao problema regulatório.

Primeiro, pois as emendas que tratam do controle judicial têm um limite grave de escopo. Ao referirem a necessidade de autorização prévia para "técnicas e meios sigilosos da Abin", constroem um comando estreito demais, pois **concentra o problema na Abin**, como se ela fosse o centro exclusivo da inteligência invasiva no país — deixando à margem, por exemplo, a inteligência militar e policial. Em termos regulatórios, a alternativa não enfrenta adequadamente nem a indeterminação do objeto controlado nem o escopo insuficiente do controle.

Outro limite está na **ausência de solução para lidar com a opacidade** operacional. As emendas não criam mecanismo institucional apto a produzir um sistema de

monitoramento contínuo, mantendo a aposta no controle parlamentar — que é importante, mas insuficiente, conforme já elaborado no diagnóstico.

4.2.2 Pacote da CCAI

O pacote em questão foi anunciado no final de 2025 pela própria CCAI (Brasil, CN 2025) em **resposta direta à crise** de legitimidade do sistema de inteligência, especialmente sob a pressão política criada pelo escândalo da chamada "Abin paralela" e pela ADPF 1143. Seu conteúdo é composto pelo **PL 6.423/2025**, que busca instituir um marco da inteligência, e pelo **anteprojeto de um PRN** que altera o funcionamento da CCAI.

Quanto ao **PL**, seu principal mérito está em estabelecer **o controle judicial** sobre algumas técnicas e em oferecer algum grau de **densificação conceitual** da atividade. O projeto, no entanto, continua sem resolver o **problema do escopo** do controle. Embora não reduza o universo regulado apenas à Abin (como é feito nas emendas da PEC), ele ainda deixa mal resolvida a situação de outros polos sensíveis, como os estados e o MP.

Além disso, por não estruturar adequadamente um procedimento judicial, o projeto **arrisca posicionar o MP como ator** processual — o que é inadequado uma vez que ele próprio produz inteligência policial. Diante da inexistência da previsão de uma autoridade especializada, a alternativa também não seria boa: deixar o juiz praticamente sozinho diante do pedido, transformando o controle judicial em mero rito homologatório.

O problema se agrava quando entram em cena questões de competência judicial. Sem reordenação constitucional prévia, as **decisões seriam na primeira instância**, demasiadamente sensível para o tema — inclusive se o alvo fosse uma autoridade

com prerrogativa de foro penal. Sem uma PEC organizando a distribuição de competências entre tribunais, o projeto arrisca produzir um controle judicial extremamente vulnerável.

O **PRN**, por sua vez, tem como principal mérito obrigar a **comunicação prévia** à comissão de operações classificadas como ultrassecretas. Embora se trate de processo de notificação, e não de autorização, esse mecanismo é importante pois reforça a mudança de um paradigma da reação para um de prevenção, além de contribuir para reduzir a assimetria informacional. A principal fragilidade aqui é que o critério ficará a cargo do próprio controlado — um tipo de equívoco comum nas arquiteturas de controle. Na prática, basta utilizar outro nível de classificação, e não haverá necessidade de comunicação, criando-se assim um incentivo inadequado para que operações sejam classificadas como secretas (com sigilo de até 15 anos), e não ultrassecretas (com sigilo até 25).

Além disso, a proposta contempla outras duas medidas importantes, ambas acolhidas no desenho de PRN deste *white paper*:

- determina a **oitiva anual** de gestores e a **entrega anual de relatórios** de trabalho do controlado, ambos **independente de requerimento**. Isso é crucial, pois reduz a pressão política em torno de pedidos, cria fluxo de trabalho e aumenta a relevância da Comissão, tendo reflexo direto na independência dos membros, na maturidade e na saliência do tema; e

- muda da forma de **ingresso no colegiado**, que deixa de ter membros natos. Hoje, metade da comissão é ocupada automaticamente por líderes da maioria e da minoria e pelos presidentes das comissões de relações exteriores. Esse desenho é problemático, pois leva ao colegiado parlamentares que nem sempre têm interesse direto na matéria e que já acumulam funções políticas de alta centralidade. A adoção do critério de

> proporcionalidade partidária é mais adequada, porque permite às lideranças indicar membros com maior vocação, disponibilidade e aderência temática para o exercício da função.

O pacote melhora a disciplina da atividade, dá mais relevância e força ao controle parlamentar e planta uma semente tímida de um controle judicial. No conjunto, são avanços inéditos — mas ainda muito **distantes da construção de um sistema** de controle. As soluções são parciais e repletas de lacunas que arriscam repetir erros clássicos já identificados, com evidências substantivas, pela literatura internacional.

Em eventual aprovação do texto, por isso, é essencial que não se crie uma **ilusão de controle**. Afinal, não são estabelecidos incentivos concretos para evitar que ilegalidades como as que deram origem à crise de legitimidade atual sigam ocorrendo. O alerta, nesse sentido, é para que o legislador tenha cuidado para não utilizar a oportunidade histórica apresentada com provisões incapaz de atacar as causas de fundo que criam a opacidade crônica do sistema.

A despeito dessas ponderações, é possível, sim, que eventual aprovação contribua em termos de aumentar a **maturidade pública** e a **saliência política** do tema. Mesmo limitados, os comandos do projeto podem ajudar a construir a compreensão coletiva de que técnicas intrusivas de inteligência exigem controle prévio, o que por si só seria um passo importante no enfrentamento do problema. Nesse sentido, talvez o PL possa funcionar como um primeiro passo imperfeito — desde que, ressalte-se, não seja tratado como solução suficiente, e sim como piso mínimo a partir do qual um sistema robusto precisa ser estabelecido.

4.2.3 Síntese

A comparação entre alternativas não pode ser conduzida como se qualquer avanço formal bastasse. Em matéria de inteligência, a viabilidade política só é um critério relevante quando associada a propostas capazes de enfrentar as causas diagnosticadas e de atender aos requisitos mínimos de um controle democrático eficaz: universalidade, substantividade, independência, proporcionalidade e caráter sistêmico. Do contrário, a **alternativa mais viável** pode ser apenas a que melhor se acomoda às estruturas que produziram o próprio problema.

Sob esse prisma, embora a PEC 18/2025 e o pacote da CCAI possam conter **ganhos marginais** e aparentem **maior transitabilidade** política, nenhuma das duas alternativas oferece resposta com densidade suficiente para enfrentar o problema regulatório em sua escala real. À luz desses parâmetros, a alternativa mais consistente continua sendo o pacote integrado proposto neste trabalho, por ser a única formulação que procura enfrentar de modo combinado os principais vetores do problema: escopo insuficiente, baixa densidade do controle, dependência do próprio controlado, opacidade operacional e fragmentação institucional.

Isso não impede reconhecer eventual utilidade do **pacote da CCAI como etapa de transição**. Seu valor, porém, depende de uma condição narrativa e política decisiva: não ser vendido como solução suficiente. Se for tratado como porta de entrada, piso inicial ou primeiro movimento útil para a construção futura de um modelo funcional de controle, sua aprovação pode contribuir para elevar a saliência do tema, consolidar premissas mínimas de supervisão e preparar terreno para uma reforma mais robusta, como a trazida neste documento.

5 Referências

Alemanha. 1990. *Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (BVerfSchG)*. BGBl. I S. 2954, de 20 dez. 1990.

Alemanha. 2001. *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10)*. BGBl. I S. 1254, de 26 jun. 2001.

Alemanha. 2024. *Bundesverfassungsschutzgesetz (BVerfSchG)*, § 12. Berlim: Bundesministerium des Innern. https://www.gesetze-im-internet.de/bverfschg/__12.html

Born, Hans, e Ian Leigh. 2005. *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*. Oslo: Publishing House of the Parliament of Norway.

Brasil. Agência Brasileira de Inteligência (Abin). 2025. "Aplicativo de mensageria msg gov é apresentado no ABINCast." *Gov.br*, 29 dez. 2025.

Brasil. Agência Brasileira de Inteligência (Abin). 2026. *Relatório de Gestão Correcional 2025*. https://www.gov.br/abin/pt-br/acesso-a-informacao/corregedoria/relatorio-de-gestao-correcional-2025

Brasil. Congresso Nacional (CN). Comissão Mista de Controle das Atividades de Inteligência. 2025. *Resultado da 7ª Reunião da CCAI, em 10 de dezembro de 2025*. Brasília: Secretaria-Geral da Mesa, 10 de dezembro de 2025. https://legis.senado.leg.br/sdleg-getter/documento/download/6abd9fd0-ef34-4287-9bfe-5059b6dcf730

Brasil. Conselho Nacional do Ministério Público (CNMP). 2024. *Resolução nº 292, de 28 de maio de 2024*. Brasília, DF. https://www.cnmp.mp.br/portal/images/CALJ/resolucoes/Resoluo-n-292.pdf.

Brasil. Ministério Público Federal (MPF). 2022. *Procedimento Administrativo nº 1.00.000.004218/2022-00*. Brasília, DF.

Brasil. Polícia Federal (PF). 2025. *Relatório final do INQ 4781/DF*. Brasília, DF.

Brasil. Supremo Tribunal Federal (STF). 2024. *Arguição de Descumprimento de Preceito Fundamental n. 1143/DF*. Brasília, DF.

Brasil. Supremo Tribunal Federal (STF). 2025. *Ação Penal n. 2668*. Brasília, DF.

Brasil. Superior Tribunal de Justiça (STJ). 2016. *Recurso Especial nº 1.439.193/RJ.* Julgado em 14 de junho de 2016.

Brasil. Tribunal de Contas da União (TCU). 2022. *TC-014.760/2021-5*. Brasília, DF.

Broeders, Dennis, Sergei Boeke, e Ilina Georgieva. 2019. *Foreign Intelligence in the Digital Age: Navigating a State of 'Unpeace'*. The Hague: The Hague Program for Cyber Norms. https://papers.ssrn.com/abstract=3493612

Cahane, Amir. 2021. "The (Missed) Israeli Snowden Moment?" *International Journal of Intelligence and CounterIntelligence* 34 (4): 694–717. https://doi.org/10.1080/08850607.2020.1838902

Clarke, Conor. 2014. "Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate." *Stanford Law Review Online* 66: 125–137.

Defty, Andrew. 2020. "From Committees of Parliamentarians to Parliamentary Committees: Comparing Intelligence Oversight Reform in Australia, Canada, New Zealand and the UK." *Intelligence and National Security* 35 (3): 367–384. https://doi.org/10.1080/02684527.2020.1732646

Dhillon, Amrit, e Michael Safi. 2021. "Indian Supreme Court Orders Inquiry into State's Use of Pegasus Spyware." *The Guardian*, 27 de outubro de 2021. https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware

Dinamarca. 2013a. *Lov om Forsvarets Efterretningstjeneste (FE)*. Lov nr. 602 af 12. juni 2013. Copenhague: Retsinformation.

Dinamarca. 2013b. *Forslag til lov om Forsvarets Efterretningstjeneste (FE)*. Lovforslag nr. LSF 163, fremsat den 27. februar 2013. Copenhague: Folketinget/Retsinformation.

Estados Unidos. 2014. Presidential Policy Directive 28: Signals Intelligence Activities (PPD-28). Washington, DC: The White House. https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

Estados Unidos. 2025. United States Code. Title 50, secs. 1801–1885c. Washington, DC: Office of the Law Revision Counsel.

Figueiredo, Lucas. 2005. *Ministério do Silêncio: A História do Serviço Secreto Brasileiro de Washington Luís a Lula (1927–2005)*. Rio de Janeiro: Record.

França. 2026. *Code de la sécurité intérieure*. Paris: Légifrance.

Gera, Vanessa. 2024. “Poland’s PM Says Authorities in the Previous Government Widely and Illegally Used Pegasus Spyware.” *Associated Press News*, 13 de fevereiro de 2024. https://apnews.com/article/poland-government-pegasus-spyware-tusk-duda-78420fc7099401926d28b5be98669192

Gill, Peter. 2020. “Of Intelligence Oversight and the Challenge of Surveillance Corporatism.” *Intelligence and National Security* 35 (7): 970–989. https://doi.org/10.1080/02684527.2020.1783875

Gill, Peter. 2022. “Intelligence, Oversight and the Ethics of Whistleblowing: The Case of Witness K.” *Australian Journal of Human Rights* 28 (2–3): 206–224. https://doi.org/10.1080/1323238X.2022.2145834

Gonçalves, Joanisval Brito, e Rodrigo Ribeiro Bedritichuk. 2024. *Parliamentary Oversight of Intelligence in Brazil: Analysis and Proposals for Changes to the Joint Committee for the Oversight of Intelligence Activities (CCAI)*. Texto para Discussão 331b. Brasília: Senado Federal.

Hansén, Dan. 2023. “Assessing Intelligence Oversight: The Case of Sweden.” *Intelligence and National Security*. https://doi.org/10.1080/02684527.2023.2222534.

Hillebrand, Claudia. 2019. “Placebo Scrutiny? Far-Right Extremism and Intelligence Accountability in Germany.” *Intelligence and National Security* 34 (1): 38–61. https://doi.org/10.1080/02684527.2018.1540175

Jasutis, Grazvydas. 2021. *Parliamentary Oversight of Military Intelligence*. Geneva: DCAF. https://www.dcaf.ch/parliamentary-oversight-military-intelligence

Klöckner, Conrado, e Luiz Antonio Joia. 2025. *“External oversight of Intelligence activities in the digital age: An exploratory model.” Brazilian Journal of Public Administration* 59 (3): e2024-0271. https://doi.org/10.1590/0034-761220240271

Kniep, Ronja, Lea Ewert, Brandon L. Reyes, Félix Tréguer, Emma McCluskey e Claudia Aradau. 2024. “Towards Democratic Intelligence Oversight: Limits, Practices, Struggles.” *Review of International Studies* 50 (1): 209–229. https://doi.org/10.1017/S0260210523000013

Lakhani, Nina. 2021. “Revealed: Murdered Journalist’s Number Selected by Mexican NSO Client.” *The Guardian*, 18 de julho de 2021. https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto

Moses, Lyria Bennett. 2022. “Oversight of Police Intelligence: A Complex Web, but Is It Enough?” *SSRN Electronic Journal* 60 (2). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4248480

Open Society Justice Initiative. 2013. *The Global Principles on National Security and the Right to Information (Tshwane Principles)*. New York: Open Society Foundations.

Países Baixos. 2017. *Wet op de inlichtingen- en veiligheidsdiensten 2017*. Stb. 2017, 317.

Parsons, Christopher. 2018. *"Law enforcement and security agency surveillance in Canada: The growth of digitally-enabled surveillance and atrophy of accountability" SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3130240

Parlamento Europeu. 2023. *European Parliament Draft Recommendation to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware*. B9-0260/2023. Bruxelas. https://www.europarl.europa.eu/doceo/document/B-9-2023-0260_EN.html

Ramiro, André. 2025. "Democratic Oversight of Government Hacking by Intelligence Agencies: A Critical Analysis of Brazil and Germany." *Weizenbaum Journal of the Digital Society* 5 (2). https://doi.org/10.34669/wi.wjds/5.2.3

Reino Unido. 2016. *Investigatory Powers Act 2016*. Londres: The National Archives.

Rocha, Antônio Sérgio. 2013. "Genealogia da Constituinte: do autoritarismo à democratização." *Lua Nova* 88: 29–87.

Scott-Railton, John, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano e Ron Deibert. 2022. *CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru*. The Citizen Lab Report no. 155. Toronto: University of Toronto. https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

Vieth, Kilian, e Thorsten Wetzling. 2019. *Data-Driven Intelligence Oversight: Recommendations for a System Update*. Berlin: Stiftung Neue Verantwortung. https://dx.doi.org/10.2139/ssrn.3505906

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

6.1 Proposta de Emenda à Constituição

Criação de uma autoridade especializada, estruturação do controle judicial e orientação geral das atividades de inteligência do país

PROPOSTA DE EMENDA À CONSTITUIÇÃO N. /2026

Legiscraft

Regula as atividades de inteligência, estabelecendo sistemas para o seu exercício e controle.

Art. 1º

Introdução à norma

Esta Emenda Constitucional cria os fundamentos para a realização de atividades de inteligência pelo Estado brasileiro, estabelecendo sistemas para o seu exercício e controle.

Art. 2º

Alterações do texto

A Constituição Federal passa a vigorar com as seguintes alterações:

Competência legislativa

I – fica inserido um novo inciso no art. 22, com a seguinte redação:

"**Art. 22**. .....

.....

XXXI – normas gerais da atividade de Inteligência."

Em linha similar, propuseram os parlamentares Fausto Pinato, Alberto Fraga e Laura Carneiro, em forma de emenda, no âmbito da PEC 18/2025.

Competência do Senado Federal

II – fica alterado o inciso II, do art. 52, que passa a ter a seguinte redação:

"**Art. 52**. .....

.....

II - processar e julgar os Ministros do Supremo Tribunal Federal, os membros do Conselho Nacional de Justiça e do Conselho Nacional do Ministério Público, os diretores da Autoridade Nacional de Controle das Atividades de Inteligência, o Procurador-Geral da República e o Advogado-Geral da União nos crimes de responsabilidade;

....."

Competência do Tribunal de Contas

III – fica inserido o § 5°, no art 71, com a seguinte redação:

"**Art. 71**. .....

.....

§ 5° Não cabe ao Tribunal de Contas da União a fiscalização operacional das atividades de inteligência."

Os tribunais de contas, como órgãos que auxiliam o parlamento na realização do controle externo, têm atribuição genérica que lhes permitiria, caso quisessem, realizar a fiscalização operacional das atividades de inteligência.

Na prática, isso nunca ocorreu, seja pela falta de cultura de controle dessas atividades, seja porque os tribunais têm a estrutura majoritariamente voltada a temas orçamentários, carecendo de expertise para tal fim.

No sistema ora proposto, cria-se uma autoridade específica para auxiliar o parlamento no controle externo das atividades de inteligência, a Ancai, seguindo-se o exemplo de outras democracias consolidadas.

Nessa nova configuração, a Ancai passa a dividir com os tribunais de contas a fiscalização contábil, financeira, orçamentária e patrimonial dessas atividades.

No entanto, fica restrito à Ancai a fiscalização operacional, dada a alta sensibilidade e especificidade da matéria.

Competência do Poder Legislativo

IV – no "TÍTULO IV – DA ORGANIZAÇÃO DOS PODERES", no "CAPÍTULO I – DO PODER LEGISLATIVO", a "SEÇÃO IX" fica renomeada para "DO CONTROLE EXTERNO, e passa a ter uma Subseção Única, contendo os arts. 75-A a 75-C, com a redação que segue:

"SEÇÃO IX
DO CONTROLE EXTERNO

.....

SUBSEÇÃO ÚNICA
DO CONTROLE DAS ATIVIDADES DE INTELIGÊNCIA

CCAI e Ancai

Art. 75-A. O controle externo das atividades de inteligência, a cargo do Poder Legislativo, será exercido por comissão parlamentar específica, com o auxílio da Autoridade Nacional de Controle das Atividades de Inteligência, à qual compete:

I – assessorar a comissão parlamentar de controle do Congresso Nacional na forma de ato próprio;

II – receber e apurar denúncias de abuso de poder e adotar medidas para proteger os denunciantes;

III – atuar nas ações judiciais de que trata o art. 144-E em defesa da conformidade constitucional e legal das atividades de inteligência;

IV – monitorar a atividade de inteligência autorizada na forma do inciso III;

V – expedir normativas complementares à legislação relacionada ao controle das atividades de inteligência.

§ 1º Enquanto não instalada a comissão parlamentar de que trata o caput, fica vedada, no âmbito do respectivo ente, a realização de atividades de inteligência de risco elevado, nos termos do § 1º do art. 144-E.

§ 2º Os órgãos e entidades que realizam atividade de inteligência prestarão contas de sua atuação operacional na forma de ato do Congresso Nacional, devendo a comissão de que trata o caput apreciá-las até 1º de dezembro do ano subsequente ao período a que se referem, ficando vedada, a partir dessa data, a realização de atividades de risco elevado até a deliberação final.

§ 3º A Autoridade Nacional de Controle das Atividades de Inteligência:

I – é órgão constitucional autônomo, auxiliar do Poder Legislativo, com autonomia funcional, administrativa e orçamentária;

II – elaborará sua proposta orçamentária anual, que será encaminhada ao Congresso Nacional para consolidação na proposta orçamentária do Poder Legislativo; e

III – terá sua organização e funcionamento disciplinados por ato do Congresso Nacional.

§ 4º Os entes subnacionais poderão instituir autoridades análogas à referida no caput, vinculadas ao parlamento local, para fins de execução das competências de que tratam os inciso I e II.

A principal referência para a construção da Ancai é a autoridade francesa de controle externo, que participa do processo decisório (opinando sobre autorizações) e tem capacidade de provocar o Judiciário.

Ao pensar a sua arquitetura, deve-se, portanto, considerar a necessidade que seja independente de fato e capaz de atuar como sujeito processual no controle judicial da inteligência.

Especialmente em razão dessa segunda dimensão, descartou-se a possibilidade de usar o TCU para esse controle, pois não foi concebido para operar como interveniente permanente em processos. A sua

lógica é a da auditoria e do controle externo clássico.

Mesmo deixando de lado a dimensão processual, há um segundo desencaixe: o controle da inteligência exige monitoramento contínuo, com capacidade de acompanhar fluxos, sistemas e conformidade ao longo do tempo – algo distinto do modelo típico de fiscalização por ciclos e achados.

Na escolha das referências institucionais internas, CNJ e CNMP contribuem mais do que o TCU porque entregam o essencial sem hipertrofia: autonomia funcional, administrativa e orçamentária, estabilidade institucional e inserção clara no sistema de freios e contrapesos, sem transformar o órgão em um "superpoder" com iniciativa legislativa própria ampla.

Aqui, o foco é calibrar: blindagem suficiente para garantir independência real e desempenho técnico, mas sem elevar desnecessariamente o custo político e os riscos de concentração institucional.

No resultado, a arquitetura combina três dimensões: força técnica (capacidade de produzir controle qualificado e contínuo), capacidade processual (participar do controle judicial e acionar o Judiciário quando necessário) e integração democrática (ser órgão auxiliar do Parlamento, com prestação de contas e legitimidade).

Membros da Ancai

Art. 75-B. São membros do conselho diretor da Autoridade Nacional de Controle das Atividades de Inteligência, com mandatos de 6 (seis) anos, vedada a recondução:

I – 2 (dois) indicados pela liderança de minoria da Câmara de Deputados;

II – 2 (dois) indicados pela liderança de maioria da Câmara de Deputados;

III – 2 (dois) indicados pela liderança de minoria do Senado Federal;

IV – 2 (dois) indicados pela liderança de maioria do Senado Federal;

V – 3 (três) indicados pela entidade responsável pela proteção de dados pessoais;

VI – 2 (dois) indicados pela Ordem dos Advogados do Brasil.

§ 1º Os indicados deverão ser brasileiros com experiência consolidada em matéria de inteligência ou seu controle, proteção de dados ou defesa de direitos fundamentais, sendo vedada a participação de parlamentares.

§ 2º As indicações deverão ser aprovadas pelo Senado Federal, após arguição pública pela comissão parlamentar de controle das atividades de inteligência.

§ 3º Os diretores da Autoridade Nacional de Controle das Atividades de Inteligência somente poderão ser removidos antes do fim do mandato por renúncia, sentença judicial transitada em julgado ou condenação por crime de responsabilidade.

Seção específica no parecer prévio

Art. 75-C. O parecer prévio sobre as contas anuais do chefe do Poder Executivo conterá seção específica relativa às atividades de inteligência e será apresentado em duas versões, uma pública e uma sigilosa."

Competência do STF

V – fica inserida uma nova alínea, no inciso I, do art. 102, com a seguinte redação:

"**Art. 102.** .....

.....

I – .....

.....

s) os pedidos de autorização para realização de atividade de inteligência, quando o alvo for autoridade arrolada na alínea b.

……"

Competência do STJ

VI – fica inserida uma nova alínea, no inciso I, do art. 105, com a seguinte redação:

"**Art. 105.** ……

……

I – ……

……

k) os pedidos de autorização para realização de atividade de inteligência, quando o alvo for autoridade arrolada na alínea a.

……"

Competência dos TRFs

VII – no art. 108, fica inserida uma nova alínea, no inciso I, do caput, e um parágrafo único, com a seguinte redação:

"**Art. 108.** .....

.....

I – .....

.....

f) os pedidos de autorização para realização de atividade de inteligência de risco elevado feitos por órgãos e entidades federais, salvo nas hipóteses descritas nos arts. 102, I, s e 105, I, k.

.....

Parágrafo único. Na hipótese da alínea f do inciso I, quando o alvo for autoridade cujos crimes comuns sejam julgados originariamente pelo Tribunal de Justiça, exigir-se-á, além da autorização prevista no caput, a autorização do Tribunal de Justiça competente."

Competência da Justiça Estadual

VIII – ficam inseridos os §§ 8º e 9º no art. 125, com a seguinte redação:

"**Art. 125.** .....

.....

§ 8º Compete aos Tribunais de Justiça processar e decidir, originariamente, os pedidos de autorização para realização de atividade de inteligência de risco elevado conduzida por órgãos ou entidades estaduais ou municipais.

§ 9º Na hipótese do § 8º, quando o alvo for autoridade cujos crimes comuns sejam julgados originariamente por tribunais federais, exigir-se-á, além da autorização prevista no caput, a autorização do respectivo tribunal."

Competência do Ministério Público

IX – fica inserido um novo parágrafo no art. 129, com a seguinte redação:

"**Art. 129.** .....

.....

§ 6º A competência de que trata o inciso VII do caput não inclui as atividades de inteligência realizadas por órgãos policiais."

O STJ já decidiu que não cabe ao MP realizar o controle externo das atividades de inteligência (RE 1271855/RJ), referindo que a competência alcança tão somente as atividades relacionadas à investigação criminal. A decisão dá concretude à necessária separação entre a atividade investigativa e de inteligência.

Faz sentido constitucionalizar esta diferença, especialmente considerando que, na última década, consolidou-se a legitimidade do Ministério Público para a condução de investigações criminais (RE 593.727/MG) – o que abriu espaço para órgãos ministeriais instituírem seus próprios núcleos de inteligência de segurança pública.

Viola qualquer sistema de incentivo fiscalizatório atribuir o controle externo a uma instituição que também realiza a atividade controlada.

Essa lógica, por óbvio, também implica a necessidade de se reavaliar a manutenção do controle externo das atividades de investigação criminal com o MP, como fez o parlamentar Alberto Fraga, no âmbito da PEC 18/2025. Essa seção da arquitetura institucional, no entanto, não será explorada, pois extrapola o escopo do presente trabalho.

Marco da inteligência

X – fica inserido, no "TÍTULO V – DA DEFESA DO ESTADO E DAS INSTITUIÇÕES DEMOCRÁTICAS", um novo capítulo, nomeado "CAPÍTULO IV – DAS ATIVIDADES DE INTELIGÊNCIA", contendo os arts. 144-A a 144-H, com a redação que segue:

"CAPÍTULO IV
DAS ATIVIDADES DE INTELIGÊNCIA

Princípios

Art. 144-A. As atividades de inteligência terão como princípios estruturantes:

I – legalidade estrita;

II – finalidade;

III – intervenção mínima;

IV – não discriminação;

V – proteção da dissidência e do sigilo da fonte;

VI – separação entre atividade de inteligência e investigação criminal ou persecução penal; e

VII – auditabilidade plena e prestação de contas.

Sisbin

Art. 144-B. O Sistema Brasileiro de Inteligência integrará as ações de planejamento e execução das atividades de inteligência dos Poderes e órgãos autônomos.

Em linha similar, propôs a parlamentar Laura Carneiro, em forma de emenda, no âmbito da PEC 18/2025.

Em relação à proposta original, acrescentou-se a menção a órgãos e entidades que não são vinculados ao Poder Executivo, trazendo para o texto constitucional algo que já faz parte da realidade, especialmente no que tange ao MP.

Parágrafo único. As ações do Sistema Brasileiro de Inteligência serão guiadas pela política de inteligência, um instrumento de Estado, aprovado em lei, atualizado a cada 4 (quatro) anos, e construído em conjunto com a sociedade civil, que fixa objetivos, diretrizes, prioridades e metas para a atividade de inteligência do respectivo ente, orientando o seu planejamento, coordenação, execução e controle, nos seguintes horizontes temporais:

I – próximos 4 (quatro) anos;

II – próximos 10 (dez) anos; e

III – próximos 20 (vinte) anos.

Abin

Art. 144-C. A Agência Brasileira de Inteligência, vinculada à Presidência da República e dirigida por oficial de inteligência, é o órgão central do Sistema Brasileiro de Inteligência.

Parágrafo único. Compete à Agência Brasileira de Inteligência exercer a atividade de inteligência de Estado, destinada ao assessoramento de autoridades governamentais para a consecução dos objetivos estratégicos do Estado e a defesa da soberania nacional, das instituições democráticas e da ordem constitucional.

Em linha similar, propôs a parlamentar Laura Carneiro, em forma de emenda, no âmbito da PEC 18/2025.

Destaca-se, aqui, a necessidade de: (1) dar a um órgão civil, vinculado a uma autoridade eleita, o papel central da condução da política de inteligência, para fins de fortalecer os mecanismos de prestação de contas e aumentar a legitimidade do sistema; e (2) manter a direção do órgão com um profissional de carreira, de modo a estimular a profissionalização e a consolidação institucional.

Sistema de controle

Art. 144-D. As atividades de inteligência realizadas pelos Poderes e órgãos autônomos, ou em seu nome, estão sujeitas ao controle social, parlamentar, judicial e especializado, sendo este último de responsabilidade da Autoridade Nacional de Controle das Atividades

de Inteligência, do Tribunal de Contas e da entidade responsável pela proteção de dados pessoais.

Parágrafo único. O acesso a informações pelas autoridades de controle, regulado em lei, assegurará o acesso irrestrito, ressalvada apenas a identificação de fontes humanas:

I – à Autoridade Nacional de Controle das Atividades de Inteligência; e

II – ao parlamentar membro de comissão parlamentar de controle das atividades de inteligência, que terá a prerrogativa individual de acesso às informações do respectivo ente, sendo desnecessária a anuência de colegiado ou de qualquer outra autoridade.

As atividades de inteligência devem operar em rede sistêmica porque o problema que elas enfrentam é transversal e dinâmico. Um arranjo integrado consegue combinar capacidades complementares, reduzir cegueira e redundância, elevar a qualidade da análise e, ao mesmo tempo, submeter a atividade a padrões comuns de governança e controle.

Estrutura em rede exige controle em rede: quando a atividade de inteligência é organizada de forma sistêmica, a fiscalização só é efetiva se também for sistêmica, apta a auditar fluxos, pontos de articulação, responsabilidades compartilhadas e a conformidade transversal com

os parâmetros comuns do sistema; do contrário, instala-se um descompasso estrutural entre uma atuação integrada e um controle fragmentado, incapaz de alcançar o ciclo completo da atividade.

Autorização judicial

Art. 144-E. A atividade de inteligência de risco elevado será precedida de autorização judicial.

§ 1º Considera-se como de risco elevado a atividade de inteligência que representa maior risco para os direitos fundamentais ou para a preservação do Estado Democrático de Direito, em razão das pessoas que têm como alvo ou das técnicas que emprega, na forma da lei.

§ 2º O pedido de que trata o caput, bem como as ações dele diretamente derivadas, nos termos da lei, serão apreciados por órgão colegiado especializado, composto por membros com mandato de 6 (seis) anos, sendo vedada a recondução.

§ 3º São partes da ação de que trata o caput exclusivamente o representante do ator de inteligência, nos termos da lei, e a Autoridade Nacional de Controle das Atividades de Inteligência.

A necessidade de um órgão especializado pode também advir de lei de iniciativa do Poder Judiciário.

A determinação de mandato fixo, por sua vez, precisa estar expressa,

pois pode ser considerada uma violação da inamovibilidade, prevista no art. 95, II, da **Constituição Federal**. No caso da justiça eleitoral, por exemplo, onde há mandato fixo, o prazo está na Constituição (art. 121, § 2º).

Da mesma forma, a restrição das partes processuais precisa estar na Constituição. De outro modo, o Ministério Público poderia intervir no processo, o que é inadequado no âmbito da arquitetura proposta – que vê o MP como ator de inteligência, sendo incompatível que assuma funções de controle.

Notificação de vigiado

Art. 144-F. É assegurada à pessoa que tenha sido alvo de atividade de inteligência de risco elevado a notificação após o encerramento da medida, na forma e prazos da lei, sendo admitida a dispensa de notificação exclusivamente por decisão unânime da Autoridade Nacional de Controle das Atividades de Inteligência.

Aprovação de dirigentes

Art. 144-G. Dependem de aprovação prévia pela comissão parlamentar de controle das atividades de inteligência do respectivo ente, após arguição pública, a investidura no cargo das seguintes autoridades:

I – diretor-geral da Agência Brasileira de Inteligência;

II – chefe de centro de inteligência das forças armadas; e

III – dirigente máximo, em órgão policial, de unidade administrativa especializada em atividades de inteligência.

Atualmente, apenas o Diretor-Geral da Abin passa por sabatina parlamentar. A lógica que justifica essa exigência também se aplica aos demais dirigentes das instituições que concentram os maiores poderes intrusivos de inteligência.

A arguição do Diretor-Geral ocorre no Senado Federal e tramita pela Comissão de Relações Exteriores e Defesa Nacional (CRE).

Considerando que já existe um foro especializado para o controle externo da atividade de inteligência (a CCAI, no âmbito federal), faz pouco sentido manter a sabatina no âmbito de uma comissão temática geral quando há um colegiado próprio, vocacionado e informado para essa função.

Vincular a sabatina à comissão especializada busca fortalecer a prestação de contas, alinhando o rito de nomeação às instâncias responsáveis por acompanhar, de modo contínuo, a direção e o controle das atividades de inteligência.

Demonstrativo específico

Art. 144-H. As despesas relacionadas à execução de atividades de inteligência de Poderes e Órgãos Autônomos serão detalhadas em demonstrativo próprio, sendo uma versão pública e uma sigilosa.

A norma acima também poderia estar na **Lei nº 4320, de 17 de março de 1964**, lei de status complementar que traz normas gerais de direito financeiro.

Art. 3º

Primeiro mandato da Ancai

Na primeira composição da Autoridade Nacional de Controle das Atividades de Inteligência, o primeiro membro indicado por força de cada inciso do **art. 75-B**, da Constituição Federal, exercerá mandato de 3 (três) anos, vedada a recondução

Art. 4º

Primeiro mandato dos colegiados judiciais

Na primeira composição dos órgãos colegiados de que trata o **art. 144-E**, metade dos membros de cada colegiado exercerá mandato de 3 (três) anos, vedada a recondução.

Art. 5º

Vigência

Esta Emenda Constitucional entra em vigor na data de sua promulgação, salvo em relação aos seguintes dispositivos, que entram em vigor no seguinte prazo a contar desta data:

I – em 2 (dois) anos:

a) os incisos V a VIII, do art. 2º, desta Emenda Constitucional;

b) a determinação constante no caput do art. 144-C, da Constituição Federal, relativa à necessidade de direção por oficial de inteligência no último nível da carreira;

c) o art. 144-E, da Constituição Federal.

II – em 1 (um) ano, o art. 75-C, da Constituição Federal.

6.2 Projeto de Lei 1

Marco geral com princípios, definições, detalhamento do controle judicial, regras de tratamentos de dados e sistema de denúncias

PROJETO DE LEI N. /2026

Legiscraft

Regulamenta o controle das atividades de inteligência.

TÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º

Escopo da norma

Esta Lei dispõe sobre o controle das atividades de inteligência realizadas pelo Poder Público brasileiro, definindo procedimentos, limites e mecanismos para prevenir e reprimir abusos de poder, dando materialidade à proteção dos direitos fundamentais e à preservação do Estado Democrático de Direito.

Art. 2º

Definições

Para fins desta Lei, considera-se:

I – atividade de inteligência: a ação desenvolvida por Poder de Estado ou órgão autônomo, ou em seu nome, destinada:

a) à obtenção, à análise e à disseminação de dados, dentro e fora do território nacional, sobre fatos e situações de imediata ou potencial influência sobre o processo decisório, a ação governamental, a salvaguarda e a segurança da sociedade, do Estado e de suas instituições democráticas;

b) à realização de contrainteligência, destinada a prevenir, detectar, obstruir e neutralizar a inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado; ou

c) à salvaguarda de informações sigilosas.

II – atividade de inteligência de risco elevado (IRE): a atividade de inteligência que representa maior risco para os direitos fundamentais ou para a preservação do Estado Democrático de Direito, em razão das pessoas que têm como alvo ou das técnicas que emprega, conforme critério objetivos definidos nesta Lei;

Os critérios para definição do que é IRE estão no **art. 5º**.

III – ator de inteligência: órgão ou entidade que realiza atividade de inteligência;

IV – autoridade de controle: órgão ou entidade que realiza o controle parlamentar, judicial ou especializado das atividades de inteligência;

V – coleta massiva: captura de dados não individualizada que abrange de forma generalizada pessoas, grupos, espaços físicos ou ambientes digitais;

VI – comissão parlamentar de controle: comissão parlamentar de qualquer ente federativo que possui como atribuição única o controle das atividades de inteligência;

VII – dado: dado, metadado, informação ou conhecimento coletado, processado, analisado ou compartilhado por meio de atividade de inteligência;

VIII – dado pessoal: aquele assim definido na forma do art. 5º, inciso I, da **Lei nº 13.709, de 14 de agosto de 2018**;

IX – dado pessoal sensível: aquele assim definido na forma do art. 5º, inciso II, da **Lei nº 13.709, de 14 de agosto de 2018**;

X – dado anonimizado: aquele assim definido na forma do art. 5º, inciso III, da **Lei nº 13.709, de 14 de agosto de 2018**;

XI – denúncia: comunicação de elementos de informação a respeito de irregularidade relacionada às atividades de inteligência;

XII – fonte aberta: dado publicamente disponível, obtível sem violação de controles de acesso, sem técnicas de intrusão ou identidade encoberta, e sem recorrer a privilégios, credenciais ou meios não acessíveis ao público em geral, abrangendo conteúdos disponibilizados por seus titulares ou por terceiros em ambientes acessíveis ao público;

XIII – grupos críticos sujeitos à proteção especial: grupo de indivíduos da sociedade civil que, em razão de sua atuação de fiscalização, contestação ou denúncia em face do Poder Público, estão potencialmente expostos a abusos ou constrangimentos por parte deste, tais como jornalistas, defensores de direitos humanos e denunciantes de crimes cometidos pelo Estado e pesquisadores, sendo a sua existência indispensável para a manutenção do Estado Democrático de Direito;

Essa previsão é específica para a sociedade civil. A proteção de agentes públicos com atuação em áreas sensíveis se dá por meio de ferramentas próprias, tais como: (1) a necessidade de autorização judicial para que sejam alvo de atividade de inteligência, prevista no no **art. 5º**, inciso I; e (2) as garantias específicas para *whistleblowers*, previstas nos **arts. 33** e **35**.

XIV – inauditável: o ato, processo, sistema ou recurso tecnológico cuja estrutura ou funcionamento impossibilite ou inviabilize, de modo total ou substancial, a realização de auditoria técnica ou institucional por autoridades de controle interno ou externo, por ausência de transparência, acesso, documentação ou verificabilidade independente, sendo exemplos:

a) o software que não pode ser monitorado de forma contínua, que não disponibiliza seu código-fonte para revisão independente pelo controle externo ou que utiliza técnicas de ofuscação que dificultam substancialmente a análise de sua lógica e operação, comprometendo a verificação completa e precisa de suas operações, algoritmos, acesso a dados e conformidade com regulamentos pertinentes;

b) o equipamento que opera de maneira opaca, sem fornecer meios adequados para revisão independente pelo controle externo, dificultando substancialmente ou impossibilitando a verificação completa e precisa de suas operações, configurações e segurança;

c) a base de dados que não permite a avaliação completa e confiável de suas estruturas, conteúdos ou acessos, seja por restrições de acesso, falta de documentação adequada ou técnicas de criptografia que impeçam a auditoria eficaz de suas informações.

A auditabilidade é o cerne de um controle efetivo. Se um sistema é opaco, o controle será sempre *pro forma*, o que é inadmissível em uma democracia, especialmente em uma área onde há autorização para flexibilização de direitos fundamentais. Definir o que é inauditável, nesse sentido, auxilia o

Estado tanto no planejamento de suas atividades quanto no seu controle.

A ausência de auditabilidade esteve no centro do uso irregular do *software First Mile* pela Abin. No relatório da Polícia Federal sobre o caso, ela refere que uma das maiores dificuldades na investigação foi "o uso de softwares proprietários de código fechado" e a existência de "vestígios criptografados" (Brasil 2025).

XV – log: registro eletrônico automático e inalterável que documenta, de forma cronológica, com marca temporal precisa, as ações realizadas por um usuário credenciado e identificado em um sistema digital;

XVI – mandado de inteligência de risco elevado: doravante mandado, consistente na autorização específica, concedida nos termos desta Lei, para que um ator de inteligência realize de atividade de inteligência de risco elevado;

O mandado é necessário nas hipóteses descritas no **art. 5º**. O anteprojeto traz dispositivos próprios para tratar dos requisitos, do conteúdo e do procedimento (**Título III**).

XVII – medida de minimização: procedimento adotado para assegurar que somente dados estritamente necessários para o objetivo da atividade de inteligência sejam coletados, processados, armazenados, analisados e/ou disseminados;

XVIII – metadado: dado gerado a partir de uma comunicação e que não constitua o seu conteúdo em si, mas seja capaz de garantir autenticidade e contexto a documento eletrônico;

XIX – proteção especial: conjunto de medidas adicionais, concretas e verificáveis de mitigação de risco, voltadas a reduzir a vulnerabilidade dos grupos críticos sujeitos à proteção especial frente ao tratamento geral;

XX – relatório especial: documento produzido a partir de dados obtidos em atividade de inteligência, destinado a subsidiar providências especificadas nesta Lei, que traduz o conteúdo dos dados em informação sintética e contextualizada, contendo apenas os elementos estritamente necessários à finalidade específica, preservando os dados em seu formato original e o sigilo dos métodos utilizados;

XXI – tratamento de dados: aquele feito nos termos do art. 5º, X, da **Lei nº 13.709, de 14 de agosto de 2018**;

XXII – Relatório de Impacto de Vigilância (RIV): documento destinado a avaliar os riscos sociais associados ao uso de determinada tecnologia, devendo identificar, no mínimo:

a) descrição técnica da tecnologia;

b) descrição dos fluxos de dados envolvidos em cada fase do ciclo de inteligência;

c) base legal aplicável e finalidade específica do uso;

d) demonstração da impossibilidade de uso de meios menos intrusivos;

e) análise de riscos:

1. de desvio de finalidade;

2. a direitos fundamentais, especialmente privacidade, liberdade de pensamento e liberdade de expressão;

3. à integridade de redes de telecomunicações, às infraestrutura críticas e à soberania nacional;

4. à segurança da informação.

f) descrição das medidas de controle interno necessárias para mitigar os riscos;

g) condições para implementação, incluindo indicadores de risco adotados e cronograma para reavaliação do uso.

XXIII – (RIPD): documento destinado a descrever os processos de tratamento de dados pessoais no uso de um bem ou serviço específico que podem gerar risco às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos, nos termos da **Lei nº 13.709, de 14 de agosto de 2018**.

TÍTULO II
DAS ATIVIDADES DE INTELIGÊNCIA

Art. 3º

Princípios

As atividades de inteligência terão como princípios estruturantes:

I – legalidade estrita;

II – finalidade;

III – intervenção mínima;

IV – não discriminação;

V – proteção da dissidência e do sigilo da fonte;

VI – separação entre atividade de inteligência e investigação criminal ou persecução penal; e

VII – auditabilidade plena e prestação de contas.

§ 1º O princípio da legalidade estrita impõe interpretação restritiva das competências e poderes dos atores de inteligência, vedada ampliação por analogia ou interpretação extensiva.

§ 2º O princípio da finalidade impõe que a atividade de inteligência seja orientada exclusivamente pela política de inteligência e por seus desdobramentos normativos e decisórios, vedada a sua utilização para fins pessoais, partidários ou estranhos aos objetivos definidos.

§ 3º O princípio da intervenção mínima impõe que a atividade de inteligência siga, dentre outras, as seguintes diretrizes:

I – adequação, necessidade, subsidiariedade e proporcionalidade em sentido estrito;

II – vedação à vigilância indiscriminada;

III – privacidade desde a concepção e por padrão no tratamento de dados pessoais; e

IV – retenção mínima e temporalmente limitada de dados pessoais.

Art. 4º

Atividades sujeitas a controle

Todas as atividades de inteligência estão sujeitas ao controle externo e interno.

Parágrafo único. As atividades de inteligência de risco elevado (IREs) ficam sujeitas a procedimentos de controle mais estritos, na forma desta Lei.

Art. 5º

Atividades de risco elevado

São consideradas IREs as atividades:

I – que tenham como alvo:

a) autoridade com foro de prerrogativa penal;

b) membro da Agência Brasileira de Inteligência;

c) oficial das forças armadas ou das polícias militares;

d) delegado de policial federal ou estadual;

e) membro da carreira diplomática;

f) membro da Autoridade Nacional de Controle das Atividades de Inteligência;

g) dirigente da entidade responsável pela proteção de dados pessoais; ou

II – que empreguem, isolada ou cumulativamente, qualquer das seguintes técnicas:

a) infiltração operacional com identidade encoberta, presencial ou digital, caracterizada pela inserção e manutenção de persona não verdadeira em ambiente-alvo não acessível ao público;

b) vigilância dirigida, consistente no acompanhamento velado, continuado e individualizado de pessoa ou do que a acompanha, por meios presenciais ou virtuais, sem interação;

c) vigilância ambiental em espaço privado, mediante instalação de dispositivo, por técnica presencial ou de sensoriamento remoto, sem necessidade de contato físico com pessoas ou coisas, destinada à captação de sinais do ambiente, tais como os acústicos, ópticos, mecânicos, eletromagnéticos ou digitais de redes locais;

d) interceptação de dado de comunicação em trânsito, por qualquer rede de telecomunicação ou sistema informático, inclusive mediante captura de pacotes ou fluxos;

e) acesso a dispositivo eletrônico, remoto ou local, por meio de software malicioso ou de outras ferramentas de intrusão e exploração, tais como spywares, trojans e keyloggers, que visem controlar o sistema, capturar entradas e saídas, ativar sensores integrados, espelhar sessões e coletar, ler ou alterar dado armazenados;

f) afastamento de sigilos financeiro, bancário e fiscal;

g) rastreamento de localização, em tempo real ou histórico, de pessoa, veículo ou dispositivo, por quaisquer meios;

h) obtenção de dados de tráfego e de atividade on-line mantidos por provedores, incluindo metadados de comunicações, registros de conexão e de aplicações, após a transmissão; ou

i) acesso a conteúdo ou dados armazenados em serviços de terceiros, quaisquer que sejam suas naturezas ou formatos.

§ 1º As hipóteses previstas nos incisos I e II são autônomas e não cumulativas, bastando a ocorrência de qualquer delas para a caracterização como IRE.

§ 2º A proteção conferida pelo inciso I se aplica enquanto o agente público estiver no exercício do cargo, função ou emprego e, após a cessação do vínculo, persiste em relação a atos e dados relativos ao período em que exerceu o mandato ou a função.

§ 3º A Ancai, por ato normativo próprio, poderá elencar outras técnicas como IRE, além das arroladas no inciso II, em razão de sua natureza invasiva ou clandestina, sem prejuízo das operações em andamento, salvo hipótese de pedido de prorrogação.

§ 4º As hipóteses do inciso II, do caput, não se aplicam à coleta de dados acessíveis por meio de fontes abertas.

§ 5º A caracterização de atividade como IRE não autoriza, por si só, seu emprego, cabendo à lei específica definir, para cada ator de inteligência, os alvos e as técnicas previstas neste artigo que integram o seu âmbito de atuação.

Art. 6º

Dever de reportar ilegalidades

Constatados indícios de ilegalidade no exercício de suas competências, é dever:

I – da autoridade de controle:

a) quando se tratar de conduta individual atribuível a agente público, encaminhar notícia de fato ao órgão de controle interno competente, para apuração de responsabilidade, salvo na hipótese do § 1º, inciso I;

b) quando se tratar de irregularidade de caráter estrutural ou procedimental, encaminhar pedido ao Tribunal de Contas competente para adoção das medidas necessárias ao exato cumprimento da lei, inclusive sustação cautelar ou definitiva do ato potencialmente irregular, sempre que houver risco concreto de violação de direitos fundamentais.

II – do órgão de controle interno do ator de inteligência: instaurar processo de apuração de responsabilidade administrativa e, se identificado indício de ilícito civil ou penal, encaminhar notícia de fato ao Ministério Público competente para apuração;

III – do agente público vinculado a ator de inteligência: comunicar o órgão de controle interno ou a Ancai.

§ 1º A autoridade de controle deverá encaminhar notícia de fato ao Ministério Público:

I – quando houver elementos que indiquem que a comunicação ao órgão de controle interno pode comprometer a apuração:

a) agente potencialmente envolvido detém posição hierárquica, influência institucional ou outra forma de poder capaz de afetar a independência da apuração; ou

b) a matéria tem relevância sistêmica, risco de retaliação, impacto coletivo ou conexão com estruturas organizacionais que tornem necessária a atuação de instância externa independente.

II – se o encaminhamento para a apuração administrativa implicar risco de prescrição de ilícito civil ou penal;

III – na hipótese de mora injustificada na apuração pelo órgão de controle interno; ou

IV – quando presentes indícios suficientes de materialidade e elementos que indiquem a plausibilidade de autoria de ilícito civil ou penal.

§ 2º É considerado ilegal o ato, processo, sistema ou recurso tecnológico inauditável.

Art. 7º

Credenciamento

O acesso a dados, instalações, sistemas ou procedimentos sigilosos relacionados às atividades de inteligência, no âmbito dos atores de inteligência e das autoridades de controle, dependerá de credenciamento de segurança, escalonado em níveis, sendo vedado concedê-lo:

I – para atuação em autoridade de controle, a quem, nos 2 (dois) anos anteriores, tenha exercido cargo ou função em ator de inteligência;

II – para atuação em ator de inteligência, a quem, nos 4 (quatro) anos anteriores, tenha exercido cargo ou função em autoridade de controle que envolvesse acesso a dados sigilosos relacionados às atividades de inteligência.

Parágrafo único. A decisão sobre o credenciamento de pessoal da autoridade de controle, observado o disposto no inciso I, do caput, cabe exclusivamente a ela, na forma de ato normativo próprio.

TÍTULO III
DA AUTORIZAÇÃO JUDICIAL

CAPÍTULO I
DO PROCEDIMENTO COMUM

Art. 8º

Ações e partes

O controle judicial das IREs será feito por meio da apreciação dos seguintes pedidos:

I – de autoria do ator de inteligência, observada o art. 9º:

a) mandado para realização de IRE;

b) prorrogação do mandado;

c) de autorização para compartilhamento de dado obtido por meio do mandado;

d) de adiamento da notificação de vigiado;

e) de retenção de dado por período maior que 1 (um) e menor 5 (cinco) anos;

II – de autoria da Ancai:

a) de controle intercorrente do mandado; e

b) destruição de dado obtido ou retido ilegalmente.

§ 1º Quando não forem a parte autora, a Ancai e a autoridade que representa o ator de inteligência serão intervenientes institucionais, participando, com pleno acesso, de todas as fases do processo.

§ 2º Nos procedimentos previstos neste artigo, somente poderão atuar como parte autora ou interveniente institucional a Ancai e a autoridade que representa o ator de inteligência, vedada qualquer outra forma de participação processual, inclusive do Ministério Público.

§ 3º O procedimento judicial tramitará em segredo de justiça.

Art. 9º

Legitimidade

Possuem legitimidade para representar judicialmente os atores de inteligência, nas ações referidas no **art. 8º**:

I – no âmbito federal:

a) o ministério responsável por matérias de defesa nacional, se os atores de inteligência forem vinculados às forças armadas;

b) o ministério responsável por matérias de segurança pública, se os atores de inteligência forem vinculados a órgãos policiais;

c) a Casa Civil, nos demais casos, ou outro ministério por ela indicado.

II – no âmbito estadual, a secretaria responsável por matérias de segurança pública;

III – no âmbito municipal, o gabinete do prefeito.

Art. 10

Sistema de dupla aprovação

O processamento dos pedidos referidos no caput, do art. 8º, I, dar-se-á por meio de um sistema de dupla aprovação, nesta ordem:

I – autorização executiva: pedido é feito pelo ator de inteligência à autoridade com legitimidade judicial, na forma do art. 9º, à qual cabe o exercício do controle interno prévio;

II – autorização judicial: pedido, após aprovado na forma do inciso I, é encaminhado pela autoridade com legitimidade ao Poder Judiciário, ao qual cabe o exercício do controle externo prévio.

§ 1º Ambos os de que tratam os incisos do caput serão subscritos pela autoridade máxima dos referidos órgãos ou entidades, vedada a delegação.

§ 2º A ausência de qualquer das aprovações previstas no caput torna nula a ação, vedada sua execução e o aproveitamento de eventuais dados obtidos.

Art. 11

Pedido de informações complementares

A autoridade judicial pode requisitar informações adicionais à parte autora, a qualquer tempo, o que não implicará a suspensão, interrupção ou prorrogação dos prazos previstos nesta Lei.

Art. 12

Manifestação do interveniente institucional

O interveniente institucional será citado para se manifestar em até 5 (cinco) dias.

Art. 13

Tutela de urgência

A tutela de urgência, se requerida, será concedida, de forma extraordinária e monocrática, quando houver elementos que evidenciem a probabilidade do direito e o perigo de dano grave, concreto e iminente:

I – à vida de alguém;

II – à segurança de infraestrutura crítica; ou

III – à continuidade de serviço público essencial.

Art. 14

Recursos admitidos

Nos procedimentos descritos no art. 8º, restringe-se a recorribilidade aos embargos de declaração, ao agravo interno, ao recurso especial e ao recurso extraordinário.

Parágrafo único. É vedada a interposição de quaisquer outros recursos ou meios autônomos de impugnação, ressalvados os remédios constitucionais.

Art. 15

Embargos de declaração

Caberão embargos de declaração, sem efeito suspensivo, no prazo de 2 (dois) dias, exclusivamente para sanar ambiguidade, obscuridade, contradição, omissão ou erro material.

§ 1º Os embargos interrompem o prazo para a interposição dos demais recursos previstos no art. 14.

§ 2º O julgamento ocorrerá no prazo de 5 (cinco) dias, a contar do protocolo.

§ 3º A decisão que apreciar os embargos não será impugnável por recurso autônomo, sem prejuízo da devolução da matéria nos recursos previstos no art. 14.

Art. 16

Agravo interno

Da decisão monocrática do relator que conceder ou indeferir tutela de urgência caberá agravo interno ao órgão colegiado competente.

§ 1º O agravo interno será interposto no prazo de *5* (cinco) dias e terá efeito exclusivamente devolutivo.

§ 2º O interveniente institucional será intimado para se manifestar em até *5* (cinco) dias, a contar do protocolo.

§ 3º O julgamento colegiado ocorrerá no prazo de *5* (cinco) dias, a contar do decurso do prazo referido no § 2º.

CAPÍTULO II
DO MANDADO

Art. 17

Requisitos do pedido

O pedido judicial de mandado para realização de IRE deve conter, obrigatoriamente:

I – a descrição clara e objetiva da medida proposta;

II – a indicação da pessoa alvo da operação;

III – os fatos e indícios que justificam a operação;

IV – a base legal que autoriza a atividade;

V – os dados que se pretende obter;

VI – a demonstração de que a sua realização é necessária, adequada e proporcional ao caso concreto, devendo explicitar, dentre outros elementos, que:

a) não há outra técnica menos invasiva aos direitos fundamentais mediante a qual se possa obter os dados; e

b) as técnicas são adequadas à obtenção dos dados pretendidos.

VII – a duração pretendida para a atividade;

VIII – as medidas de minimização a serem adotadas.

Art. 18

Conteúdo mínimo da decisão

A decisão judicial que autorizar a atividade deverá conter, ao menos:

I – a indicação de que os requisitos do pedido foram atendidos;

II – o prazo de validade; e

III – de forma precisa, o objetivo, o alvo e o alcance da atividade.

§ 1º A atividade autorizada terá prazo máximo de duração de 3 (três) meses.

§ 2º São vedadas decisões judiciais genéricas ou com prazo indeterminado.

CAPÍTULO III
DA PRORROGAÇÃO

Art. 19

Requisitos do pedido

O mandado para realização de IRE poderá ser prorrogado mediante requerimento acompanhado, no mínimo:

I – da indicação dos resultados obtidos;

II – das razões que justificam sua continuidade;

III – da avaliação da adequação das medidas de minimização adotadas, devendo-se propor ajustes caso tenham se mostrado insuficientes.

Art. 20

Prazo máximo de prorrogação

O prazo máximo total, incluídas as renovações, não poderá ultrapassar 12 (doze) meses.

CAPÍTULO IV
DO CONTROLE INTERCORRENTE

Art. 21

Requisitos do pedido

A Ancai poderá, a qualquer tempo, ingressar com pedido de controle intercorrente do mandado, diante do indício de materialização ou risco de ocorrência de qualquer das seguintes hipóteses:

I – desvio de finalidade;

II – inauditabilidade de software, equipamento ou procedimento;

III – extrapolação dos limites do mandato;

IV – perda de objeto ou mudança substancial dos fatos e indícios que justificam a operação;

V – insuficiência das medidas de minimização;

VI – impacto social negativo de grande proporção não debatido quando da aprovação do mandado.

§ 1º Nas hipóteses de que trata o caput, pode ser determinado:

I – o cancelamento ou suspensão do mandado;

II – a destruição de dado obtido ou retido ilegalmente;

III – a anonimização de dado;

IV – a restrição do uso ou do compartilhamento de dado;

V – o estabelecimento de novas salvaguardas;

VI – a limitação do escopo do mandado.

§ 2º A Ancai poderá ingressar com ação judicial autônoma de destruição de dado obtido ou retido ilegalmente na hipótese de não ser possível identificar qual mandado foi excedido.

§ 3º A tomada de providências, nos termos do caput, não elimina o dever de reportar ilegalidades, previsto no **art. 6º**.

CAPÍTULO V
DO RELATÓRIO DE CONCLUSÃO

Art. 22

Prazo e conteúdo

Encerrada a operação, o ator de inteligência responsável deverá juntar, no prazo de 30 (trinta) dias, nos autos do respectivo mandato, relatório detalhado contendo:

I – descrição das ações realizadas;

II – resultados obtidos e a relevância para a política de inteligência vigente;

III – dados coletados e medidas de minimização utilizadas;

IV – na hipótese de a IRE ter envolvido a instalação de tecnologia de captura de dados em dispositivo eletrônico:

a) a descrição técnica da tecnologia, indicando o que ela faz; e

b) a comprovação técnica, verificável pela autoridade de controle, de que a ferramenta foi removida ao término da ação.

V – fundamentos não genéricos que justifiquem, se for o caso:

a) a retenção de dados;

b) o adiamento da notificação de vigiados.

CAPÍTULO VI
DA NOTIFICAÇÃO DO VIGIADO

Art. 23

Conteúdo, prazo e forma

Toda a pessoa física ou jurídica que tenha sido alvo de IRE deverá ser notificada, pelo ator responsável, no prazo máximo de 12 (doze) meses após o encerramento da atividade.

§ 1º A notificação de que trata o caput deverá indicar, no mínimo:

I – número identificador dos autos do mandado que autorizou a IRE;

II – autoridade judicial responsável pela autorização;

III – ator de inteligência responsável;

IV – alínea do inciso II, do **art. 5º**, que identifica a técnica de coleta de dados utilizada;

V – período de duração da coleta;

VI – descrição da natureza e alcance das informações coletadas;

VII – prazo de retenção dessas informações.

§ 2º A notificação de que trata o caput será feita por meio de plataforma digital unificada.

§ 3º Constatada, em juízo, a realização de IRE em desacordo com o previsto nesta Lei, o vigiado deverá ser comunicado a respeito no prazo máximo de 1 (um) mês, a contar da decisão que reconhece a irregularidade, sendo vedado, nesse caso, o adiamento ou dispensa de notificação.

§ 4º Na notificação de que trata o § 3º, devem constar as informações referidas no § 1º, quando disponíveis, e qual a irregularidade identificada.

A proposta é que este cadastro seja mantido pela Ancai, na forma proposta no anteprojeto de Resolução do Congresso Nacional, no Apêndice D.

Art. 24

Adiamento da notificação

O adiamento da notificação do vigiado pode ser pedido pelo ator de inteligência ao juízo que deferiu o mandado se demonstrado que sua efetivação:

I – compromete ações de inteligência em curso;

II – afeta gravemente a segurança nacional; ou

III – expõe terceiros a risco grave.

Parágrafo único. O adiamento:

I – por período superior a 1 (um) e inferior a 5 (cinco) anos depende de autorização anual;

II – por período superior a 5 (cinco) anos depende de autorização quinquenal, sendo requisito complementar a manifestação favorável da unanimidade do conselho diretor da Ancai.

Art. 25

Dispensa de notificação

A dispensa permanente da notificação do vigiado pode ser pedida pelo ator de inteligência ao juízo que deferiu o mandado se presentes os seguintes requisitos:

I – alguma das possibilidades que autorizam o adiamento previsto no **art. 24**:

a) ainda está presente 5 (cinco) anos após a descontinuação da atividade de inteligência; e

b) continuará aplicável por prazo indeterminável;

II – os dados em questão tiverem sido excluídos por todos os atores de inteligência que a eles tiveram acesso; e

III – houver manifestação favorável da unanimidade do conselho diretor da Ancai.

TÍTULO IV
DO TRATAMENTO DE DADOS

CAPÍTULO I
DAS NORMAS GERAIS

Art. 26

Alteração na LGPD

A **Lei nº 13.709, de 14 de agosto de 2018**, passa a vigorar com as seguintes alterações:

I – no art. 4º, fica alterada a redação do § 2º e das alínea a e b, do inciso III, bem como ficam revogadas as alíneas c e d do mesmo inciso, conforme redação que segue:

"**Art. 4º** .....

.....

"III – .....

.....

a) atividades de inteligência dedicadas à segurança pública, defesa nacional ou segurança do Estado, observado o art. 55-J; ou

b) atividades de investigação criminal ou persecução penal; ou"

c)

.....

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que deverão observar a limitação imposta no § 4º deste artigo, e que serão objeto de informe específico à autoridade nacional na hipótese da alínea b.

....."

Art. 27

Regulamentação

O detalhamento dos padrões técnicos de coleta, processamento, análise, armazenamento, acesso e compartilhamento de dados no âmbito das atividades de inteligência e de seu controle será definido em regulamento da Ancai, ouvida a ANPD, seguindo-se os padrões internacionais mais protetivos em termos de

segurança da informação, proteção de dados pessoais e gestão de evidências digitais.

Parágrafo único. O tratamento de dados pessoais de que trata esta Lei observará os princípios gerais de proteção e os direitos do titular previstos na **Lei nº 13.709, de 14 de agosto de 2018**.

Art. 28

Separação da investigação criminal

O tratamento de dados deverá permanecer segregado daquele realizado no âmbito de atividades de investigação criminal e persecução penal, vedada integração automática de bases ou compartilhamento de dados entre as atividades de inteligência e estas, salvo nas hipóteses e condições previstas nesta Lei.

Art. 29

Tratamento por privados

O tratamento de dados por pessoa de direito privado observará o disposto no art. 4º, § 4º,da **Lei nº 13.709, de 14 de agosto de 2018**.

Art. 30

Deveres dos atores

Os atores de inteligência devem:

I – adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou

ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, desde a fase de concepção até o uso softwares, equipamentos e procedimentos;

II – assegurar que os procedimentos, softwares e equipamentos sejam auditáveis desde a concepção, buscando sempre facilitar a atividade das autoridades de controle;

III – garantir a rastreabilidade de cada ação dentro de uma atividade de inteligência, assegurando que todas as etapas do ciclo possam ser verificadas, mediante registro estruturado, em log inviolável, das fontes de dados, das metodologias e tecnologias empregadas, devendo constar, no mínimo:

a) identificação da decisão judicial que autorizou a atividade, no caso de IRE;

b) identificação dos agentes responsáveis por sua execução;

c) finalidade específica e base legal da ação;

d) data, hora e duração da ação;

e) descrição da ação realizada, dos meios técnicos utilizados e dos dados ou sistemas acessados;

f) identificador único de evento, que permita o encadeamento e a verificação cronológica dos registros;

g) assinatura eletrônica que garantam a integridade e autenticidade do registro; e

h) as medidas de minimização de dados e de limitação de coleta, tratamento e retenção adotadas.

IV – garantir a cadeia de custódia na gestão dos dados coletados;

V – destruir de forma imediata e permanente, de ofício ou a pedido, dado obtido ou retido ilegalmente, observado o § 2º.

§ 1º O registro de que trata o inciso III, alínea h, deve ser tecnicamente verificável, possuir métricas objetivas de necessidade e ser acompanhado de justificativa expressa, não genérica.

§ 2º Dados obtidos ou retidos de forma ilegal são considerados prova ilícita em qualquer procedimento, administrativo ou judicial.

CAPÍTULO II
DA CONTRATAÇÃO DE SOLUÇÃO TECNOLÓGICA

Art. 31

Relatórios de controle

No processo de aquisição de bens ou contratação de serviços, nacionais ou estrangeiros, necessários à execução de IRE, deverão integrar a instrução do processo administrativo da contratação os seguintes relatórios:

I – pelo o ator de inteligência contratante: RIV a respeito do objeto do edital:

a) quando da publicação do edital; e

b) um ano após o recebimento dos bens ou início dos serviços; e

II – pelo potencial contratado: RIPD a respeito da solução por ele proposta:

a) na primeira oportunidade de envio de documentos após o edital; e

b) um ano após a entrega dos bens ou início dos serviços.

§ 1º Na hipótese de o bem ou serviço envolver a utilização de automação decisória, deverá constar no RIPD uma avaliação algorítmica, composta, pelo menos:

I – pela documentação dos modelos, com explicabilidade suficiente;

II – pelos mecanismos que garantem o cumprimento do disposto no art. 54.

§ 2º O disposto neste artigo também se aplica nas hipóteses de:

I – dispensa e inexigibilidade de licitação; e

II – uso de novo bem ou serviço desenvolvido pelo próprio Estado, sem necessidade de contratação de terceiro.

§ 3º A Ancai e a ANPD:

I – devem ser cientificadas, no prazo de 5 (cinco) dias, quando da juntada, respectivamente, do RIV e do RIPD;

II – podem exigir, respectivamente, a qualquer tempo, a apresentação de novo RIV ou RIPD.

Art. 32

Cadastro unificado de contratações

Os contratos firmados para fins, planejamento, execução e controle de atividades de inteligência de risco elevado serão registrados em um portal nacional unificado, de acesso restrito.

A proposta é que este cadastro seja mantido pela Ancai, na forma proposta no anteprojeto de Resolução do Congresso Nacional, no Apêndice D.

§ 1º O registro de cada contrato receberá um número único e contará, no mínimo, com as seguintes informações:

I – a sua finalidade;

II – as unidades administrativas usuárias, identificadas no menor nível hierárquico existente;

III – caso tenham sido adquiridos ou contratados:

a) em relação ao instrumento licitatório:

1. o número identificador;

2. a sua íntegra;

3. a justificativa para dispensa ou inexigibilidade de licitação, se for o caso.

b) em relação ao contrato:

1. o número identificador;

2. a sua íntegra, incluídos quaisquer aditivos;

IV – as despesas empenhadas, pagas e liquidadas no âmbito do contrato no exercício atual e nos dois anteriores; e

V – os RIVs e RIPDs a ele relacionados.

§ 2º O número único a que se refere o § 1º deverá constar como marcador em todas as operações contábeis e processos administrativos relacionados ao contrato.

§ 3º O cadastro e a marcação de documentos de que trata este artigo deverão ser feitos de ofício pelos atores de inteligência de todos os entes, desde a publicação do edital, em até 5 (cinco) dias após o surgimento ou atualização da informação, sob pena de configuração de negativa de acesso à informação, punível na forma do **art. 50**.

CAPÍTULO III
DA COLETA

Art. 33

Controle de acesso a tecnologias

O acesso a tecnologias cuja técnica de coleta de dados seja qualificada como IRE será auditável, controlado de forma estrita e limitado a usuários previamente autorizados, sendo observadas, no mínimo, as seguintes exigências:

I – em relação à autenticação dos usuários:

a) adoção de mecanismos de autenticação forte com múltiplos fatores independentes;

b) segregação de perfis, com aplicação do princípio do menor privilégio;

c) implementação de política de gestão de credenciais, vedado o compartilhamento;

d) exigência de certificado digital qualificado no âmbito da ICP-Brasil, nos termos da Lei nº 14.063/2020, de 23 de setembro de 2020.

II – existência de sistema de logs.

Art. 34

Tipos de coleta vedados

Fica vedada a coleta:

I – massiva, por meio das técnicas qualificadas como IRE, salvo aquelas descritas nas alíneas a e b, do inciso II, do caput, do **art. 5º**;

II – de dados de áudio, imagem ou biometria mediante intrusão em sensores de dispositivos eletrônicos pessoais; ou

III – de dados de áudio ou imagem, ou de quaisquer dados que constituam representação equivalente destes, ainda que obtidos por meio diverso, dentro de espaço:

a) domiciliar; ou

b) profissional onde for desenvolvida atividade de:

1. confissão religiosa;

2. advocacia;

3. saúde;

4. serviço social;

5. contabilidade; e

6. jornalismo.

Parágrafo único. Aplica-se a qualquer dado coletado em desconformidade com o caput o dever do **art. 30**, inciso V e § 2º.

Art. 35

Notificação por alvo sensível

A Ancai deverá ser notificada sempre que um dado coletado fizer menção a pessoa que se enquadre em qualquer das hipóteses a seguir:

I – exerça cargo ou função prevista no **art. 5º**, inciso I;

II – seja advogado ou jornalista.

Art. 36

Dados sob custódia do Estado

O ator de inteligência poderá receber dados de:

I – outros atores de inteligência, na forma do Capítulo VII, **Seção I**;

II – de investigação criminal ou processo penal, concluído ou em andamento, mesmo que em sigilo ou segredo de justiça, cabendo ao juízo de origem avaliar o pleito.

Parágrafo único. O pedido de que trata o inciso II, do caput, deverá ter anuência do órgão colegiado especializado caso os dados se enquadrem nas hipóteses do **art. 5º**.

CAPÍTULO IV
DO PROCESSAMENTO E ANÁLISE

Art. 37

Vedação de uso secundário

A análise de dados será realizada exclusivamente para a finalidade específica que justificou a coleta, vedada qualquer uso secundário, salvo se autorizado expressamente por esta Lei.

Art. 38

Revisão humana

O ator de inteligência deverá realizar revisão humana prévia a qualquer ação que:

I – resulte em restrição ou suspensão de direito individual ou coletivo;

II – torne alguém alvo de atividade de inteligência.

CAPÍTULO V
DO ARMAZENAMENTO E EXCLUSÃO

Art. 39

Diretrizes

O armazenamento de dados:

I – assegurará integridade, confidencialidade e disponibilidade;

II – adotará classificação de acesso por níveis de sigilo;

III – limitar-se-á ao período estritamente necessário.

Art. 40

Regra geral dos prazos de retenção

O prazo de armazenamento dos dados pessoais coletados por meio de atividade de inteligência é de 10 (dez) anos, salvo na hipótese de terem sido obtidos por meio de IRE.

Parágrafo único. Os logs dos sistemas de informação utilizados pelos atores de inteligência devem ser mantidos por 30 (trinta) anos.

Art. 41

Prazos de retenção para IRE

Os dados obtidos por meio de IRE serão excluídos imediatamente após o encerramento do prazo do mandado judicial, salvo se o ator de inteligência responsável justificar, de forma expressa e não genérica, a necessidade de sua conservação, indicando o fundamento legal e a finalidade, observados os requisitos temporais do § 1º.

§ 1º A retenção dos dados:

I – por período de até 1 (um) ano depende de comunicação do juízo que deferiu o mandado;

II – por período superior a 1 (um) e inferior a 5 (cinco) anos depende de autorização anual do juízo que deferiu o mandado;

III – por período superior a 5 (cinco) anos depende de autorização quinquenal do juízo que deferiu o mandado, sendo requisito complementar a manifestação favorável da unanimidade do conselho diretor da Ancai.

§ 2º A prorrogação do período de retenção não afasta automaticamente o dever de notificação do vigiado.

CAPÍTULO VI
DAS REGRAS GERAIS DE COMPARTILHAMENTO

Art. 42

Alcance e escopo

O compartilhamento de dados somente poderá ocorrer nas hipóteses expressamente previstas nesta Lei.

Parágrafo único. O disposto no caput aplica-se exclusivamente às informações classificadas em algum grau de sigilo.

Art. 43

Regra do controle na origem

O compartilhamento e a alteração do grau de sigilo de dados compete exclusivamente ao ator de inteligência de origem, sendo vedada a retransmissão sem sua anuência, ressalvadas as hipóteses de acesso por autoridades de controle.

§ 1º O disposto no caput não impede a revisão de decisões de compartilhamento ou de grau de sigilo por órgãos hierarquicamente superiores ao ator de inteligência de origem, por força de lei ou decisão judicial.

§ 2º No ato de transmissão, deve ser informado o grau de sigilo e o prazo de retenção do dado, sendo dever do destinatário excluí-lo após o decurso do prazo.

Art. 44

Impacto sobre prazos

O compartilhamento de dados não implica na suspensão, interrupção ou prorrogação de qualquer dos prazos previstos nesta Lei, obrigando, quando aplicável, também o destinatário.

Art. 45

Salvaguardas técnicas

Os órgãos que realizarem o compartilhamento de dados deverão:

I – realizar, antes do envio, medidas de minimização;

II – assegurar a sua traçabilidade, registrando obrigatoriamente:

a) a data da transmissão;

b) a finalidade da transmissão;

c) a descrição resumida do produto transmitido;

d) a identidade da pessoa responsável pelo envio;

e) a identidade da pessoa responsável pelo recebimento.

Art. 46

Meios de transmissão vedados

É vedado o compartilhamento de dados por meio de serviço de comunicação:

I – sob controle efetivo de pessoa jurídica estrangeira; ou

II – ofertado ao público em geral.

Art. 47

Proteção de fontes

Em qualquer hipótese, o compartilhamento de dados deve ser precedido da anonimização ou pseudonimização de dados que permitam a identificação de fontes humanas, mesmo que o destinatário seja uma autoridade de controle.

Parágrafo único. Os elementos que permitem a identificação de fonte humana devem permanecer sob guarda exclusiva do ator de inteligência de origem.

CAPÍTULO VII
DO COMPARTILHAMENTO PELO ATOR DE INTELIGÊNCIA

Seção I
Do compartilhamento com outro ator de inteligência

Art. 48

Requisitos

O compartilhamento de dados poderá ocorrer, sempre precedido de termo de cooperação:

I – entre atores de inteligência do mesmo ente federativo;

II – entre atores de inteligência de diferentes entes federativos;

III – entre atores de inteligência nacionais e estrangeiros.

§ 1º O compartilhamento previsto no inciso I do caput será previamente informado ao juízo que deferiu o mandado.

§ 2º O compartilhamento previsto no inciso II do caput depende de autorização do juízo que deferiu o mandado.

§ 3º O compartilhamento previsto no inciso III do caput somente será possível se, cumulativamente:

I – a análise de risco de compartilhamento internacional indicar que existem salvaguardas institucionais adequadas no outro país, conforme disciplinado na **Seção I**, do Capítulo IX, do Título IV;

II – houver autorização do juízo que deferiu o mandado; e

III – no caso de recebimento de ator estrangeiro, o dado tenha sido obtido por meios não vedados pelo ordenamento jurídico brasileiro.

Seção II
Do compartilhamento com autoridade de controle

Art. 49

Níveis de acesso

O compartilhamento de dados sob custódia do Poder Público ou de pessoa de direito privado com autoridades de controle se dará via requisição destas, que terão os seguintes níveis de acesso:

I – a Ancai possui acesso irrestrito em nível nacional;

II – os Parlamentos possuem acesso irrestrito no nível do respectivo ente;

III – a ANPD e os Tribunais de Contas possuem acesso limitado ao cumprimento de suas finalidades institucionais;

IV – o Poder Judiciário possui acesso limitado ao objeto da lide, sempre nos autos do procedimento judicial correspondente.

§ 1º O acesso referido no inciso I do caput inclui o acesso direto e em tempo real a softwares e seus logs, bancos de dados, equipamentos e instalações destinadas às atividades de inteligência, sob custódia do Poder Público ou de pessoa de direito privado, independente de requerimento.

§ 2º Os requerimentos de informação das autoridades de controle deverão ser cumpridos no prazo improrrogável de 10 (dez) dias a contar da data de envio.

Art. 50

Consequência diante de negativa indevida

A negativa de acesso a dados incompatível com esta Lei configura:

I – por parte da autoridade requerida:

a) crime de prevaricação, na forma do art. 319, do **Código Penal**;

b) ato de improbidade administrativa, na forma do art. 11, inciso VI, da **Lei nº 8.429, de 2 de junho de 1992**;

c) infração administrativa, na forma do art. 32, da **Lei nº 12.527, de 18 de novembro de 2011**; e

d) crime de responsabilidade, caso aplicável à autoridade requerida;

II – por parte da pessoa de direito privado requerida, na pessoa do responsável pelo contrato:

a) crime de falsidade documental, na forma de um ou mais tipos descritos nos arts. 297 a 299, do **Código Penal**;

b) infração administrativa de dificultar atividade de fiscalização ou intervir em sua atuação, na forma do inciso art. 155, inciso XII, da **Lei nº 14.133, de 1º de abril de 2021**, combinado com o art. 5º, inciso V, da **Lei nº 12.846, de 1º de agosto de 2013**.

§ 1º Na hipótese de indício de negativa indevida de acesso, a autoridade de controle deverá encaminhar os pedidos de apuração de responsabilidade de que trata o caput prazo de 30 (trinta) dias a contar da data em que constatou o indício.

§ 2º Não será considerada justificativa para a não prestação da informação a alegação de classificação sigilosa da informação, de risco para a segurança da sociedade e do Estado ou de segredo de justiça.

Seção III
Do compartilhamento com outras autoridades

Art. 51

Investigações e urgências

Os dados devem ser compartilhados pelo ator de inteligência que os detiver, por meio de relatório especial, nas seguintes hipóteses, mediante autorização judicial:

I – com a autoridade investigativa competente, se for encontrado indício:

a) por mera serendipidade, de crime consumado, em execução ou em fase de preparação, cuja pena máxima seja de 10 (dez) anos ou mais; e

b) de crime consumado, em execução ou em fase de preparação relacionado ao planejamento ou execução das atividades de inteligência; e

II – com autoridades públicas competentes, se for encontrado indício de perigo grave, concreto e iminente:

a) à vida de alguém;

b) à segurança de infraestrutura crítica;

c) à continuidade de serviço público essencial;

d) à segurança de sistema de informação mantido pela referida autoridade.

Art. 52

Utilização como prova

À exceção da hipótese de apuração de responsabilidade criminal, civil, ou administrativa referente a ilícito cometido no âmbito das atividades de inteligência:

I – os dados não serão utilizados como meio de prova ou juntados em processos de qualquer natureza, devendo o seu conteúdo ser traduzido na forma de relatório especial;

II – o agente público vinculado a ator de inteligência não poderá ser convocado a depor.

Seção IV
Do compartilhamento com privado

Art. 53

Perigo a sistemas de informação

Os dados podem ser compartilhados com pessoa de direito privado nacional, por meio de relatório especial, mediante autorização judicial, se for encontrado

indício de perigo grave, concreto e iminente à segurança de sistema de informação desenvolvido ou mantido por ela, podendo afetar:

I – infraestrutura crítica;

II – a continuidade de serviço público essencial;

III – a segurança de dados pessoais de consumidores e usuários.

CAPÍTULO VIII
DO COMPARTILHAMENTO PELA AUTORIDADE DE CONTROLE

Seção I
Do compartilhamento com outra autoridade de controle

Art. 54

Requisitos

O compartilhamento de dados entre autoridades de controle, sendo:

I – ambas nacionais: será precedido de termo de cooperação e levará em consideração os níveis de acesso previstos no **art. 49**;

II – uma delas estrangeira: somente será possível se, cumulativamente:

a) a análise de risco de compartilhamento internacional indicar que existem salvaguardas institucionais adequadas no outro país;

b) houver termo de cooperação internacional entre as autoridades de controle.

Seção II
Do compartilhamento com outras autoridades

Art. *55*

Investigações e urgências

Os dados devem ser compartilhados pela autoridade de controle que os detiver, por meio de relatório especial, nas seguintes hipóteses:

I – com a autoridade investigativa competente, se for encontrado indício de crime consumado, em execução ou em fase de preparação relacionado ao planejamento e execução das atividades de inteligência;

II – com autoridades públicas competentes, se for encontrado indício de perigo grave, concreto e iminente:

a) à vida de alguém;

b) à segurança de infraestrutura crítica;

c) à continuidade de serviço público essencial;

d) à segurança de sistema de informação mantido pela referida autoridade.

CAPÍTULO IX
DO COMPARTILHAMENTO INTERNACIONAL

Seção I
Da análise de risco

Art. 56

Exigência de salvaguardas institucionais

O compartilhamento internacional de dados somente será possível se o destinatário ou remetente internacional possuir salvaguardas institucionais adequadas para garantir que os dados compartilhados sejam utilizados ou tenham sido produzidos de forma compatível com os princípios do direito brasileiro.

Parágrafo único. A aferição da qualidade das salvaguardas institucionais será feita por meio de análise de risco de compartilhamento internacional.

Art. 57

Critérios de análise

A análise de risco de compartilhamento internacional, de responsabilidade da Ancai, consultada a ANPD, avaliará se o ordenamento jurídico e as práticas administrativas do outro país, devendo observar, no mínimo, a qualidade dos sistemas de:

I – controle externo das atividades de inteligência;

II – prevenção e combate à tortura;

III – proteção da atividade jornalística;

IV – proteção de testemunhas ameaçadas;

V – proteção de denunciantes de crimes cometidos pela administração pública.

§ 1º Não serão consideradas adequadas as salvaguardas institucionais do país se qualquer dos sistemas arrolados no caput for considerado insuficiente.

§ 2º A análise do país será única, não havendo distinção se o objetivo for enviar ou receber dados.

Art. 58

Procedimento e validade

O processo de análise de risco de compartilhamento internacional poderá ser iniciado a pedido de ator de inteligência ou de ofício.

Parágrafo único. A análise possui validade máxima de 4 (quatro) anos.

Seção II
Do termo de cooperação

Art. 59

Requisitos

O termo de cooperação internacional somente será válido se:

I – as partes tiverem competência territorial nacional;

II – houver previsão expressa de acesso total das autoridades de controle externo de ambos os países aos dados compartilhados, independente de autorização da origem;

III – houver compromisso expresso de:

a) não retransmissão, sem autorização da origem, dos dados compartilhados, exceto para fins do inciso II; e

b) no caso de o destinatário ser estrangeiro, destruição permanente dos dados nos mesmos prazos definidos pela legislação brasileira.

IV – for dada ciência de seu conteúdo e de eventual alteração à Ancai e ao parlamento do respectivo ente.

TÍTULO V
DO SISTEMA DE DENÚNCIAS

Art. 60

Dever de proteção do denunciante

É assegurada a proteção a denunciantes de possíveis ilegalidades cometidas no âmbito das atividades de inteligência, com vistas a prevenir retaliações, intimidações ou constrangimentos decorrentes de sua ação.

Art. 61

Formas de denúncia

A denúncia poderá ser:

I – formal, quando apresentada à Ancai; ou

II – pública, quando apresentada por outros meios, na forma do art. 64.

Parágrafo único. Aplica-se a esta Lei o disposto nos arts. 10 e 11, da Lei nº 13.460, de 26 de junho de 2017.

Art. 62

Requisitos da denúncia formal

A denúncia formal poderá ser feita por escrito ou oralmente, de forma presencial ou eletrônica, por pessoa física ou jurídica.

Parágrafo único. São admitidas denúncias anônimas, desde que utilizadas apenas para subsidiar a adoção de diligências preliminares de verificação.

Art. 63

Canal de denúncias

A Ancai instituirá canal próprio, seguro, criptografado e acessível, destinado ao recebimento de denúncias formais.

§ 1º O denunciante terá direito às seguintes informações simplificadas e datadas sobre o trâmite de sua denúncia:

I – confirmação do protocolo, com indicação do número de registro;

II – se resultou na instauração de procedimento de apuração ou de auditoria;

III – se resultou na expedição de recomendação;

IV – se foi arquivada; e

V – caso tenha sido remetida a outra autoridade:

a) a identificação do destino;

b) se foi arquivada;

c) se resultou em responsabilização civil, administrativa ou criminal.

§ 2º No cumprimento do disposto no § 1º, é vedada a divulgação de informação sob sigilo.

§ 3º Caso a denúncia tenha sido apensada a outro caso, o denunciante terá direito às informações relacionadas a este.

§ 4º A denúncia formal somente será encerrada após o arquivamento de todos os procedimentos abertos pelas outras autoridades às quais foi remetida.

Art. 64

Requisitos da denúncia pública

O agente público poderá fazer denúncia pública, pelo meio que julgar adequado, se cumpridos, cumulativamente, os seguintes requisitos:

I – a denúncia envolve informação sigilosa à qual o referido agente possui acesso em razão de seu cargo, função ou emprego;

II – existe denúncia formal feita à Ancai, pelo mesmo agente, com o mesmo conteúdo; e

III – inexiste encaminhamento preliminar, pela Ancai, no período de 1 (um) ano a contar da data de protocolo da denúncia formal.

Parágrafo único. Considera-se encaminhamento preliminar qualquer das seguintes ações:

I – conclusão de procedimento de apuração ou de auditoria;

II – expedição de recomendação;

III – arquivamento;

IV – remessa para apuração por outra autoridade de controle ou de investigação, exceto se for para órgão de controle interno.

Art. 65

Medidas gerais de proteção

A autoridade de controle deverá utilizar os meios necessários para garantir a proteção do denunciante desde a denúncia até o momento em que se fizer cessar o risco à sua integridade.

§ 1º São medidas mínimas de proteção, aplicáveis a todos os denunciantes:

I – preservação de identidade, em qualquer hipótese, salvo se expressamente manifestado de forma contrária pelo denunciante; e

II – imunidade a sanções administrativas, civis ou penais, em razão do envio da denúncia na forma desta Lei;

III – medidas constantes no art. 4º-C, da **Lei nº 13.608, de 10 de janeiro de 2018**.

§ 2º Na hipótese de a denúncia motivar a abertura de qualquer procedimento, administrativo ou judicial, fora do escopo da Ancai, as informações que permitam a identificação do denunciante devem ser precedidas da anonimização ou pseudonimização.

§ 3º Os elementos que permitam a identificação do denunciante devem permanecer sob guarda exclusiva da Ancai, permanecendo sob sigilo pelo prazo de cem anos, conforme o disposto no inciso I, do § 1º, do art. 31, da **Lei nº 12.527, de 2011**.

Art. 66

Ausência de dever de sigilo por terceiros

A divulgação de informações classificadas como sigilosas por pessoa que não detiver o dever de manter o sigilo não ensejará responsabilização cível, administrativa ou criminal, exceto quando comprovado que tenha participado de ato ilícito para obtê-las.

Art. 67

Recompensa

A Ancai poderá estabelecer formas de recompensa pelo oferecimento de informações que sejam úteis para a prevenção, a repressão ou a apuração de crimes ou ilícitos no âmbito das atividades de inteligência.

Parágrafo único. Entre as recompensas a serem estabelecidas, poderá ser instituído o pagamento de valores em espécie.

TÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 68

Regras de transição

Para a aplicação desta Lei, devem ser consideradas as seguintes regras de transição:

> I – o disposto nos incisos, do caput, do **art. 7º**, aplica-se exclusivamente aos credenciamentos concedidos ou renovados a partir da data de publicação desta Lei;

II - o dever de notificação do vigiado, previsto no **Capítulo VI – Da Notificação do Vigiado**, do Título III – Da Autorização Judicial, aplica-se exclusivamente para atividades realizadas a contar da sua entrada em vigor, nos termos do **art. 69**, inciso I.

Art. 69

Vigência

Esta Lei entra em vigor na data de sua publicação, salvo os seguintes dispositivos, que entram em vigor no seguinte prazo a contar desta data:

I – em dois anos, o **Título III – Da Autorização Judicial**;

II – em um ano, os arts. **31**, **32**;

III – em 6 (seis) meses, o § 2º, do **art. 49**;

IV – em 60 (sessenta) dias:

a) as alíneas d, f, g e h, do inciso III, do **art. 30**; e

b) o **art. 46**.

6.3 Projeto de Lei 2

Alteração das competências da Agência Nacional de Proteção de Dados

PROJETO DE LEI N. /2026

Legiscraft

Altera a **Lei nº 13.709, de 14 de agosto de 2018** (LGPD), para adicionar competências relativas ao controle das atividades de inteligência à ANPD.

Art. 1º

Alterações na LGPD

Na **Lei nº 13.709, de 14 de agosto de 2018**, em seu art. 55-J, ficam acrescidos os §§ 7º e 8º, com a seguinte redação:

"**Art. 55-J** .....

.....

§ 7º No âmbito do controle especializado das atividades de inteligência, compete à ANPD:

I – exercer as competências previstas no caput, quando aplicáveis;

II – acompanhar o processo de aquisição de bens e contratação de serviços para essas atividades, nos termos da lei específica;

III – expedir recomendações para a proteção de dados pessoais tratados nessas atividades;

IV – requerer justificativa escrita para o não cumprimento de recomendação sua;

V – produzir relatório anual sobre sua atividade, com duas versões:

a) uma pública, para fins de controle social; e

b) uma sigilosa, para fins de controle parlamentar e da Ancai.

§ 8º A ANPD possui plena independência no exercício de suas competências, sendo inalteráveis e insubstituíveis os seus pareceres, recomendações e demais conclusões técnicas.

Art. 2º

Vigência

Esta Lei entra em vigor na data de sua publicação.

6.4 Projeto de Resolução do Congresso Nacional

Criação de um órgão especializado vinculado ao Legislativo e reformas na comissão mista de controle

PROJETO DE RESOLUÇÃO

DO CONGRESSO NACIONAL N. /2026

Legiscraft

Dispõe sobre o Sistema Nacional de Controle das Atividades de Inteligência, a Autoridade Nacional de Controle das Atividades de Inteligência e altera a **Resolução do Congresso Nacional nº 2, 22 de novembro de 2013**, que dispõe sobre a Comissão Mista de Controle das Atividades de Inteligência.

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º

Introdução à norma

Esta Resolução dispõe sobre o Sistema Nacional de Controle das Atividades de Inteligência (Conint), a Autoridade Nacional de Controle das Atividades de Inteligência (Ancai) e altera o formato, as competências e os procedimentos da Comissão Mista de Controle das Atividades de Inteligência (CCAI).

CAPÍTULO II
DAS SISTEMA NACIONAL DE CONTROLE

Art. 2º

Competência

Fica instituído o Sistema Nacional de Controle Externo das Atividades de Inteligência (Conint), por meio de atuação coordenada das autoridades de controle de todos os entes, em articulação com a sociedade civil, com a finalidade de:

I – zelar pelo cumprimento desta Lei;

II – fornecer subsídios para que as autoridades de controle tenham condições de exercer de forma plena a sua função fiscalizatória;

III – fomentar a criação de órgãos de controle vinculados aos parlamentos dos entes subnacionais;

IV – promover a padronização dos procedimentos de controle e a segurança de dados das autoridades de controle;

V – propiciar a profissionalização das atividades controladas, assegurando a observância de padrões técnicos, éticos e legais, bem como a sua plena auditabilidade;

VI – adotar e propor medidas de proteção efetiva a denunciantes, especialmente àqueles ligados à comunidade de inteligência;

VII – assumir e sugerir medidas que permitam o controle social das atividades de inteligência, sendo, em todo o caso, protegido o sigilo a elas inerente.

Art. 3º

Composição

O Conint é integrado pela Autoridade Nacional de Controle das Atividades de Inteligência (Ancai) e pela CCAI, sendo convidados a participar:

I – as comissões parlamentares de controle das atividades de inteligência de parlamentos subnacionais;

II – os autoridades de controle análogas à Ancai em nível subnacional;

III – a Agência Nacional de Proteção de Dados;

IV – os tribunais de contas.

Parágrafo único. Cabe à Ancai, órgão central do Conint:

I – autorizar o ingresso dos atores arrolados nos incisos I e II, na forma de regulamento próprio, tendo como critérios mínimos:

a) a existência do órgão ou entidade há mais de 2 (dois) anos;

b) a instituição de procedimentos de controle regulares e padronizados;

c) a cumprimento dos requisitos de estrutura mínima definidos no **art. 5º**;

d) a capacidade de gerenciar denúncias de forma eficiente e segura para o denunciante.

II – celebrar convênios com seus membros e com os órgãos responsáveis pelo controle interno das atividades de inteligência, para fins exclusivos de prestação de contas, visando à compatibilização de sistemas de informação e à integração de dados;

III – instituir centros integrados de controle das atividades de inteligência para a cooperação entre os integrantes do sistema, com vistas à atuação nacional, regional, estadual, distrital ou municipal, de forma sistemática ou esporádica.

CAPÍTULO II
DA AUTORIDADE NACIONAL

Art. 4º

Competência

Compete à Ancai:

I – realizar auditorias, de ofício ou mediante provocação de pelo menos um terço dos membros de comissão parlamentar de controle federal, em qualquer órgão ou entidade, ou em privado que atue em seu nome, com vistas a verificar a conformidade das atividades de inteligência;

II – assessorar a CCAI na análise da Prestação de Contas das Atividades de Inteligência (PCAI) e da seção do parecer prévio dedicada às atividades de inteligência;

III – receber e apurar denúncias de abuso de poder e adotar medidas para proteger os denunciantes;

IV – atuar nas ações judiciais de autorização de atividade de inteligência de risco elevado (IRE), nos termos da lei, em defesa da conformidade constitucional e legal das atividades de inteligência;

V – monitorar a atividade de inteligência autorizada na forma do inciso IV.

VI – expedir recomendações para a adoção de práticas que previnam e reprimam desvios de finalidade nas atividades de inteligência;

VII – acompanhar a aquisição, o desenvolvimento e a implementação de tecnologias, de modo a garantir que estejam em conformidade com a lei;

VIII – produzir e manter atualizadas a análises de risco de compartilhamento internacional de dados;

IX – manter um cadastro nacional unificado de contratações feitas pelos atores de inteligência;

X – produzir relatório anual sobre sua atividade, com duas versões:

a) uma pública, para fins de controle social, constando, no mínimo, estatísticas referentes às notificações de vigiados realizadas, adiadas e dispensadas, segregadas por ator de inteligência; e

b) uma sigilosa, para fins de controle parlamentar.

XI – expedir normativas para fins de:

a) incluir outras técnicas no rol de medidas consideradas atividade de inteligência de risco elevado (IRE);

b) determinar salvaguardas adicionais para:

1. procedimentos operacionais;

2. o uso de técnicas específicas;

3. a gestão de dados;

4. a proteção especial direcionadas a cada um dos grupos críticos;

XII – autorizar o ingresso de órgãos parlamentares subnacionais no Conint.

Art. 5º

Estrutura

A Ancai terá espaço físico exclusivo, estrutura de pessoal própria e procedimentos de segurança adequados para garantir a independência e confidencialidade do seu trabalho.

Parágrafo único. As equipes serão especificamente qualificadas para a atividade, submetidas a processo de credenciamento e verificação de segurança, mediante assinatura de termo de confidencialidade, e participarão de formação inicial e continuada, abrangendo, entre outros, os seguintes temas:

I – proteção de dados;

II – segurança da informação; e

III – estado da arte das técnicas de inteligência.

CAPÍTULO III
DA CONSELHO NACIONAL

Art. 6°

Competência

Fica instituído o Conselho Nacional de Controle das Atividades de Inteligência – Concai, órgão consultivo da Ancai, ao qual compete:

I – propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Inteligência e para a atuação da Ancai;

II – elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Inteligência e das ações dos órgãos de controle;

III – sugerir ações a serem realizadas pela Ancai;

IV – elaborar estudos e realizar debates e audiências públicas sobre o controle das atividades de inteligência;

V – disseminar o conhecimento sobre o controle das atividades de inteligência à população.

Art. 7º

Composição

O Concai será composto de 13 (treze) representantes, titulares e suplentes, tendo como origem:

I – 1 (um) do Conselho Nacional de Justiça;

II – 1 (um) do Conselho Nacional do Ministério Público;

III – 1 (um) da Ordem dos Advogados do Brasil;

IV – 1 (um) da Federação Nacional dos Jornalistas;

V – 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de denunciantes ou de vítimas da violência estatal;

VI – 2 (duas) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais;

VII – 2 (duas) de instituições científicas, tecnológicas e de inovação relacionadas à área de inteligência;

VIII – 2 (duas) de entidades representativas do setor empresarial nacional relacionadas à área de inteligência.

§ 1º Os representantes serão designados por ato do Presidente da CCAI.

§ 2º As instituições arroladas nos incisos I a IV do caput serão convidadas a indicar representantes para o Concai.

§ 3º Os representantes de que tratam os incisos V a VIII do caput deste artigo e seus suplentes:

I – serão indicados na forma de regulamento;

III – terão mandato de 3 (três) anos, permitida 1 (uma) recondução.

§ 4º A participação no Concai será considerada prestação de serviço público relevante, não remunerada.

CAPÍTULO IV
DA REFORMA DA COMISSÃO

Art. 8º

Alterações na CCAI

A **Resolução do Congresso Nacional nº 2, 22 de novembro de 2013**, passa a vigorar com as seguintes alterações:

Escopo

I - fica alterado o art. 1º, que passa a ter a seguinte redação:

> "**Art. 1º** Esta Resolução é parte integrante do Regimento Comum do Congresso Nacional e dispõe sobre a Comissão Mista de Controle das Atividades de Inteligência (CCAI), comissão permanente do Congresso Nacional, órgão de controle externo da atividade de inteligência.
>
> **Parágrafo único.** Para fins desta Resolução, considera-se atividade de inteligência: a ação desenvolvida por Poder de Estado ou órgão autônomo, ou em seu nome, destinada:
>
> a) à obtenção, à análise e à disseminação de dados, dentro e fora do território nacional, sobre fatos e situações de imediata ou potencial influência sobre o processo decisório, a ação governamental, a salvaguarda e a segurança da sociedade, do Estado e de suas instituições democráticas;
>
> b) à realização de contrainteligência, destinada a prevenir, detectar, obstruir e neutralizar a inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado; ou
>
> c) à salvaguarda de informações sigilosas."

O texto atual dá a entender que o controle externo das atividades de inteligência foi delegado ao parlamento pela Lei nº 9.883/1999, que cria o Sisbin.

O texto não faz qualquer sentido, visto que o parlamento detém a titularidade do controle externo sobre toda a atividade estatal por força constitucional, o que por óbvio inclui as atividades de inteligência, sendo irrelevante o que diz uma lei ordinária.

Acrescentou-se também a definição de atividade de inteligência, atualizada e deslocada do art. 2º, que trata do objetivo da Comissão.

Objetivo

II - fica alterado o art. 2º, que passa a ter a seguinte redação:

> "**Art. 2º** A CCAI tem como objetivo fazer o controle político e assegurar a conformidade normativa das atividades de inteligência realizadas por órgãos e entidades federais.

O texto atual tem problemas de técnica legislativa, misturando objetivo, competência e definições legais. Manteve-se aqui apenas o objetivo.

Além disso, retirou-se a restrição à atuação sobre os órgãos e entidades do Executivo, visto que outros Poderes e Órgãos Autônomos também realizam atividades de inteligência e precisam passar pelo escrutínio da instituição que

possui legitimidade do voto popular.

Competências

III - no art. 3º, fica alterada a redação dos incisos I e II e inseridos os incisos XV a XXI e o parágrafo único, com a seguinte redação:

"**Art. 3º**.....

I - realizar o controle externo das atividades de inteligência realizadas em todo o ciclo da inteligência, inclusive em nível operacional;

Aqui não há inovação, mas apenas deslocamento do que estava mal localizado no art. 2º.

II - examinar e apresentar sugestões à Política Nacional de Inteligência a ser fixada em lei;

Atualmente, o texto diz que a Política é de responsabilidade da presidência. Como propomos que ela seja positivada em lei, precisa ser ajustado.

.....

XV – determinar à Ancai a realização de auditoria sobre as atividades de inteligência, com vistas a verificar a sua conformidade normativa;

XVI – determinar ao Tribunal de Contas da União a realização de auditoria sobre as atividades de inteligência, com vistas a verificar a sua conformidade normativa;

> Os dois incisos que antecedem dão ao controle parlamentar os recursos de expertise necessários para um controle eficaz.
>
> No caso do TCU, repete-se a prerrogativa regimental dada à CMO (**Resolução do Congresso Nacional nº 1, de 22 de dezembro de 2006**, art. 3º, I).
>
> Ainda, cabe destacar que o parágrafo único garante que essas ferramentas possam ser utilizadas por minorias, bastando que um terço dos membros requeiram (a exemplo das CPIs), de modo a impedir que o controle seja obstado por maiorias governistas.

XVII – realizar arguição pública de pessoas indicadas para:

a) o conselho diretor da Ancai;

b) cargos de direção ou chefia de órgãos de inteligência, nas hipóteses previstas na Constituição Federal;

XVIII – aprovar a investidura em cargo de direção ou chefia de órgão de inteligência, nas hipóteses previstas na Constituição Federal;

XIX – receber e analisar as Prestações de Contas das Atividades de Inteligência (PCAI); e

XX – analisar a seção do parecer prévio dedicada à atividades de inteligência, encaminhando o resultado de sua análise à CMO;

> Assim como a CCAI participa do processo de aprovação da LOA, deve fazer parte do processo de aprovação do parecer prévio, fechando o ciclo orçamentário.

XXI – convocar qualquer agente público integrante de órgãos e entidades que realizam atividade de inteligência para prestar, pessoalmente, informações;

> Atualmente, somente podem ser convocados ministros e titulares de órgãos vinculados à presidência. A ideia é ampliar para qualquer agente público, seguindo a lógica de que quem pode mais, pode menos. A ideia tem como base análise feita por Gonçalves e Bedritichuk (2024).

XXII – acessar dados e instalações dos órgãos e entidades controlados, independentemente do seu grau de sigilo.

O teor deste dispositivo estava no art. 2º. Além de ser deslocado, foi retirada de seu comando a necessidade de aviso prévio para a entrada em instalações, o que desnatura o caráter fiscalizatório.

Parágrafo único. As competências de que tratam os incisos XV e XVI, do caput, serão exercidas mediante requerimento de pelo menos um terço dos membros da Comissão."

Acesso à informação

IV – fica alterado o art. 4º, que passa a ter a seguinte redação:

"**Art. 4º** O parlamentar membro poderá requerer acesso a dados relacionados às atividades de inteligência sob custódia de órgão ou entidade federal, ou de privado contratado para tal fim, independente de anuência do plenário da Comissão ou de sua Presidência.

§ 1º O requerimento de que trata o caput será encaminhado por meio da Presidência da Comissão diretamente ao órgão ou entidade responsável.

§ 2º As informações deverão ser fornecidas no prazo de 10 (dez) dias a contar da data de envio.

§ 3º Na hipótese de negativa de acesso, a Presidência deverá encaminhar, no prazo de 30 (trinta) dias, pedidos de apuração de responsabilidade:

I – em relação à da autoridade requerida, por:

a) crime de prevaricação, na forma do art. 319, do **Código Penal**;

b) ato de improbidade administrativa, na forma do art. 11, inciso VI, da **Lei nº 8.429, de 2 de junho de 1992**;

c) infração administrativa, na forma do art. 32, da **Lei nº 12.527, de 18 de novembro de 2011**; e

d) crime de responsabilidade, caso aplicável à autoridade requerida; e

II – em relação ao privado requerido, na pessoa do responsável pelo contrato, por:

a) crime de falsidade documental, na forma de um ou mais tipos descritos nos arts. 297 a 299, do **Código Penal**;

b) infração administrativa de dificultar atividade de fiscalização ou intervir em sua atuação, na forma do inciso art. 155, inciso XII, da **Lei nº 14.133, de 1º de abril de 2021**, combinado com o art. 5º, inciso V, da **Lei nº 12.846, de 1º de agosto de 2013**.

§ 4º Não será considerada justificativa para a não prestação da informação a alegação de classificação sigilosa da informação, de risco para a segurança da sociedade e do Estado ou de segredo de justiça.

Convocação de autoridades

V – fica alterado o art. 5º, que passa a ter a seguinte redação:

"**Art. 5º** Comparecerão à CCAI anualmente, independente de convocação e vedada a delegação, entre abril e junho:

a) o Ministro-Chefe da Casa Civil;

b) os ministérios responsáveis pela segurança institucional da Presidência da República, pela defesa, pela segurança pública e pela política penal;

c) o Diretor-Geral da ABIN;

d) os dirigentes dos centros de inteligência das forças armadas;

e) os dirigentes dos órgãos de polícia federais.

Parágrafo único. A ausência injustificada é considerada negativa de acesso à informação."

Composição e presidência

VI – no art. 7º, ficam alterados o inciso III, do caput, e os §§ 1º e 2º, além de serem criados dois novos, que serão os §§ 2º-A e 2º-B, conforme redação que segue:

"**Art. 7º.** A escolha dos parlamentares que comporão a CCAI sedará da seguinte maneira:

I – 5 (cinco) Senadores e 5 (cinco) Deputados, dividindo-se as vagas de cada Casa entre as bancadas partidárias pelo critério da proporcionalidade;

II – 1 (um) Senador e 1 (um) Deputado, sendo suas vagas destinadas ao Partido que não tiver alcançado lugar na Comissão pelo critério da proporcionalidade, nos termos do art. 10-A do Regimento Comum do Congresso Nacional;

III – 1 (um) Senador eleito pela Comissão de Relações Exteriores e Defesa Nacional do Senado Federal, mediante votação secreta de seus membros; e

IV – 1 (um) Deputado eleito pela Comissão de Relações Exteriores e de Defesa Nacional da Câmara dos Deputados, mediante votação secreta de seus membros.

§ 1° As vagas previstas nos incisos I e II deste artigo serão preenchidas mediante indicação dos respectivos líderes.

§ 2° O cálculo da proporcionalidade e as indicações das lideranças serão feitos no início da primeira sessão legislativa.

§ 3° Os parlamentares eleitos para as vagas dos incisos III e IV não necessitam ser membros da respectiva Comissão.

§ 4° Os membros da CCAI terão um mandato de 4 (quatro) anos, não podendo ser substituídos nesse período, salvo em hipótese de mudança de partido ou de renúncia unilateral à vaga, situações em que a respectiva vaga será novamente preenchida de acordo com o procedimento estabelecido neste artigo.

§ 5° A Presidência e a Vice-Presidência da CCAI terão mandato de dois anos e serão eleitas por seus pares ao início da primeira e da terceira sessões legislativas, cabendo as vagas respectivamente:

I – à Câmara de Deputados e ao Senado Federal, na eleição da primeira sessão legislativa; e

II – ao Senado Federal e à Câmara de Deputados, na eleição da terceira sessão legislativa.

§ 6º Entre o início da primeira sessão legislativa e a eleição da Presidência, esta será exercida de forma temporária pelo Presidente da Comissão de Relações Exteriores e Defesa Nacional da Câmara de Deputados

§ 7º Cabe à Presidência temporária ou a um terço dos membros a convocação da reunião de instalação do colegiado."

O teor deste dispositivo repete a proposta feita no pacote da CCAI, que elimina os membros natos. Atualmente, a metade da comissão é preenchida por líderes de maioria e minoria e pelos presidentes das comissões de relações exteriores. Esse formato é danoso, pois implica colocar na colegiado alguém que não necessariamente quer estar ali e que tem diversas outras funções políticas relevantes. Utilizar a proporcionalidade é melhor, pois permite que as lideranças partidárias indiquem parlamentares mais vocacionados para a matéria.

A única diferença desta proposta para a da CCAI é que ela estende os mandatos de 2 para 4 anos, aumentando a estabilidade dos trabalhos, a autonomia dos membros e a profissionalização do colegiado.

Afastamento de membro

VII – fica inserido o art. 7º-A, com a seguinte redação:

Art. 7º-A. Na hipótese de existir fundada suspeita de que membro da Comissão possa estar envolvido em crime relacionado às atividades

por ela fiscalizadas, a Comissão poderá, mediante proposta do Presidente ou de um terço de seus membros, aplicar as seguintes medidas temporárias em relação ao referido membro:

I – restringir parcial ou por completo o acesso a determinados expedientes;

II – reduzir o nível de acesso da credencial de segurança;

III – suspender a eficácia da credencial de segurança;

IV – afastar o membro da Comissão.

§ 1º As medidas constantes no caput devem ter relação direta com a fundada suspeita, devendo-se respeitar o princípio da proporcionalidade e fundamentar detalhadamente cada uma das restrições.

§ 2º A decisão sobre a aplicação das medidas constantes no caput será tomada por dois terços dos membros da Comissão, sendo irrecorrível.

§ 3º No caso de aplicação da medida constante no inciso IV, do caput, o membro afastado poderá ser substituído, na hipótese:

I – dos incisos I e II, do **art. 7º**, pelos seus vices;

II – do inciso III, do **art. 7º**, por outros indicados."

Prestação de contas

VIII – fica alterado o título da Seção I, do Capítulo IV, os arts. 10 e 11, bem como são inseridos os arts. 11-A a 11-E, conforme redação que segue:

"Seção I
Da Prestação de Contas das Atividades de Inteligência

Relatórios, prazos e atores obrigados

Art. 10. A Prestação de Contas das Atividades de Inteligência (PCAI), ferramenta de controle parlamentar, é composta pelos seguintes documentos:

I – Relatório de Execução da Política (REP);

II – Relatório de Estado Tecnológico (RET);

III – Relatório de Atividades de Risco Elevado (RAR);

IV – Relatório de Compartilhamento de Informações (RCI).

§ 1º Devem encaminhar a PCAI à Comissão, independente de solicitação, até o dia 31 de março de cada ano:

I – os ministérios responsáveis pela segurança institucional da Presidência da República, pela defesa, pela segurança pública e pela política penal;

II – a Agência Brasileira de Inteligência;

III – os centros de inteligência das Forças Armadas;

IV – as diretorias de inteligência das polícias federais;

V – outros atores de inteligência, a pedido do parlamento.

§ 2º A Casa Civil da Presidência da República deve encaminhar à Comissão, independente de solicitação, até o dia 10 de março de cada ano, o Relatório de Soberania Nacional (RSN).

§ 3º A ausência total ou parcial de entrega da PCAI, nas datas previstas neste artigo configura negativa de acesso à informação.

Relatório de Execução da Política

Art. 11. O REP deve informar a contribuição do ator de inteligência para a implementação da Política Nacional de Inteligência, devendo nele constar, pelo menos:

I – a relação entre a política e:

a) a estrutura organizacional adotada;

b) as estratégias e diretrizes técnico-operacionais adotadas;

c) o histórico das atividades desenvolvidas.

II – indicadores objetivos e mensuráveis sobre o avanço obtido no período em termos de materialização da política;

III – a descrição pormenorizada das despesas das atividades de inteligência pagas no exercício anterior, vedadas rubricas genéricas ou agregações que impeçam a compreensão e a rastreabilidade integrais.

Relatório de Estado Tecnológico

Art. 11-A. O RET deve conter a relação de softwares, bases de dados e equipamentos utilizados nas atividades de inteligência, no exercício anterior, devendo indicar, em relação a cada um deles, de forma detalhada, no mínimo:

I – a sua finalidade;

II – as unidades administrativas usuárias, identificadas no menor nível hierárquico existente;

III – caso tenham sido adquiridos ou contratados:

a) em relação ao instrumento licitatório:

1. o número identificador;

2. a sua íntegra;

3. a justificativa para dispensa ou inexigibilidade de licitação, se for o caso.

b) em relação ao contrato:

1. o número identificador;

2. a sua íntegra, incluídos quaisquer aditivos;

3. a íntegra dos processos administrativos correlatos, incluídos os relacionados à fiscalização e sanções;

4. a totalidade de recursos empenhados, a ele relacionados, no exercício anterior.

c) as medidas de controle interno adotadas para:

1. evitar o uso abusivo;

2. proteger os dados de acessos não autorizados e de situações acidentais ou irregulares de destruição, perda, alteração, comunicação ou difusão.

d) detalhamento de todas as fases de tratamento de dados pessoais envolvidas no seu uso, incluindo o nome e localização das organizações, públicas ou privadas, onde o dado é tratado;

e) na hipótese de a tecnologia ser desenvolvida por organização estrangeira ou de seu funcionamento incorrer em operações de tratamento de dados pessoais que sejam realizadas fora do território nacional, informar:

1. detalhamento do componente tecnológico e das operações de tratamento de dados pessoais realizadas fora do território nacional;

2. a justificativa para não adotar solução nacional;

3. os potenciais riscos para a soberania nacional, incluindo possíveis transferências de dados sensíveis e limitações à auditabilidade pelo controle nacional.

Relatório de Atividades de Risco Elevado

Art. 11-B. O RAR deve conter a relação de mandados judiciais concedidos ou prorrogados no exercício anterior, independente de sua conclusão, cada qual acompanhada dos seguintes dados:

I – identificação do alvo e/ou técnica que a classifica como atividade de inteligência de risco elevado (IRE);

II – justificativa da ação;

III – sobre a decisão judicial que a autorizou:

a) número identificador dos autos;

b) data da decisão;

c) prazo da autorização.

Relatório de Compartilhamento de Informações

Art. 11-C. O RCI deve conter a relação de informações produto de IRE compartilhadas com atores de inteligência internacionais, no exercício anterior, ou deles recebidas, devendo-se indicar em relação a cada um delas:

I – sobre a decisão judicial que a autorizou o compartilhamento:

a) número identificador dos autos;

b) data da decisão;

c) a íntegra do parecer da Ancai, caso tenha sido contrário ao compartilhamento ou ao recebimento.

II – um resumo das informações compartilhadas ou recebidas.

Relatório de Soberania Nacional

Art. 11-D. O RSN deve conter o estado de dependência de tecnologias estrangeiras para a realização de atividades de inteligência, devendo nele constar, pelo menos:

I – quais os principais desafios para a redução da dependência;

II – de que forma as ações do Poder Executivo Federal, no exercício anterior, contribuíram para a redução da dependência;

III – quais ações estão sendo tomadas pelo Poder Executivo Federal, neste exercício, para a redução da dependência;

IV – quais ações precisam ser tomadas nos próximos 4 (quatro), 10 (dez) e 20 (vinte) anos para o enfrentamento de cada um dos desafios apontados pelo inciso I.

Procedimento

Art. 11-E. A PCAI será distribuída, por sorteio e de forma automática, a um dos membros da Comissão, que emitirá parecer no prazo improrrogável de 120 (cento e vinte) dias.

§ 1º Após a distribuição, a PCAI será imediatamente remetida à Ancai para análise preliminar, a ser exarada no prazo improrrogável de 60 (sessenta) dias, tendo como conteúdo:

> I – uma avaliação indicando se houve cumprimento do dever de prestar informação pelo órgão ou entidade, na forma desta Lei;
>
> II – uma avaliação indicando se as informações prestadas indicam violação ou risco de violação do ordenamento jurídico;
>
> III – recomendações para garantir o desenvolvimento das atividades do ator de inteligência em conformidade com o ordenamento jurídico;
>
> IV – recomendações de diligências complementares, se for o caso.

§ 2º O parecer será submetido à aprovação por maioria simples do plenário da comissão, 15 (quinze) dias após a sua entrega, sendo

dispensada a sua leitura no dia da apreciação e vedados os pedidos de vista.

§ 3º Se o parecer não obtiver o número de votos necessários à sua aprovação, será designado outro membro da comissão, dentre os prolatores dos votos majoritários, para emitir novo parecer.

§ 4º Uma vez aprovado o parecer, o presidente da comissão, em 30 (trinta) dias úteis, encaminhará:

I – a sua íntegra ao ator de inteligência controlado e ao órgão ao qual é imediatamente subordinado ou vinculado;

II – eventuais pedidos de apuração de responsabilidade.

Relatório de atividades

IX – no art. 13, fica alterado o caput, que passa a ter a seguinte redação:

"**Art. 13.** O Presidente da CCAI produzirá relatório anual, de caráter ostensivo, publicado em dezembro, elaborado com base nas informações constantes nas Prestações de Contas das Atividades de Inteligência, dele não podendo constar, sob hipótese alguma:

....."

Parecer prévio

X – fica inserida a Seção III-A, no Capítulo V, contendo os arts. 21-A e 21-B, conforme redação que segue:

"Seção III-A
Da análise da seção do parecer prévio dedicada às atividades de inteligência

Versão pública e sigilosa

Art. 21-A. O parecer prévio sobre as contas anuais do chefe do Poder Executivo, encaminhado pelo Tribunal de Contas, conterá seção específica relativa às atividades de inteligência, com duas versões:

I – uma pública, para fins de controle social; e

II – uma sigilosa, para fins de controle parlamentar.

Procedimento

Art. 21-B. O parecer prévio será distribuído, por sorteio e de forma automática, a um dos membros da comissão, que emitirá parecer no prazo improrrogável de 30 (trinta) dias, a contar do recebimento do parecer prévio.

§ 1º A versão sigilosa será previamente analisada pela Ancai, no prazo de 15 (quinze) dias, a contar do recebimento do parecer prévio.

§ 2º Aplica-se à tramitação as regras dos §§ 2º e 3º, do **art. 11-E**.

§ 3º Uma vez aprovado o parecer, o presidente da comissão o encaminhará imediatamente à CMO, na forma dos incisos do caput, sendo uma versão pública e outra sigilosa.

Art. 9º

Vigência

Esta Resolução entra em vigor na data de sua publicação, salvo os seguintes dispositivos, que entram em vigor no seguinte prazo a contar desta data:

I – um ano após o início da sessão legislativa subsequente, os incisos **VIII** e **X**, do **art. 8º**;

II – no início da sessão legislativa subsequente, os incisos **V**, **VI** e **IX**, do do **art. 8º**; e

III – em 6 (seis) meses, o prazo de 10 (dias), dado pela nova redação do § 2º, do **art. 4º**, da **Resolução do Congresso Nacional nº 2, de 22 de novembro de 2013**, seguindo-se no interregno o prazo de 30 (trinta) dias.

Agradecimentos

Este trabalho foi desenvolvido com contribuições de pesquisadores do ciclo de 2025 do Legiscraft e enriquecido por revisões externas e diversos diálogos com representantes da academia, do parlamento e da comunidade de inteligência, incluindo pessoas consultadas que solicitaram não ser nominadas.

O autor agradece, em ordem alfabética, aos seguintes interlocutores, que ofereceram contribuições críticas ou sugestões estruturantes para o desenho final da arquitetura proposta: Amir Cahane (Hebrew University of Jerusalem), Daragh Murray (Queen Mary University of London), Eric Denécé (Centre Français de Recherche sur le Renseignement), Jaseff Raziel Yauri-Miranda (Erasmus University Rotterdam), Lena Riecke (Leiden University) e Thorsten Wetzling (interface).

As opiniões aqui expressas são de exclusiva responsabilidade do autor e não refletem necessariamente as posições dos interlocutores ou de suas instituições.

Legiscraft

Ficha técnica

Título

Fundamentos para o controle da inteligência no Brasil

Autor

Conrado Klöckner

Tipo de documento

White paper

Instituição

Legiscraft

Ano

2026

Autores colaboradores

Débora Coward Fogliatto, Gabriel Oliveira Bohm, Isadora Zorzi, Luiz Eduardo Antonello, Renato Maciel Damiani, Samuel Alfredo Forneck, Vitória Battisti da Silva

Revisores internos

Samuel Alfredo Forneck, Vitória Battisti da Silva

Revisores externos

André Ramiro, Pedro Saliba, Vinicius Silva

Licença

Idioma

Português. Versão em inglês prevista.

Permalink

https://www.legiscraft.org/intelligence-governance


Legiscraft
Arquitetura legislativa