FGV EBAPE

RAP
REVISTA DE ADMINISTRAÇÃO PÚBLICA

Artigo

Controle externo das atividades de inteligência na era digital: um modelo exploratório

Conrado Klöckner [1]

Luiz Antonio Joia [1]

[1] Fundação Getulio Vargas / Escola Brasileira de Administração Pública e de Empresas, Rio de Janeiro - RJ, Brasil

O presente estudo desenvolve um modelo exploratório para avaliar o controle externo das atividades de inteligência em um país. Para esse fim, foi realizada uma revisão narrativa da literatura, por meio da qual foram coletadas e analisadas publicações científicas sobre esse tema. A partir daí, os elementos que caracterizam um sistema de controle externo de excelência das atividades de inteligência foram mapeados e estruturados sob a forma de um modelo de análise. O processo de criação do modelo trouxe, como resultados singulares, a clarificação do construto "capacidade de controle" e a apresentação do estado da arte da literatura científica acerca do controle externo das atividades de inteligência. O modelo proposto para avaliar o referido controle visa ser útil para estudos de caso e análises comparadas, facilitando, assim, o diagnóstico de fragilidades e subsidiando debates para sua própria melhoria. O uso do modelo objetiva proporcionar maior homogeneidade metodológica ao controle externo das atividades de inteligência na esfera digital, facilitando a compreensão global da temática, a comparação de resultados e a criação de hipóteses futuras a serem testadas. Por fim, este artigo apresenta um modelo exploratório e, portanto, ainda não testado, e a concentração geográfica dos dados obtidos pode ter limitado o alcance de sua aplicabilidade.
Palavras-chave: atividades de inteligência; controle externo; capacidade de controle; era digital.

Control externo de las actividades de inteligencia en la era digital: un modelo exploratorio

El presente estudio desarrolla un modelo exploratorio para evaluar el control externo de las actividades de inteligencia en un país. Para ello, se llevó a cabo una revisión narrativa de la literatura, mediante la cual se recopilaron y analizaron publicaciones científicas sobre el tema. Este proceso permitió mapear y estructurar los elementos que caracterizan un sistema de control externo de excelencia en forma de un modelo de análisis. Entre los principales aportes del proceso de construcción del modelo, se destacan la clarificación del constructo teórico "capacidad de control" y la presentación de los últimos avances/del nivel de desarrollo de la literatura científica sobre el control externo de las actividades de inteligencia. El modelo propuesto tiene como objetivo servir de herramienta útil para estudios de caso y análisis comparativos, lo cual facilita el diagnóstico de debilidades y respalda debates

ISSN: 1982-3134

DOI: https://doi.org/10.1590/0034-761220240271
Artigo submetido em 21 de agosto de 2024 e aceito para publicação em 28 de abril de 2025.
Editora-chefe:
Alketa Peci (Fundação Getulio Vargas, Rio de Janeiro / RJ – Brasil)
Editor-adjunto:
Sandro Cabral (Insper Instituto de Ensino e Pesquisa, São Paulo / SP – Brasil)
Pareceristas:
Francisco Wilson Ferreira da Silva (Universidade Federal do Ceará, Fortaleza / CE – Brasil)
Ricardo Rocha de Azevedo (Universidade de São Paulo, São Paulo / SP – Brasil)
Anna Carolina Mendonça Lemos Ribeiro (Instituto de Pesquisa Econômica Aplicada – Ipea, Brasília / DF – Brasil)
Relatório de revisão por pares:
O relatório de revisão por pares está disponível em https://periodicos.fgv.br/rap/article/view/94495/88065

orientados a su perfeccionamiento. Se espera que el uso del modelo proporcione mayor coherencia metodológica al control externo de las actividades de inteligencia en la era digital, favoreciendo una comprensión global del tema, la comparación de resultados y la formulación de hipótesis para futuras investigaciones. Finalmente, este artículo presenta un modelo exploratorio que aún no ha sido testado, y la concentración geográfica de los datos recopilados puede limitar el alcance de su aplicabilidad.
Palabras clave: actividades de inteligencia; control externo; capacidad de control; era digital.

External oversight of Intelligence activities in the digital age: An exploratory model

This study develops an exploratory model to assess the external oversight of a country's intelligence activities based on a narrative literature review. This process revealed key elements that characterize a high-quality accountability system, which were mapped and structured into an analytical model. Additionally, it led to a clear definition of the construct "oversight capacity" and offered an overview of the current literature on external oversight of intelligence activities. The proposed model serves as a valuable tool for case studies and comparative analyses, thereby facilitating the diagnosis of weaknesses in the accountability system and supporting discussions that may contribute to refining the model itself. Its use can improve methodological consistency in this area of study, leading to a more comprehensive understanding of the subject, promoting comparisons of results, and helping to generate hypotheses for future tests. Regarding its limitations, (i) the model is exploratory and, therefore, remains untested; and (ii) the geographic concentration of the data collected to develop the model may limit its scope of application.
Keywords: intelligence; oversight; oversight capacity; digital age.

1. INTRODUÇÃO

Há mais de uma década, Snowden (2019) revelou que qualquer dispositivo conectado poderia ser transformado em um espião capaz de recriar e prever, em minúcias, a rotina e as preferências de um indivíduo (Parson, 2018; Zuboff, 2020; União Europeia [UE], 2023). Desde então, as técnicas usadas pelos profissionais de inteligência foram bastante refinadas, tornando-se ainda mais invasivas (Xu, 2021). Nessa linha, a combinação de big data, inteligência artificial (IA), armazenamento em nuvem e internet das coisas, entre outras tecnologias emergentes, permite que qualquer governo crie seu próprio "kit distopia"[1], trazendo grave risco às liberdades individuais e à própria existência de regimes democráticos (UE, 2023).

Nessa esteira, o poder dos atores atuantes no mundo da inteligência tem aumentado de forma célere e contínua. No âmbito do controle externo das atividades de inteligência, todavia, não se vê progressos correspondentes (Korff et al., 2017; Cayford et al., 2018; Vieth & Wetzling, 2020; Roberts et al., 2021), o que tem gerado acirrados debates acerca da necessidade de robustas reformas institucionais (Weinstein et al., 2017). A presente pesquisa se insere nesse contexto, buscando, por meio da proposição de um modelo de avaliação do controle externo das atividades de inteligência, auxiliar a academia e os tomadores de decisão na avaliação de alternativas para um controle externo mais eficaz dessas atividades na era digital. Em outras palavras, este trabalho objetiva propor uma abordagem — fundamentada na literatura científica sobre o tema — para avaliação de sistemas de controle externo das atividades de inteligência conduzidas em um país, por meio da proposição de um framework e seus respectivos indicadores, de modo a compor um modelo exploratório para conduzir tal atividade.

Assim, adotando-se como estratégia uma revisão narrativa de literatura, este artigo explora os critérios comumente usados para analisar a eficácia de sistemas de controle externo das atividades de

[1] A expressão evoca a capacidade estatal de articular aparatos tecnológicos voltados à vigilância, aproximando a realidade de cenários distópicos em que a liberdade se estreita e a democracia se esvazia (Zuboff, 2019).

inteligência na era digital. Para essa análise, um modelo indutivo é proposto e apresentado, visando trazer maior harmonia para o desenvolvimento de estudos nessa área ainda pouco explorada, dar transparência às suposições e às etapas de pesquisas sobre essa temática, e permitir que outros estudiosos repliquem e aprimorem as análises aqui realizadas (Mershon & Shvetsova, 2019).

A pesquisa sobre sistemas de controle externo das atividades de inteligência — embora não seja novidade no Brasil (Cepik, 2003; Gonçalves, 2010) — é ainda limitada e com diversas lacunas identificadas na literatura acadêmica. Nessa linha, estudos recentes destacam a necessidade de aprofundamento da compreensão e eficácia dos mecanismos de controle externo das atividades de inteligência no Brasil (Klöckner, 2023; Ribeiro, 2023). Essa é, portanto, a lacuna de pesquisa que este artigo visa preencher por meio de suas contribuições.

De fato, algumas dimensões do controle externo das atividades de inteligência vêm sendo estudadas, como a importância de uma supervisão democrática (Born et al., 2015), a necessidade de equilíbrio entre segurança e transparência (Wills & Vermeulen, 2011) e os desafios na implementação de sistemas de controle das atividades de inteligência (Gill & Phythian, 2018). Por outro lado, outras temáticas associadas ao assunto continuam pouco exploradas, como o impacto efetivo desse controle externo (Born & Wills, 2012), o controle externo em contextos autoritários e híbridos (Abuza, 2016), a integração do controle com tecnologias digitais emergentes (Chesterman, 2021) e a perspectiva dos atores envolvidos (Gill, 2016).

Por outro lado, é mister enfatizar que o foco deste artigo é especificamente no controle externo das atividades de inteligência — o que o diferencia do controle externo das atividades do Estado, em geral (Phythian et al., 2008). O controle das atividades de inteligência se diferencia do genérico por algumas características únicas, as quais decorrem da natureza sensível, sigilosa e estratégica das operações de inteligência. Essas especificidades exigem abordagens e mecanismos distintos para garantir transparência e *accountability*, enquanto se protege a segurança nacional e as informações classificadas. De fato, o controle externo das atividades de inteligência é mais restritivo e especializado do que o controle geral do Estado. Ele deve equilibrar a necessidade de proteger informações sensíveis com a exigência democrática de prestação de contas. Esse controle frequentemente é realizado por comissões parlamentares e órgãos especializados, em vez de depender de mecanismos amplos e públicos usados para a supervisão de outras áreas governamentais (Caparini, 2016).

Dito isso, no que tange à estrutura deste trabalho, na próxima seção são apresentados os conceitos básicos e as definições operacionais usadas na pesquisa. A terceira seção, em seguida, detalha a metodologia adotada neste trabalho. Nas seções quatro e cinco, o modelo desenvolvido é, respectivamente, apresentado e discutido. Finalmente, na seção final de conclusão, detalham-se as implicações deste trabalho — tanto para o âmbito acadêmico como para a geração e avaliação de políticas públicas —, propondo-se uma agenda de pesquisa para a área de controle externo das atividades de inteligência empreendidas na era digital.

2. CONCEITOS BÁSICOS E DEFINIÇÕES OPERACIONAIS

2.1. Atividades de inteligência

Para Gill e Phythian (2018), são consideradas atividades de inteligência aquelas destinadas a melhorar a segurança ou a manter o poder de um agente em relação a seus concorrentes, por meio da previsão de ameaças e oportunidades. Neste estudo, entretanto, buscando analisar a eficácia do controle dessas ações, optou-se por adotar uma definição operacional mais restrita, limitando-se o escopo do trabalho às atividades mais desafiadoras para o controle — i.e., aquelas destinadas a produzir inteligência política, militar e policial. Esse grupo de ações, além de ser protegido pela narrativa permissiva da segurança coletiva, é caracterizado pelo sigilo e pela intrusividade.

De acordo com Gonçalves (2017), a inteligência política é aquela que subsidia o processo decisório nas esferas mais altas da administração pública, como as chefias de governo e de Estado. A inteligência militar, por sua vez, fornece subsídios ao processo decisório para fins de defesa nacional. A inteligência policial, por fim, objetiva produzir informações relevantes ao processo decisório dos órgãos responsáveis pela repressão e investigação criminal.

As atividades de inteligência desempenham um papel estratégico na segurança nacional, na proteção de interesses econômicos e na formulação de políticas públicas. No entanto, com o avanço da era digital, essas atividades passaram por transformações profundas, impulsionadas pelo acesso a grandes volumes de dados, uso de tecnologias digitais emergentes e aumento da conectividade global (Montasari, 2023; Polido, 2024).

As atividades de inteligência englobam ações relativas à coleta, análise e disseminação de informações para apoiar decisões críticas em contextos governamentais e empresariais. Essas ações, tradicionalmente dependentes de fontes humanas e físicas, evoluíram de modo a incluir métodos digitais e automatizados, redefinindo os limites da capacidade de inteligência (Khan et al., 2021).

O processo de inteligência engloba cinco etapas principais: planejamento e direção, coleta de dados, processamento, análise e produção, e disseminação (Ebell et al., 2021). A era digital, entretanto, trouxe mudanças significativas em todas as etapas desse processo. O advento do big data possibilitou a coleta massiva de informações de fontes diversificadas, como redes sociais, sensores IoT (Internet das Coisas) e registros eletrônicos. Esse cenário ampliou significativamente a base de dados disponíveis para análise, ao mesmo tempo que apresentou desafios relacionados à filtragem e ao gerenciamento de informações relevantes (Ainslie et al., 2023). Além disso, o uso de IA e aprendizado de máquina permitiu o desenvolvimento de sistemas capazes de identificar padrões complexos em grandes conjuntos de dados, prever comportamentos e antecipar ameaças. Essas tecnologias aumentaram a eficiência e a precisão das análises requeridas, reduzindo a dependência de processos manuais (Li, 2024). Em suma, as tecnologias digitais emergentes têm desafiado a atividade de controle externo da inteligência, tornando ainda mais relevante seu controle externo (Pătrașcu, 2021).

Por outro lado, a governança das atividades de inteligência é outro aspecto fundamental, exigindo adequada atenção. Esse conceito refere-se ao conjunto de políticas, normas e mecanismos de supervisão que regulam as práticas de inteligência, buscando equilibrar a eficácia operacional com os valores democráticos e os direitos humanos (Wegge, 2017). Estudos sugerem que a transparência e o *accountability* são essenciais para garantir que as atividades de inteligência sejam conduzidas de maneira ética e conforme as leis internacionais (Lester, 2015). No entanto, a complexidade das

tecnologias digitais utilizadas e a natureza confidencial dessas operações dificultam a implementação de mecanismos de supervisão adequados.

Desse modo, as atividades de inteligência desempenham um papel central em contextos nacionais e internacionais, especialmente em um mundo cada vez mais interconectado e digitalizado (Brantly, 2020). É crucial, no entanto, que essas práticas sejam desenvolvidas e implementadas com responsabilidade, respeitando os limites éticos e legais, e promovendo uma governança que assegure o equilíbrio entre segurança e direitos fundamentais (Kniep et al., 2024). Nessa linha, é mister que essas atividades sejam controladas, como explicado a seguir.

2.2. Controle das atividades de inteligência

As atividades de inteligência são usualmente supervisionadas por três tipos principais de controle: interno, externo e social — cada um com funções específicas para garantir a conformidade ética, legal e operacional dessas ações (Caparini, 2016).

O controle interno ocorre dentro das próprias agências de inteligência, envolvendo auditorias internas, supervisão hierárquica e códigos de conduta. Esses mecanismos buscam assegurar que as operações estejam alinhadas às normas institucionais e prevenir abusos de poder (Phythian et al., 2008). Além disso, unidades especializadas de conformidade garantem que os agentes sigam regulamentações internas e externas (Born & Wetzling, 2007).

O controle externo é exercido por órgãos independentes, como comitês legislativos, judiciário e agências fiscalizadoras. Esses mecanismos permitem maior *accountability* ao monitorar orçamentos, estratégias e operações das agências. Por exemplo, parlamentos e tribunais têm papel fundamental na validação da legalidade das operações, limitando abusos e promovendo a transparência institucional (Herman, 1996; Caparini, 2007).

Já o controle social é realizado por atores da sociedade civil, como a mídia, Organizações não Governamentais (ONGs) e cidadãos, que promovem maior supervisão por meio da pressão pública e da transparência. A mídia investigativa, por exemplo, desempenha um papel crucial ao expor irregularidades, enquanto organizações de direitos humanos monitoram práticas que possam violar liberdades civis (Zuboff, 2020; Gill, 2012). Além disso, iniciativas de liberdade de informação contribuem para aumentar o escrutínio público sobre essas atividades (Banisar, 2006).

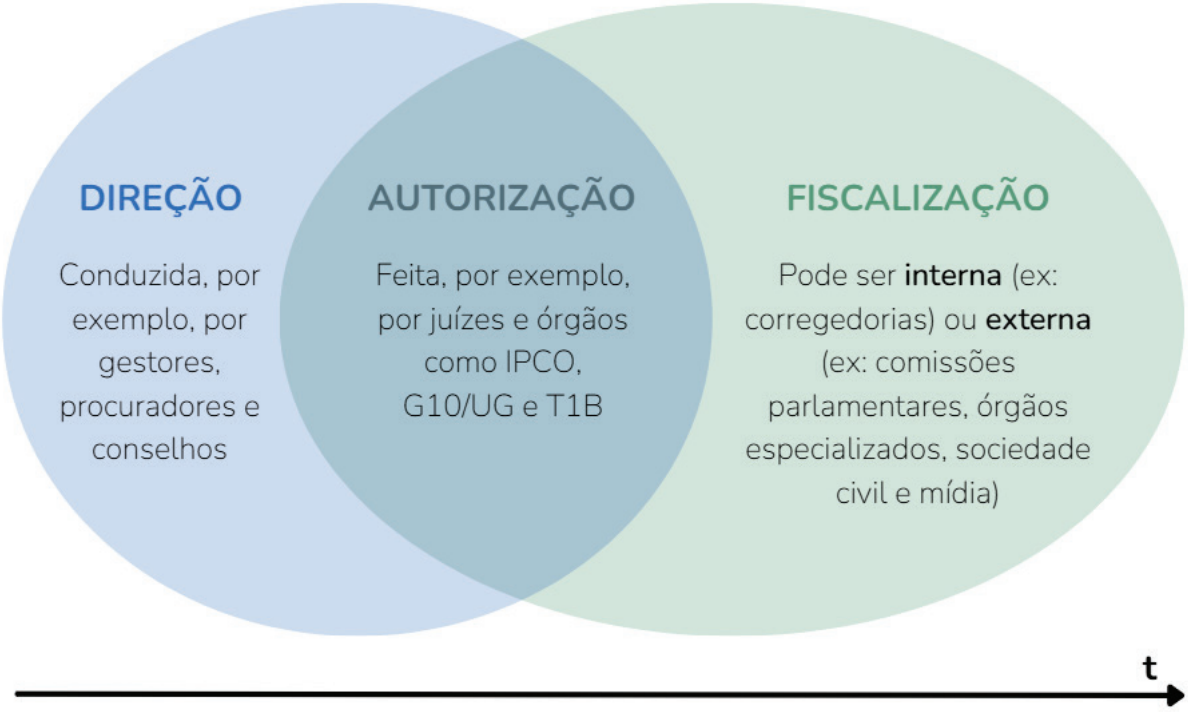
Esses três tipos de controle são complementares e cruciais para compatibilizar a capacidade de controle operacional das agências de inteligência com a proteção de direitos fundamentais e a promoção de valores democráticos.

Seguindo Gill (2020), o controle das atividades de inteligência engloba uma série de ações que podem ser agrupadas nos estágios de direção, autorização e fiscalização (Figura 1). A ação de direção (*control*) se refere à gestão e ao direcionamento das atividades de inteligência. A de autorização (*prior authorisation*), por sua vez, envolve a decisão de permitir que determinada atividade seja conduzida. Por fim, as ações de fiscalização (*oversight*) visam o escrutínio da eficiência, efetividade e conformidade de tais atividades.

Como dito, as ações, quando exercidas pelo próprio órgão controlado, são de controle interno; já quando exercidas por forças externas a ele, são identificadas como de controle externo. No âmbito da ciência política, considera-se que uma força é externa quando advém de uma estrutura organizacional independente daquela do controlado — o que, via de regra, envolve outro poder constitucional (Meirelles, 2015), como o Parlamento ou o Judiciário.

A concepção acima de Meirelles (2015) tem como premissa básica a existência de alguma instituição formal executando o controle externo das atividades de inteligência — foco deste trabalho. Entretanto, no âmbito das atividades de inteligência, a literatura aponta para a necessidade de se estender o conceito de controle externo para além das instituições formais, abarcando, também, a sociedade civil[2] (controle social) — que, historicamente, é quem tem conseguido, de fato, desempenhar esse papel. Nessa linha, autores como Parsons (2018), Dobson (2019), Gill (2022) e Kniep et al. (2024) defendem que essa inclusão é especialmente relevante, pois são os vazamentos e as denúncias feitas por *whistleblowers*[3], jornalistas e ativistas que têm possibilitado avanços reais em termos da *accountability* dessas atividades.

FIGURA 1 ESTÁGIOS DO CONTROLE DAS ATIVIDADES DE INTELIGÊNCIA



Fonte: Adaptada de Gill (2020, p. 972).

A seguir, discute-se de que forma a literatura científica tem abordado como avaliar a eficácia do controle externo de uma atividade estatal — neste caso, as atividades de inteligência.

[2] Leia-se ONGs, associações de direitos humanos, organizações comunitárias, sindicatos, universidades, jornalistas e outros atores que promovem a transparência, *accountability* e proteção dos direitos fundamentais em relação às ações de inteligência do Estado (Caparini & Cole, 2008).

[3] *Whistleblower* (ou denunciante) é uma pessoa que expõe informações confidenciais, ilegais, antiéticas ou prejudiciais sobre uma instituição pública ou empresa.

2.3. Medindo a eficácia do controle externo de atividades estatais

Não existe consenso sobre como mensurar a eficácia do controle de uma atividade estatal. De acordo com Kinyondo et al. (2015), a literatura sobre esse assunto se divide em quatro abordagens. A primeira defende que a eficácia sequer é mensurável; enquanto as outras três argumentam que ela pode ser medida por meio de variáveis *proxy* — sendo elas: (1) capacidade de controle, adotada nesta pesquisa; (2) nível de atividade de controle; e (3) qualidade das instituições.

Mensurar a eficácia do controle de uma atividade estatal com base na capacidade de controle significa avaliar se o controlador, caso queira, tem os insumos necessários para exercer seu trabalho — tais como recursos humanos e prerrogativas legais. Nessa abordagem, a principal fragilidade advém da compreensão de que a existência desses insumos não implica em que eles sejam de fato usados (Pelizzo & Stapenhurst, 2012). Kinyondo et al. (2015) argumentam, ainda, que essa abordagem é incapaz de explicar as variações de eficácia ao longo do tempo, em um sistema cuja capacidade de controle permanece a mesma.

Já a mensuração baseada no nível de atividade de controle reflete o volume de ações concretas executadas pelo controlador (e.g., quantas auditorias foram realizadas). Kinyondo et al. (2015) argumentam que a sua aplicabilidade como *proxy* pode levar a sérias imprecisões. Primeiro, porque o emprego de um instrumento de controle não necessariamente será eficaz. Segundo, porque a ausência de atividades de controle pode indicar, eventualmente, sua própria eficácia (via dissuasão), induzindo o pesquisador ao erro. Além disso, o uso dessa variável, no caso específico das atividades de inteligência, esbarra no sigilo que recai sobre os dados operacionais — o que torna esse tipo de mensuração praticamente inviável (Dobson, 2019).

Por fim, pode-se mensurar a eficácia do controle de uma atividade estatal por meio de variáveis relacionadas à qualidade das instituições, tais como aquelas que mensuram sua robustez democrática. A lógica por trás dessa escolha é que um controle eficaz impacta diretamente a saúde das instituições, a qual pode ser medida por variáveis como a citada. Aqui, o problema fundamental é que essas variáveis são influenciadas por diversos outros elementos que vão muito além dos sistemas de controle (e.g., a percepção de corrupção ou a participação eleitoral), tornando cientificamente inviável estabelecer relação causal dessas variáveis com um controle eficaz (Kinyodo et al., 2015). Além disso, essas variáveis envolvem construtos demasiadamente maleáveis, os quais dependem demasiadamente do juízo de valor de quem os formula.

Assim, verifica-se que todas as alternativas apresentadas têm limitações. Entretanto, a fragilidade associada ao uso da variável "capacidade de controle" para mensurar a eficácia do controle de uma atividade estatal parece ser a menos difícil de contornar na pesquisa científica (Caparini, 2016). Por outro lado, a mais óbvia vantagem de seu uso é a necessidade da análise de insumos que, via de regra, estão descritos em documentos públicos — o que é definitivo em estudos sobre inteligência. Além disso, deve-se notar que a análise de outras variáveis necessariamente precisa passar por ela. De fato, a capacidade de controle é anterior à ação de controle em si, e ao seu respectivo impacto. Poderia ocorrer, por exemplo, de a capacidade de controle externo disponibilizada ao controlador não ser por ele utilizada. Porém, se não houver capacidade de controle, certamente não haverá ação de controle — e, muito menos, um controle eficaz (Pelizzo & Stapenhurst, 2012).

3. PROCEDIMENTO METODOLÓGICO

Esta pesquisa adotou como estratégia a realização de uma revisão de literatura visando ao desenvolvimento de um modelo teórico para avaliação da capacidade de controle externo das atividades de inteligência (Paul & Criado, 2020; Post et al., 2020). Assim, foi conduzida uma revisão narrativa de literatura (Theile & Beall, 2024), sendo tal escolha justificada pela escassez de estudos sobre o tema, necessidade de explorar conceitos teóricos, multidisciplinaridade da temática e limitações impostas pela confidencialidade. Além disso, a flexibilidade da revisão narrativa de literatura permite integrar informações diversas e gerar uma análise crítica, contribuindo para o avanço do conhecimento em um campo ainda pouco explorado (Baumeister & Leary, 1997; Green et al., 2006; Grant & Booth, 2009; Ferrari, 2015).

Para condução dessa revisão de literatura, foram usadas três importantes bases de dados: Scopus, *Web of Science* e SSRN. Mongeon e Paul-Hus (2016) recomendam o uso das duas primeiras bases de dados pela sua abrangência superior a de outras bases, interface amigável e funcionalidades bibliométricas, cobertura multidisciplinar e revisão por pares (*double blind review*). Da mesma forma, Chadegani et al. (2013) as recomendam por sua robustez metodológica, alinhada às exigências associadas a revisões narrativas de alta qualidade. Adicionalmente, como sugerido por Veletsianos e Shepherdson (2016), foram buscados artigos científicos no repositório SSRN — base especializada em trabalhos em ciências sociais, economia e direito —, a qual oferece acesso a pesquisas em estágio inicial e documentos de trabalho. De fato, essa base inclui estudos que podem não estar disponíveis em revistas indexadas tradicionais, garantindo-se, assim, a inclusão de discussões recentes e inovadoras.

A revisão de literatura foi realizada ao longo do 1º trimestre de 2024 — segundo as etapas sugeridas por Okoli e Schabram (2010) —, valendo-se, entretanto, de eventuais flexibilizações inerentes a revisões narrativas de literatura (Siddaway et al., 2019). Seu propósito foi clarificar o construto "capacidade de controle" e mapear os elementos que compõem a ideia de capacidade de controle em um cenário de excelência — ou seja, o que, afinal, um controlador precisa ter para conseguir executar, de forma eficaz, seu trabalho. A partir desses subsídios, foi possível desenvolver um modelo de análise.

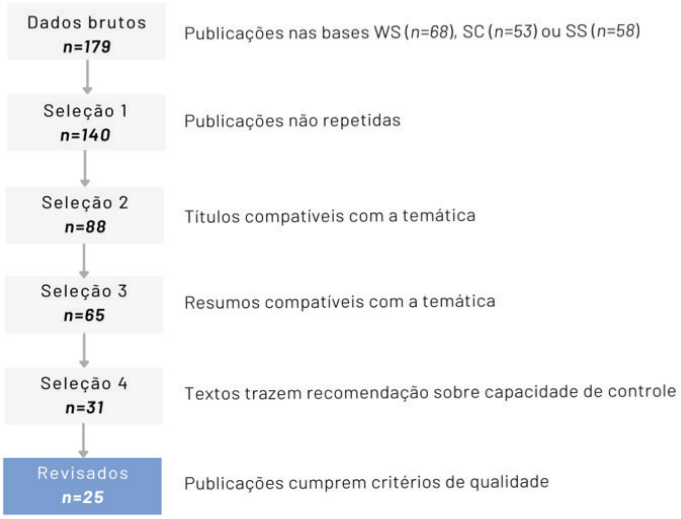
A revisão de literatura teve como ponto de partida as publicações sobre controle das atividades de inteligência encontradas a partir dos critérios de busca detalhados no Quadro 1. Os dados foram tratados tendo como referência os preceitos da teoria fundamentada, a qual prevê um processo cíclico de coleta e análise que somente finda quando identificada a saturação teórica (Thiry-Cherques, 2009; Wolfswinkel et al., 2013). No estudo, estes ciclos de coleta e análise foram sendo feitos por ano, de forma descendente, começando por 2023. Isto é, os artigos foram coletados e analisados ano a ano, via seus títulos e resumos e, em caso de interesse, de seu texto integral. A seguir, passava-se para o ano seguinte em escala descendente. Ao chegar-se a artigos publicados antes de 2018, verificou-se que, além de serem cada vez mais escassos, eles apenas reforçavam temas já identificados em anos mais recentes, sem acrescentar insights significativos — o que indicou uma saturação teórica (Minayo, 2017) e levou ao fim do procedimento de busca. O processo de triagem desses dados está detalhado na Figura 2.

QUADRO 1 CRITÉRIOS DE BUSCA

Categoria	Critério
Base de dados	Scopus, ou *Web of Science*, ou SSRN
Tipo de publicação	Artigos científicos
Data da publicação	Entre os anos de 2018 e 2023 (até 1º de abril)
Idioma	Inglês
Termos de busca (operador booleano) no título e resumo dos artigos pesquisados	"*surveillance oversight*" OR "*surveillance accountability*" OR "*surveillance regulation*" OR "*intelligence oversight*" ou "*intelligence accountability*" ou "*intelligence regulation*"

Fonte: Elaborado pelos autores.

FIGURA 2 ETAPAS DE TRIAGEM DOS DADOS



Fonte: Elaborada pelos autores.

Na fase de coleta, foram selecionados textos cujo objetivo principal era gerar recomendações[4] específicas relativas à eficácia de sistemas de controle. Excluiu-se, assim, aqueles que traziam apenas recomendações genéricas e abrangentes sobre o funcionamento de sistemas de controle, assim como aqueles voltados a outras formas de controle que não o externo.

[4] Por recomendações, entenda-se as conclusões e opiniões manifestadas pelos autores dos artigos analisados, os quais identificaram que determinado elemento afetava positivamente um sistema de controle.

Por fim, os artigos foram submetidos a um controle de qualidade abarcando dois critérios: (i) terem sido publicados em revista com revisão por pares (*blind peer-reviewed*); ou (ii) serem vinculados a uma instituição de pesquisa dedicada ao tema de controle da inteligência.

Ao fim, foram selecionados 25 textos, conforme apresentado nos Quadros 2 e 3.

QUADRO 2 SELEÇÃO FINAL DE ARTIGOS (I) – *BLIND PEER-REVIEWED*

Referência	Revista
Berman (2022)	*University of Illinois Law Review*
Bihar (2020)	*International Journal of Intelligence and CounterIntelligence*
Cahane (2020)	*International Journal of Intelligence and CounterIntelligence*
Defty (2020)	*Intelligence and National Security*
Defty (2022)	*Intelligence and National Security*
Dobson (2019)	*The British Journal of Politics and International Relations*
Duroy (2022)	*Journal of International Dispute Settlement*
Gill (2020)	*Intelligence and National Security*
Gill (2022)	*Australian Journal of Human Rights*
Gogolewska (2021)	*Connections: The Quarterly Journal*
Hillebrand (2019)	*Intelligence and National Security*
Kniep et al. (2024)	*Review of International Studies*
Krivokapić et al. (2021)	*Journal of Regional Security*
Mayer (2018)	*Yale Law Journal*
Moses (2022)	*Osgoode Hall Law Journal*
Muchwa (2021)	*Intelligence and National Security*
Obuobi (2018)	*International Journal of Intelligence and CounterIntelligence*
Van Brakel (2021)	*Surveillance & Society*
Walsh (2022)	*Intelligence and National Security*
Young et al. (2019)	*Big Data & Society*

Fonte: Elaborado pelos autores.

QUADRO 3 SELEÇÃO FINAL DE ARTIGOS (II) – INSTITUCIONAIS

Referência	Instituição
Broeders et al. (2019)	The Hague Program for Cyber Norms
Cahane (2021)	Heinrich Böll Stiftung
Cordero e Fellow (2019)	Center for New America Security
Parsons (2018)	Citizen Lab
Vieth e Wetzling (2020)	Stiftung Neue Verantwortung

Fonte: Elaborado pelos autores.

A coleta e a análise dos dados seguiram as diretrizes traçadas por Wolfswinkel et al. (2013). Assim, a partir da leitura integral das publicações, os excertos relevantes ao atingimento do objetivo da pesquisa foram extraídos, comparados, categorizados e articulados — em um processo contínuo de codificação. Nesse processo, algumas categorias centrais se sobressaíram, permitindo conectá-las com a construção teórica (Langley, 1999). Nesta pesquisa, conforme detalhado na seção seguinte, essas categorias foram: "*Garantias de Autonomia*", "*Poderes*" e "*Meios*". A integração e o refinamento dessas categorias, de modo a formar um todo coeso, permitiram a construção de um modelo teórico para avaliação do controle externo das atividades de inteligência.

4. MODELO PARA AVALIAÇÃO DO CONTROLE EXTERNO DAS ATIVIDADES DE INTELIGÊNCIA

O ponto de partida para a proposição de um modelo para avaliação do controle externo das atividades de inteligência foi a definição de "capacidade de controle". Para tal, adotou-se uma estratégia que se desdobrou em duas etapas: (1) compilar os excertos da revisão empreendida que, expressamente, citavam "capacidade"; e (2) submeter esses excertos à comparação analítica, buscando, por meio de codificação, identificar as categorias centrais. No Quadro 4, as quatro definições de capacidade de controle encontradas foram fragmentadas e codificadas, de modo a facilitar a identificação do cerne deste construto.

QUADRO 4 CODIFICAÇÃO DAS DEFINIÇÕES DE CAPACIDADE DE CONTROLE

Referência	Categorias que compõem a "capacidade de controle"		
	Garantias de Autonomia	Poderes	Meios
Hillebrand (2019)	Vontade Política		Recursos e Expertise
Vieth e Wetzling (2020)		Concessão de Mandato	
Duroy (2022)	Controlador Independente		Recursos
Moses (2022)		Outorga de Prerrogativas	Expertise

Fonte: Elaborado pelos autores.

O processo de codificação indicou que o construto "capacidade de controle" abarca uma série de elementos que podem ser organizados segundo três categorias principais: as garantias de autonomia, os poderes e os meios. Essas categorias representam, respectivamente, as condições volitivas[5], formais e materiais associadas à ação de controle.

Os poderes[6] representam as ferramentas dadas ao controlador pela legislação. Na prática, são previsões abstratas de ação. Para que elas deixem de ser ações em potencial e se materializem, são necessários recursos — i.e., os meios. Por fim, de nada adianta ter poderes e meios, se o controlador não tem autonomia para agir — ou seja, se a arquitetura institucional não dispuser de mecanismos para impedir ou mitigar ameaças ao livre exercício de sua vontade.

A partir dessa lógica, observa-se que cada uma das três categorias acima é, isoladamente, indispensável para uma eficaz ação de controle. Satisfeitas essas condições, pressupõe-se que o controlador poderá agir, se assim o desejar. A partir desse entendimento, pode-se definir a capacidade de controle como: "o conjunto de garantias de autonomia, poderes e meios fornecido ao agente de controle para que ele possa exercer as suas funções".

Na sequência, o estudo mapeia os elementos que compõem cada uma dessas três categorias em um sistema de controle de excelência. Para fins didáticos, as categorias ficam doravante identificadas como dimensões Autonomia, Poderes e Meios.

4.1. Dimensão Autonomia

Para que a vontade do controlador seja livre e, portanto, exista a possibilidade de uma ação de controle, é preciso construir mecanismos para impedir ou mitigar tentativas de coação ao controlador. Ações

[5] As condições volitivas representam o estado interno de vontade ou disposição de uma pessoa, sendo fundamentais para explicar decisões e comportamentos. Ou seja, dizem respeito à vontade, intenção ou poder de escolha de um indivíduo (Pires & Andrade, 2022).

[6] A expressão "Poderes" não deve ser confundida com o conceito de "Poder". Poderes, na pesquisa sobre controle externo das atividades de inteligência, refere-se às condições externas — ferramentas — concedidas ao controlador por quem de direito. Portanto, "Poderes", no sistema de controle externo de inteligência, diz respeito à autoridade legal conferida, potencialmente, a órgãos externos para supervisionar, monitorar e, se necessário, investigar as atividades de serviços de inteligência, assegurando que estes órgãos não ultrapassem os limites do direito e da liberdade individual. Gill (2020) diferencia muito bem "ter poderes" de "exercer poder"", destacando a importância do contexto político e operacional para que os poderes concedidos se traduzam em ações eficazes.

irregulares de inteligência podem derrubar governos, criar crises diplomáticas e colocar pessoas importantes atrás das grades. É natural, portanto, presumir que haja pressão sobre os responsáveis por apurar e processar eventuais irregularidades (Caparini, 2016). Dado que os atingidos por esse controle são quase sempre autoridades políticas, policiais ou de inteligência — nada menos que especialistas em coação —, a pressão pode atingir patamares elevadíssimos (Borghard & Lonergan, 2017).

Assim, para mitigar a possibilidade de coação, a literatura revisada apresenta um grupo de estratégias visando salvaguardar a autonomia do agente de controle, conforme apresentado abaixo.

4.1.1. Regulamentação

O primeiro passo para se atingir autonomia está na construção de uma regulamentação clara acerca das atividades de inteligência e de seu controle. O argumento é que uma normatização frágil funciona como força de dissuasão do controlador. Controlar implica comparar a realidade com um padrão (Zairi, 2010). Assim, se esse padrão não está claro, ou se o controlador não tem segurança de como pode atuar, qualquer ação sua será arriscada. De um lado, se o embasamento jurídico de sua ação não está claro, a chance de impunidade aumenta; por outro lado, essa mesma insegurança jurídica pode levá-lo a temer retaliações à sua pessoa. Assim sendo, a falta de nitidez promove a dissuasão tanto pelo medo de retaliações quanto pela sensação de impotência gerada.

De fato, essa falta de clareza normativa é apontada por Berman (2022) como uma das razões centrais pelas quais o descontrole crônico é um padrão no âmbito da inteligência. Para resolver isso, a literatura recomenda uma regulamentação que detalhe os poderes e limites das ações de inteligência e de seu controle (Obuobi, 2018; Broeders et al., 2019; Gill, 2020), trazendo clareza às definições operacionais (Parsons, 2018; Young et al., 2019; Berman, 2022) e indicando, de forma precisa, os atores responsáveis (Gogolewska, 2021).

4.1.2. Freios tradicionais

A independência institucional entre o controlador e o controlado é apontada como um atributo central para o controle das atividades de inteligência (Hillebrand, 2019; Gill, 2020). Como essas atividades são, via de regra, levadas a cabo pelo Poder Executivo, a literatura recomenda que o seu controle seja feito por autoridades vinculadas a outros poderes, mormente em democracias emergentes, como no caso do Brasil (Matei & Bruneau, 2011). Na forma tradicional dos sistemas de freios e contrapesos, o controle da administração cabe ao Parlamento e ao Judiciário.

As menções da literatura à importância do Judiciário estão relacionadas ora à atividade típica de controle de legalidade dos atos administrativos, ora à prerrogativa específica de autorizar previamente a coleta de dados por meio de ações intrusivas (Cahane, 2020; Gill, 2022; Kniep et al., 2024). Quando existente, a função autorizativa tende a ser alocada a jurisdições especializadas em inteligência (Mayer, 2018; Cahane, 2020; Berman, 2022).

O Judiciário, por ser uma força desenhada para atuar de forma contramajoritária, tende a ser o poder mais independente de pressões políticas. No que se refere ao Parlamento, a questão da independência material é mais espinhosa. Nas democracias, os governos necessitam construir bases de apoio para manter a governabilidade — o que deixa o Legislativo em uma posição mais vulnerável em termos de autonomia.

Pode-se citar, por exemplo, a África do Sul, Sérvia e os Estados Unidos, onde Gill (2020) observa que as comissões parlamentares geralmente são controladas pela base do governo — o que por si só tende a afastá-las de ações críticas à gestão executiva. Nessa linha, em artigo sobre o sistema de controle da inteligência polonês, Gogolewska (2021) argumenta que os parlamentares relutam em responsabilizar o governo, sendo raras as manifestações críticas decorrentes. Semelhantemente, em artigo sobre o sistema de controle de inteligência de Uganda, Muchwa (2021) observa que, apesar de o Parlamento ter poder para ir muito além, ele se limita a acompanhar as questões orçamentárias.

Em um estudo comparado, Defty (2020) aprofunda esse diagnóstico, apontando com maior detalhamento razões práticas para tal ingerência. Em sua análise, que trata do funcionamento das comissões parlamentares de quatro países (Canadá, Austrália, Nova Zelândia e Reino Unido), a conclusão é de que todas elas eram controladas pelo Executivo. No Canadá, todos os membros são escolhidos pelo Primeiro-Ministro; na Nova Zelândia, o próprio Chefe de Governo preside a comissão; na Austrália, a maioria dos membros deve ser da base governista; e no Reino Unido, a comissão somente pode iniciar uma investigação a pedido do próprio governo ou do conjunto da casa legislativa, limitando ainda mais a criação de uma agenda de controle externo independente.

Diante dessa tendência à interferência, a literatura recomenda mecanismos de mitigação, os quais se materializam ora por meio de limitações à participação direta do governo, ora via garantias de maior participação de partidos de fora da base aliada. Seguindo a primeira linha, Defty (2020) demonstra contrariedade à possibilidade de o governo escolher membros dessas comissões ou ter assento nelas. Já Gogolewska (2021) critica a possibilidade de o governo ter poderes de vetar o acesso de algum parlamentar à comissão. Cordero e Fellow (2019) e Defty (2020), por sua vez, apresentam mecanismos para garantir uma maior participação de partidos não governistas, seja por meio de uma cota mínima de assentos na comissão, seja recomendando que a presidência dela fique sempre com a oposição.

4.1.3. Freios complementares

Outra estratégia apontada pela literatura envolve aumentar a diversidade de atores na trincheira do controle (Chesterman, 2008). A ideia é pensar na autonomia como um atributo não só de um controlador específico, mas de uma rede de controle externo. Nessa linha, a fraqueza de um ator pode ser suplantada pela força de outro, de modo que haja caminhos possíveis em caso de omissão. Tal abordagem se revela importante, na medida em que os freios tradicionais (Judiciário e Parlamento) apresentam uma série de limitações.

O Judiciário é um poder naturalmente inerte, trabalhando apenas quando alguma demanda lhe é trazida por interessados no cumprimento da lei (Junior & de Quadros, 2021). No caso das atividades de inteligência, em razão do sigilo, essas demandas sequer são conhecidas. Assim, no formato tradicional, uma ilegalidade somente será submetida ao controle judicial em duas hipóteses: (i) se alguma autoridade de controle externo com poder de monitorar tais atividades identificar a ilegalidade; ou (ii) se houver algum vazamento de informações.

O Parlamento, por sua vez, é bastante sensível às interferências do Executivo. Gill (2007) argumenta que o controle das atividades de inteligência talvez seja o maior desafio do Parlamento. Hegemann (2018) e Obuobi (2018) explicam que esse desafio se deve a diversas peculiaridades envolvidas nesse processo, especialmente à dificuldade de dele tirar frutos eleitorais, já que a atuação é sigilosa e qualquer crítica pode facilmente ser lida como uma ameaça à segurança nacional.

A seguir, alguns possíveis freios complementares são descritos.

i) Controle especializado

Gill (2020) defende que o controle parlamentar seja complementado por um órgão especializado. O autor argumenta que os políticos têm status e legitimidade para desenvolver a ação fiscalizatória, mas geralmente carecem de tempo, expertise e vontade política para tal. Esses últimos atributos poderiam ser oferecidos a um órgão especializado. Broeders et al. (2019) seguem a mesma linha, propondo um órgão complementar que seja capaz de conduzir investigações e prestar contas ao Parlamento.

Em estudo sobre as atividades de inteligência de Israel, Cahane (2020, 2021) chega à mesma conclusão. Em uma avaliação sobre a atuação do Parlamento Israelense na fiscalização de tecnologias de rastreamento usadas na pandemia, o autor ressalta sua incapacidade de ir além de questões políticas e legislativas em nível macro, sendo necessário um órgão complementar para fazer o controle em nível operacional.

Nessa linha, diversos países já possuem órgãos do tipo, podendo-se citar como exemplos: o *Investigatory Powers Commissioner's Office* – IPCO ("Escritório do Comissário para os Poderes de Investigação"), do Reino Unido; a *Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* – CTIVD ("Comissão de Supervisão dos Serviços de Inteligência e Segurança"), dos Países Baixos; e o *Tilsynet med Efterretningstjenesterne* – TET ("Supervisão dos Serviços de Inteligência"), da Dinamarca.

ii) Controle público

Em caso de ineficácia dos mecanismos formais de controle, alguns autores defendem que denúncias possam ser trazidas a público (Gill, 2022; Kniep et al., 2024). Essa possibilidade funciona como uma espécie de última cartada para defender a autonomia da rede de controle externo. Diferentemente da denúncia tradicional, feita às instituições formais, a denúncia pública é feita diretamente à sociedade, seja por meio da mídia ou de organizações civis.

Para defender essa possibilidade, Kniep et al. (2024) argumentam que são os escândalos — e não as respostas institucionais — que movimentam a história do controle. De acordo com os autores, são os vazamentos e as denúncias feitas por *whistleblowers,* jornalistas e ativistas que têm gerado os constrangimentos necessários para construir avanços capazes de eliminar ou mitigar abusos cometidos em nome da inteligência.

Esse fenômeno também foi observado por Parsons (2018) e Dobson (2019). Para exemplificá-lo, Kniep et al. (2024) citam o caso Snowden. Os programas de vigilância revelados pelo *whistleblower* já eram de conhecimento dos freios tradicionais. Não obstante, as autoridades em questão foram incapazes (ou não quiseram) detê-los. Em relatório recente sobre o mau uso de softwares espiões, a União Europeia (2023) apontou preocupação no mesmo sentido, destacando a permissividade dos agentes de controle.

Essa inação do controle tradicional teria como causa central o que a literatura identifica como "*ring of secrecy*" — uma espécie de "clube do segredo". Esse "clube" representa o fenômeno de aproximação entre os controladores e controlados, que passam a participar do restritíssimo grupo que tem alto nível de acesso a informações sigilosas (Kniep et al., 2024). De acordo com a tese, a proximidade pessoal nesse círculo tenderia a suavizar ou afastar interpretações mais radicais, criando uma tendência ao *groupthink* (Duroy, 2022). Ademais, o fato de o controlador, em geral, depender do controlado para

obter informações incentivaria posturas colaborativas. Essa característica também obstaria checagens independentes, compelindo o controlador a anuir com o que está posto. Por fim, a exigência de segredo impediria o livre extravasamento de críticas (Hegemann, 2018).

Um exemplo desse fenômeno é trazido por Cahane (2021), em estudo sobre o controle externo das atividades de inteligência em Israel. Nesse país, tanto a coleta de dados de comunicação quanto a colocação de escutas para fins de persecução criminal são submetidos a um controle judicial *ex-ante* — i.e., exige-se uma autorização prévia. De acordo com o autor, pedidos do tipo são indeferidos em menos de 0,5% dos casos — o que indicaria uma postura omissa por parte dos controladores.

Assim, as denúncias públicas, de acordo com os autores que as defendem, serviriam para quebrar essas barreiras de inércia institucional. Em termos práticos, Kniep et al. (2024) ressaltam a importância de fornecer respaldo jurídico para os denunciantes. Para esse fim, os autores apontam como referência de marco legal os princípios de Tshwane (American Civil Liberties Union [ACLU], 2013), que definem, por exemplo, o tipo de conteúdo que pode ser trazido a público e como funciona o ônus da prova.

4.2 Dimensão Poderes

Para que consiga cumprir suas funções, o controlador deve receber da legislação um conjunto robusto de ferramentas (tais como a possibilidade de realizar investigações ou requisitar informações). A presente seção trata dessas ferramentas em duas partes. Uma primeira é destinada a compreender seu alcance — ou seja, até onde o controlador pode ir com o uso de tais prerrogativas (nesse caso, analisa-se, por exemplo, se uma requisição de informação poderia alcançar dados de operações de inteligência). A segunda parte é destinada a apresentar cada uma das ferramentas, por meio do mandato necessário e das prerrogativas concedidas.

4.2.1. Mandato

Por mandato, entenda-se os limites da jurisdição do controlador — i.e., até onde ele pode ir no uso de suas prerrogativas (Firmo, 2022). Nesse aspecto, a literatura a seguir aponta que um controle eficaz necessita de um mandato com alcance significativamente maior.

A primeira questão diz respeito a quem está sendo controlado. A literatura aponta que a inteligência atual não envolve mais somente agências tradicionais, alongando-se por meio de uma vasta rede de *stakeholders* que facilmente escapa ao devido controle — incluindo polícias, setor privado e atores de outros países (Gill, 2020; Moses, 2022).

Quanto às polícias, Korff et al. (2017) e Bloch-Wehba (2021) destacam a crescente interconexão entre as suas funções e as desempenhadas pelas agências tradicionais, reforçando que ambas já estão em pé de igualdade em termos de capacidade técnica e potencial de intrusividade. Gill (2020), por sua vez, aponta para a crescente participação do setor privado, que segue apartado do controle, apesar de fornecer a maior parte dos softwares, equipamentos e serviços que movimentam a inteligência contemporânea.

Por fim, com a expansão das cooperações internacionais, houve aumento significativo tanto no risco de um país receber informações obtidas de forma inadequada, quanto de ter informações suas usadas para fins que jamais admitiria em seu território. Por essa razão, defende-se que as cooperações precisam se submeter a um processo de controle (Broeders et al., 2019; Walsh, 2022). Uma prática trazida pela literatura é a dos Países Baixos, onde o compartilhamento de informações com outros

países passa por uma análise de riscos feita pelo próprio controlador (Gill, 2020; Vieth & Wetzling, 2020). Por meio dela, seria possível, por exemplo, avaliar se o país destinatário tem salvaguardas suficientes para impedir que a informação compartilhada seja utilizada para fins não admitidos no país de origem.

Em razão dessa expansão da rede de atores, defende-se que o critério para definição do mandato do controlador deixe de ser institucional para ser funcional (Gill, 2020). No primeiro caso, dá-se ao controlador a responsabilidade sobre determinados atores (e.g., Exército). No segundo, dá-se a responsabilidade sobre determinada finalidade (e.g., ações de inteligência voltadas à defesa nacional). Considerando-se a complexa rede contemporânea de atores, a tendência é de que o uso do critério institucional possa deixar uma série de atividades a descoberto (Gill, 2020).

Além desse aumento de alcance subjetivo, a literatura também recomenda que o controle possa abarcar atividades operacionais, deixando de cuidar apenas de questões macro, como as normativas e as financeiras (Matias-Pereira, 2022). Fazer o controle operacional significa acompanhar o trabalho de inteligência na ponta, o que inclui, por exemplo, ter acesso a dados sobre uma ação clandestina ou ter acesso direto aos softwares usados pelas agências (Broeders et al., 2019).

Em resumo, a literatura indica, quanto ao aspecto subjetivo, o critério funcional como o mais adequado para o controle da rede contemporânea de inteligência (Gonçalves, 2019; Gill, 2020). Quanto ao aspecto material, a literatura destaca que um controle eficaz precisa "descer" ao nível operacional (Broeders et al., 2019; Defty, 2020; Berman, 2022).

Por outro lado, a literatura científica também enfatiza a necessidade de mandatos protegidos e proteção legal para o controlador — i.e., a estabilidade dos mandatos dos membros do órgão controlador, protegidos contra remoções arbitrárias, é fundamental, impedindo interferências políticas e assegurando continuidade nas funções de controle (Born et al., 2005).

4.2.2. Prerrogativas

Na sequência, a partir da revisão de literatura, são apresentadas as cinco prerrogativas que um sistema de controle externo das atividades de inteligência deve ter para ser considerado eficaz.

i) Acesso à informação

Informação é a matéria-prima para o controle. Um controlador que não souber com o que está lidando é invariavelmente incapaz de realizar o seu trabalho (Hillebrand, 2019; Defty, 2020; Vieth & Wetzling, 2020). Defty (2020), em estudo sobre o controle parlamentar em quatro países da *Commonwealth*, identificou uma série de limitações ao exercício desse poder. A principal é a vedação de acesso a dados operacionais. Além disso, de forma mais geral, o autor critica a tendência dos governos em apelar para critérios vagos — como "segurança nacional" — de modo a indeferir o acesso dos controladores à informação.

Vieth e Wetzling (2020) aprofundam essa análise, apontando caminhos para um controle efetivo das práticas de vigilância em massa. Esses autores explicam que, diante de uma quantidade expressiva de dados, o controle somente é possível se for feito de forma contínua e com acesso direto aos sistemas operacionais do controlado. Para um controle efetivo, esses autores julgam que seria necessário, por exemplo, que a autoridade tivesse algoritmos para acompanhar qualquer compartilhamento, exclusão

ou busca de dados que fugisse do padrão usual. Ou ainda, que tivesse um sistema capaz de vincular cada dado colhido à sua autorização prévia, de modo que pudesse facilitar a aferição de sua conformidade.

As medidas acima demandam um amplo nível de acesso à informação, o qual, de acordo com os autores, envolve não somente a análise de bases de dados exportadas, mas também o acesso completo e direto aos sistemas operacionais usados pelos órgãos de inteligência. Como *benchmark*, citam o órgão especializado de controle da Dinamarca, o TET, que tem total acesso aos sistemas operacionais e aos *logs*.

Vieth e Wetzling (2020) também observam que não basta a previsão de acesso à informação. É essencial que as informações sejam tratadas de modo que uma auditoria seja possível. Para esse fim, sugerem a inserção das autoridades de controle já na fase de construção dos processos e sistemas usados pelos órgãos de inteligência. Para que essa participação seja efetiva, esses autores sugerem que as medidas necessárias para permitir o controle devam ser obrigatoriamente incorporadas pelos órgãos (*oversight-by-design principle*)[7].

ii) Aprovação do orçamento e prerrogativa orçamentária do órgão controlador

A aprovação do orçamento pelo Parlamento, conhecida como poder da bolsa, é uma prática consolidada para todo gasto público, não sendo extraordinário sugerir o mesmo em relação às atividades de inteligência. Cordero e Fellow (2019), entretanto, dão um passo além, trazendo dois elementos para qualificar o uso dessa ferramenta. O primeiro refere-se a alocar a autoridade orçamentária em comissões parlamentares dedicadas especificamente ao tema da inteligência. O segundo elemento, ligado ao primeiro, sugere que as autorizações de programas de inteligência estejam nas mesmas mãos que aprovam o orçamento — o que não somente qualifica o controle, como também dá maior poder de barganha ao controlador.

Nessa mesma linha, a prerrogativa de o órgão controlador elaborar sua previsão orçamentária — ou seja, sua capacidade de definir seu próprio orçamento de forma livre — é também, segundo a literatura científica, altamente desejável para que o controle externo das atividades de inteligência possa ser bem-sucedido (Born et al., 2015).

iii) Independência na nomeação da liderança da agência de inteligência

Em governos democráticos, é comum que algumas chefias estratégicas não sejam de livre escolha do administrador da vez (Lopes & Vieira, 2023). Um dos processos de seleção usado para mitigar essa discricionariedade é a submissão do nome indicado pelo governo ao escrutínio do Parlamento (Krause et al., 2006). Dois dos artigos compilados via revisão de literatura recomendam essa prática em relação às agências de inteligência (Obuobi, 2018; Muchwa, 2021). Ambos são estudos de sistemas de controle externo das atividades de inteligência de países africanos (Gana e Uganda, respectivamente) — e em ambos os casos o Parlamento analisado não possuía essa prerrogativa. Obuobi (2018) relata claramente que a livre escolha da chefia da agência de inteligência pelo Poder Executivo de Gana deixa a agência instável e vulnerável à captura política.

[7] Conjunto de medidas destinadas a garantir a auditabilidade dos sistemas desde sua construção — também conhecido como compliance by design (Moses, 2022).

iv) Autorização de ações intrusivas

A ideia de um controle *ex-ante* das atividades de inteligência visa diminuir as possibilidades de impunidade e evitar que somente haja uma reação quando o estrago já está feito. Isso é especialmente relevante no âmbito das ações de inteligência, onde as violações facilmente atingem o núcleo de diversos direitos fundamentais, podendo, inclusive, impactar a legitimidade das instituições democráticas ou mesmo sua própria existência (Gill & Phythian, 2013).

Em pesquisas sobre a qualidade do controle das atividades de inteligência, Duroy (2022) e Gill (2020) elencam a autorização *ex-ante* de poderes intrusivos como um relevante indicador de qualidade do controle. Mayer (2018), por sua vez, sugere um rígido controle *ex-ante* especificamente para os casos em que haja interceptação de comunicação em tempo real, muito comum na inteligência contemporânea. Em defesa desse modelo, Mayer (2018) cita o procedimento adotado nos Estados Unidos, onde se exige um "supermandado" repleto de cuidados e critérios especiais.

No entanto, essa autorização prévia, ao mesmo tempo que pode representar um controle necessário para supervisão das atividades de inteligência, pode também ser elemento de fragilização das ações de inteligência — por demandar tempo e trazer à tona algo que, muitas vezes, deveria ser mantido restrito a um grupo pequeno de stakeholders (Gill, 2020). Nessa linha, alguns autores sugerem que essa autorização prévia seja concedida via regras gerais, reduzindo seu tempo de concessão, assim como a possibilidade de publicização exagerada do controle externo das atividades de inteligência (Leigh & Wegge 2018; Lester & Rogg, 2018). Mayer (2018), por sua vez, sugere um rígido sistema de autorização *ex-ante* do controle, especificamente para os casos em que haja interceptação de comunicação em tempo real, algo frequente na inteligência contemporânea. Na defesa desse modelo, o autor cita o procedimento adotado nos Estados Unidos, via jurisprudência, que exige um "supermandado" repleto de cuidados e critérios para tais casos.

Portanto, como se pode depreender, este é um tema ainda em aberto na literatura científica pesquisada.

v) Supervisão externa sobre o controlador

A criação de mecanismos de supervisão sobre o órgão controlador, como comitês legislativos ou agências internacionais, pode reforçar sua independência ao dificultar sua captura institucional (Born et al., 2005). Nessa linha, ONGs e a mídia (tradicional ou digital) podem exercer supervisão externa sobre o órgão controlador, de modo que este não seja cooptado pelo *establishment* vigente (Keane, 2009). De fato, a mídia pode atuar como um vigilante independente, investigando e divulgando informações sobre as operações dos serviços de inteligência. Assim, ao expor possíveis abusos ou irregularidades, a mídia pode informar o público e pressionar por reformas e responsabilização (Hillebrand, 2012). Nessa mesma linha, as ONGs podem contribuir monitorando e avaliando as atividades de inteligência, assim como assegurando que estas respeitem os direitos humanos e as liberdades civis. Podem, também, realizar pesquisas, publicar relatórios e advogar por políticas que garantam a responsabilização dos órgãos de inteligência (Kniep et al., 2024).

vi) Realização de investigações

Um processo de investigação pode envolver diversas ações, tais como convocar alguém a depor, quebrar sigilos ou fazer interceptações. A literatura estudada não traz essas especificações, indicando apenas que o poder de conduzir investigações próprias é fundamental para um controle eficaz (Gill, 2020; Moses, 2022). Dois textos vão além, destacando a importância de o controlador poder iniciar investigações, sem provocação ou autorização de terceiros (Broeders et al., 2019; Defty, 2020).

Uma recomendação conexa é a do monitoramento contínuo, que sugere a insuficiência de investigações meramente reativas (Berman, 2022; Moses, 2022). O monitoramento, como uma antessala da investigação, serve para garantir que o caráter sigiloso das ações não sirva para promover a impunidade. Essa prerrogativa é especialmente relevante diante das tecnologias atuais, que possibilitam a extração indiscriminada e contínua de dados pessoais (Bajpai, 2017).

Veja-se o exemplo do aplicativo espião *Pegasus* — utilizado para perseguir jornalistas, opositores e ativistas em diversos países (Kirchgaessner et al., 2021). O relatório da União Europeia (2023) sobre o uso desse aplicativo destaca que, nas interceptações telefônicas comuns, autorizações judiciais prévias devem demarcar o limite das informações que podem ser acessadas. Quando se invade um smartphone, no entanto, tem-se um acesso irrestrito e descontrolado à vida do indivíduo-alvo. A autorização prévia, nesses casos, dificilmente será suficiente para conter abusos. Isso também se aplica a investigações reativas. Nesse caso, a fiscalização somente seria de fato possível se o controlador pudesse realizar o monitoramento contínuo da ação de vigilância, o que implica, como sugerem Vieth e Wetzling (2020), em ter acesso direto aos softwares usados pelas agências e a seus respectivos *logs*.

4.3. Dimensão Meios

Os meios são os recursos humanos e materiais necessários para que os controladores consigam materializar suas prerrogativas. A suficiência desses recursos aparece na literatura — ora como uma referência genérica à necessidade de recursos e pessoal, ora sob a forma de demanda por maior especialização dos quadros (Broeders et al., 2019; Gill, 2020; Vieth & Wetzling, 2020; Duroy, 2022; Van Brakel, 2021).

Van Brakel (2021), analisando o controle das atividades de inteligência na Bélgica, traz um exemplo da importância dos meios. Na sua avaliação, os órgãos de controle do país, apesar de terem as prerrogativas necessárias para realizar investigações, não apresentam condições materiais e humanas para tal. Tal fato é, também, identificado por Defty (2020) em estudo sobre o controle parlamentar em quatro países da *Commonwealth*. A partir de sua análise, esse autor identifica que em apenas um dos países estudados — Austrália — a comissão possuía pessoal próprio. Nos outros três, os recursos humanos eram fornecidos pelo próprio Executivo, podendo inclusive envolver agentes oriundos dos próprios órgãos de inteligência. Essa influência, conclui Defty (2020), afeta não somente as condições materiais, mas também a autonomia do controle.

A conexão entre suficiência de recursos e autonomia também surge em Gill (2020), que aponta como essencial a existência de uma sede própria, separada do Executivo, bem como a capacidade de executar os protocolos que dão segurança às informações tratadas. A questão da sede própria também foi trazida por Defty (2020), que destacou essa deficiência em relação ao comitê parlamentar britânico.

A seguir, detalha-se dois dos meios mais necessários para um adequado controle das atividades de inteligência: expertise e dedicação exclusiva.

4.3.1. Expertise e dedicação exclusiva

A inteligência contemporânea envolve tecnologias emergentes cujo uso e compreensão exigem altíssimo conhecimento técnico. Por isso, alguns autores vão além do pleito simples por recursos humanos, qualificando a sua demanda por meio de expressões como expertise (Krivokapić et al., 2021; Van Brakel, 2021). Moses (2022), nessa linha, afirma que de nada adianta ter pleno acesso aos dados, se não há pessoal capacitado para entender e avaliar o seu conteúdo.

Walsh (2022), por sua vez, ressalta a importância de se recrutar especialistas em áreas que dominam o debate atual, tais como interferência estrangeira, inteligência artificial e tecnologias de uso dual. Já Vieth e Wrestling (2020) defendem que a autoridade controladora deve ter os subsídios necessários para estar — pelo menos — tecnologicamente em par de igualdade com as agências. A expertise, apontam, é elemento essencial para que os controladores possam ter autonomia em relação a consultores externos e agências controladas.

Por outro lado, parte da literatura científica também sugere que o controle das atividades de inteligência seja realizado por atores exclusivamente instituídos para esse fim, em dedicação exclusiva. No parlamento de Gana, por exemplo, Obuobi (2018) aponta como um problema o fato de o tema ser tratado por uma comissão genérica sobre defesa e interior, atuando em tempo parcial. Outros autores vão além, sugerindo a criação de um novo órgão, independente e complementar, voltado em dedicação exclusiva à tarefa de controle das atividades de inteligência (Cahane, 2020; Gill, 2020).

4.4. Modelo de análise

Os resultados da revisão de literatura oferecem subsídios para a construção de um modelo de avaliação do controle externo das atividades de inteligência, por meio da consolidação das três dimensões e dos sete elementos de análise apresentados. Este modelo tem como alicerce as seguintes premissas:

a) as ações estatais não alcançadas pelo controle externo são espaços de abuso de poder em potencial, conforme a teoria dos freios e contrapesos (Lowenstein, 1979);

b) a capacidade de controle é uma condição mínima e necessária para que o controle exista (Pelizzo & Stapenhurst, 2012);

c) a capacidade de controle é uma variável *proxy* adequada para avaliar a eficácia do controle das atividades de inteligência;

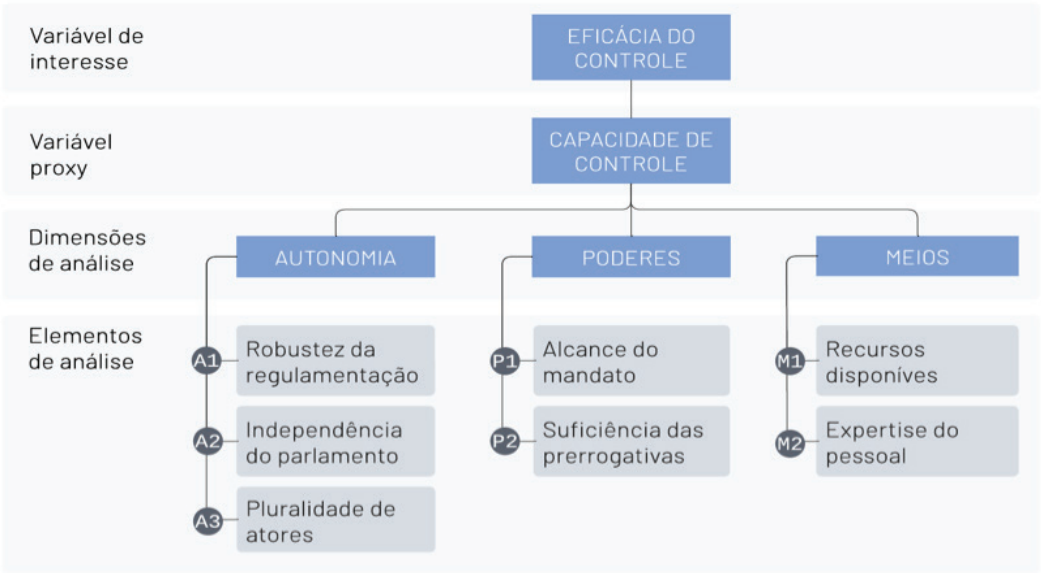
d) a capacidade de controle pode ser entendida como o conjunto de garantias de autonomia, poderes e meios fornecido ao agente de controle para que ele possa exercer as suas funções;

e) cada uma das três dimensões da capacidade de controle (autonomia, poderes e meios) é, isoladamente, uma condição necessária para a existência de capacidade de controle;

f) e, em conjunto, as três supracitadas dimensões são condição suficiente para a existência de capacidade de controle.

Assim, tendo como base esse alicerce lógico, as recomendações identificadas na literatura foram agrupadas sob forma de um modelo — isto é, de uma estrutura lógica e funcional dedicada a facilitar análises e avaliações futuras do controle externo das atividades de inteligência (Figura 3).

FIGURA 3 MODELO DE ANÁLISE PROPOSTO



Fonte: Elaborada pelos autores.

Os elementos de análise de cada dimensão foram representados de modo a permitir a setorização da análise e o agrupamento de eventuais indicadores. Assim, tanto as dimensões quanto os elementos de análise podem ser lidos como variáveis do modelo em questão. Estudos futuros podem operacionalizar essas variáveis por meio de indicadores.

Para abrir caminho para essa operacionalização, o conjunto de recomendações advindas da literatura revisada foi estruturado em um rol de critérios de análise, cada qual vinculado a um dos sete elementos de análise apresentados no modelo, conforme descrito no Quadro 5.

QUADRO 5 CRITÉRIOS DE ANÁLISE PARA CADA ELEMENTO DO MODELO

A1	Robustez da regulamentação	Referências
A1.1	Regulamentação das atividades de inteligência	Parsons (2018); Broeders et al. (2019); Young et al. (2019); Gill (2020); Gogolewska (2021); Krivokapić et al. (2021); Berman (2022)
	1) tem status de lei;	
	2) detalha atores, mandato, finalidades, poderes e seus limites.	

(Continua)

A1.2	Regulamentação do controle das atividades de inteligência 1) tem status de lei; 2) detalha atores, mandato, finalidades, poderes e seus limites.	Obuobi (2018); Gill (2020)
A2	**Independência do Parlamento**	**Referências**
A2.1	Existe comissão específica para o controle da inteligência	Cordero e Fellow (2019); Defty (2020)
A2.2	Comissão parlamentar que faz controle da inteligência tem regras para: 1) vedar membros do governo na composição; 2) garantir a composição multipartidária; 3) garantir à oposição poder para escolher ou vetar a presidência.	Cordero e Fellow (2019); Defty (2020)
A3	**Pluralidade de atores**	**Referências**
A3.1	Existe unidade judiciária específica para demandas relacionadas ao controle da inteligência	Mayer (2018); Cahane (2020); Berman (2022)
A3.2	Existe órgão especializado de controle da inteligência, independente do Executivo, com função de controle complementar às do Parlamento e do Judiciário	Broeders et al. (2019); Cahane (2020); Gill (2020); Cahane (2021)
A3.3	Existe sistema legal de proteção para denúncias públicas sobre ilegalidades no âmbito da inteligência	Gill (2022); Kniep et al. (2024)
P1	**Alcance do mandato**	**Referências**
P1.1	Escopo do mandato alcança atividades em nível operacional	Broeders et al. (2019); Defty (2020); Berman (2022)
P1.2	Escopo do mandato é definido com referência à finalidade da atividade controlada, e não ao órgão (primazia do critério funcional)	Gill (2020); Moses (2022)
P1.3	Escopo do mandato alcança atividades de inteligência que tenham como finalidade: 1) segurança de Estado; 2) defesa nacional; 3) segurança pública; 4) investigação criminal.	Gill (2020); Moses (2022)
P2	**Suficiência de prerrogativas**	**Referências**
P2.1	Controle tem poder de requisitar acesso a qualquer informação sob custódia do controlado e de empresas que prestam serviços a este, incluindo: 1) acesso direto aos softwares e sistemas operacionais, bem como seus *logs* e códigos-fonte; 2) acesso a informações recebidas por meio de cooperações internacionais; 3) acesso às instalações físicas.	Obuobi (2018); Broeders et al. (2019); Hillebrand (2019); Defty (2020); Gill (2020); Vieth e Wetzling (2020); Duroy (2022); Moses (2022); Kniep et al. (2024)
P2.2	Controle tem poder de determinar alterações nos sistemas e processos considerados inauditáveis	Vieth e Wetzling (2020)

(Continua)

P2.3	Controle tem poder de decidir se um membro do seu quadro de pessoal pode receber credencial de segurança	Gogolewska (2021)
P2.4	Controle tem poder de aprovar a indicação de chefia dos órgãos controlados	Obuobi (2018); Muchwa (2021)
P2.5	Controle tem poder de aprovar o orçamento dos órgãos controlados e tem autonomia orçamentária própria	Born e Leigh (2015); Cordero e Fellow (2019)
P2.6	Controle tem poder de autorizar previamente a coleta de dados por meios intrusivos	Mayer (2018); Cahane (2020); Gill (2020); Duroy (2022); Berman (2022)
P2.7	Controle tem poder de iniciar e conduzir investigações para averiguar a legalidade de atividades de inteligência	Broeders et al. (2019); Hillebrand (2019); Defty (2020); Gill (2020); Moses (2022)
P2.8	Controle tem poder de realizar monitoramento contínuo do controlado e de solicitar supervisão externa independente	Born et al. (2005); Born et al. (2015); Vieth e Wetzling (2020); Berman (2022); Moses (2022)
M1	**Recursos disponíveis**	**Referências**
M1.1	Controle tem recursos materiais, financeiros e humanos em quantidade compatível com as suas atribuições	Broeders et al. (2019); Gill (2020); Vieth e Wetzling (2020); Duroy (2022); Van Brakel (2021)
M2	**Expertise do pessoal**	**Referências**
M2.1	Nível de expertise do pessoal dos controladores é equivalente ao dos atores controlados	Hillebrand (2019); Cahane (2020); Gill (2020); Vieth e Wetzling (2020); Cahane (2021); Krivokapić et al. (2021); Van Brakel (2021); Berman (2022); Moses (2022)

Nota: A = Dimensão Autonomia; P = Dimensão Poderes; M = Dimensão Meios.
Fonte: Elaborado pelos autores.

O rol de critérios apresentado traduz todas as recomendações encontradas na revisão de literatura conduzida. A escolha por apresentá-las por completo no Quadro 5 fundamenta-se na necessidade de permitir que, nessa fase inicial, o modelo proposto seja uma ferramenta flexível de exploração (Mershon & Shvetsova, 2019). O que se busca, afinal, não é construir mandatoriamente um espelho da realidade, mas sim facilitar a compreensão do fenômeno estudado (Shoemaker et al., 2004).

5. DISCUSSÃO

A literatura científica demonstra que o atual estado da arte das atividades de inteligência é de grave descontrole, sendo imperativo o avanço de agendas de reforma institucional capazes de promover um maior controle sobre as referidas atividades (Weinstein et al., 2017; Gill, 2020). A partir da revisão de literatura conduzida, pode-se observar que as publicações voltadas à análise da capacidade de controle das instituições podem fornecer subsídios importantes para esses processos de reforma. Geralmente, esses estudos têm como objetivo avaliar se os controladores possuem as condições necessárias para exercer as suas funções. Como resultado, esses trabalhos trazem diagnósticos potencialmente relevantes tanto para os agentes políticos quanto para a academia.

O conjunto desses estudos peca, no entanto, pela falta de harmonia metodológica. De fato, os critérios e as categorias de análise utilizados nesses trabalhos variam bastante de autor para autor. Tal fato dificulta não apenas o desenvolvimento de novas pesquisas nessa temática, mas, também, a

comparação de resultados, a compreensão global da temática, a criação de hipóteses e seu consequente uso para fins de construção e reforma das políticas públicas associadas ao controle externo das atividades de inteligência.

Obuobi (2018), por exemplo, busca avaliar a efetividade do sistema de controle de Gana. Seu texto, no entanto, não informa quais são os critérios de análise, restringindo-se a apresentar uma descrição das instituições envolvidas, seguida de uma avaliação desacoplada de uma teoria de base capaz de sustentar as conclusões apresentadas e justificar o procedimento metodológico adotado. Uma tendência que reforça essa debilidade é a prevalência de pesquisas que focam em apenas parte do sistema de controle. Defty (2020), por exemplo, trata apenas de um dos agentes controladores — o Parlamento; Moses (2022), por sua vez, aborda apenas um dos controlados — a Polícia. Embora ambos sejam estudos comparados de um conjunto quase idêntico de países, a falta de uma gramática comum dificulta a avaliação conjunta dos resultados oriundos dessas pesquisas.

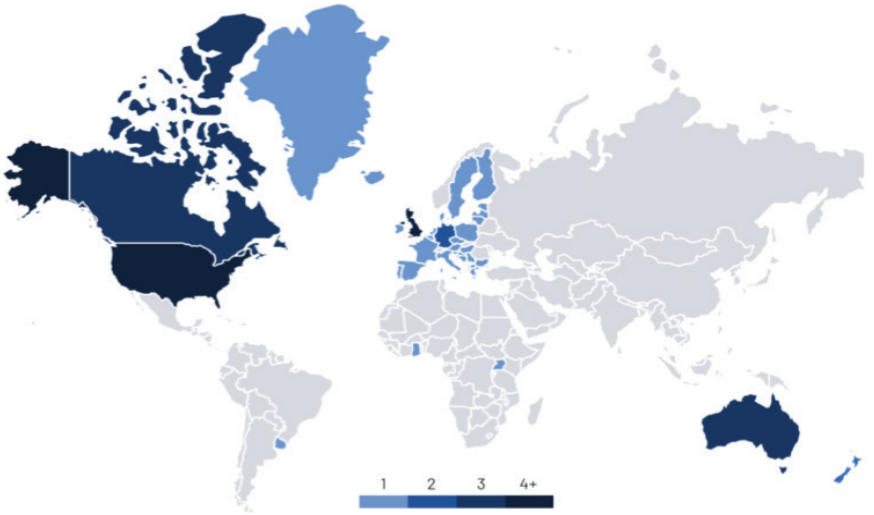
Assim sendo, um pesquisador ou agente político que queira avaliar a capacidade de controle das instituições de seu país terá dificuldade em saber para onde olhar e que régua utilizar. Nessa linha, o modelo proposto busca preencher essa lacuna e, desse modo, satisfazer uma precondição para o avanço das pesquisas no domínio do controle externo das atividades de inteligência. Sua estrutura é, assim, especialmente útil para estudos de caso e análises comparadas, mormente quando o objetivo for diagnosticar fragilidades do sistema de controle externo das atividades de inteligência.

Dito isso, torna-se necessário discutir duas potenciais limitações importantes à aplicabilidade do modelo proposto, quais sejam: (1) o modelo foi desenhado para facilitar a análise do sistema de controle externo como um todo, e não de um órgão controlador de forma isolada; e (2) os elementos e critérios de análise têm como origem, principalmente, estudos sobre instituições localizadas nas democracias ocidentais — o que pode, eventualmente, limitar seu uso em outros contextos.

Em relação ao primeiro ponto, o modelo foi idealizado a partir da compreensão de que tanto as atividades de inteligência quanto seu controle são difusos, sendo pouco útil um diagnóstico que avalie instituições de forma isolada. Tome-se, por exemplo, o elemento de análise "alcance de controle", cuja avaliação demanda investigar se o mandato do conjunto de controladores cobre todas as atividades de inteligência. Pode ocorrer, por exemplo, de as lacunas do controle parlamentar serem compensadas por prerrogativas de uma autoridade judicial — e isso somente se percebe em uma análise conjunta das instituições. Assim, a única setorização que o modelo contempla é baseada em dimensões ou elemento de análise — tendo-se sempre como pano de fundo o conjunto de instituições. É possível, por exemplo, comparar diversos países, avaliando especificamente se o seu sistema de controle tem prerrogativas suficientes — elemento de análise P2 no modelo proposto (ver Quadro 5 para um maior detalhamento).

Em relação ao segundo ponto, deve-se destacar possíveis limites de aplicabilidade do modelo, decorrentes do contexto de onde foram extraídos os dados que o originaram. De fato, a maior parte das pesquisas analisadas tiveram como objeto de estudo os sistemas de controle de países ocidentais desenvolvidos, especialmente os anglo-saxões, os quais respondem por 53% das publicações — um fenômeno já identificado pela literatura (Defty, 2020; Kniep et al., 2024). Estudos voltados ao Sul Global, por sua vez, respondem por apenas 12% das referências levantadas. A Figura 4 dá uma dimensão dessa concentração.

FIGURA 4 FREQUÊNCIA DE VEZES EM QUE CADA PAÍS FOI OBJETO DE ESTUDO



Frequência: (1) Áustria, Bélgica, Bósnia Herzegovina, Croácia, Eslovênia, Gana, Macedônia do Norte, Polônia, Sérvia, Uganda, União Europeia, Uruguai; (2) Alemanha, Israel, Nova Zelândia; (3) Austrália, Canadá; (4) Reino Unido; (5) Estados Unidos.

Fonte: Elaborada pelos autores.

Assim sendo, quando o sistema político onde o modelo proposto pretende ser aplicado se afasta do padrão vigente nas democracias ocidentais, há que se ter cuidado ao usar os elementos e critérios de análise propostos pelo modelo — atentando-se, assim, à variação dos fatores culturais e institucionais (Davison & Martinsons, 2016). Essa limitação, no entanto, não deve ser vista como um impeditivo para a aplicação dos resultados desta pesquisa. Um modelo em fase embrionária, como o acima proposto, é uma ferramenta exploratória que pode (e deve) ser moldado e adaptado, conforme surjam novas evidências.

6. CONCLUSÕES

A revisão de literatura empreendida identificou que existe certa dissonância metodológica entre as pesquisas científicas que abordam o controle externo das atividades de inteligência, o que dificulta a compreensão global sobre essa temática, a comparação de resultados e a criação de hipóteses. Assim, o presente trabalho almeja auxiliar no fechamento dessa lacuna, na medida em que descreve o estado da arte da produção científica na área e fornece, por meio de um modelo exploratório, uma estrutura conceitual que permite o desenvolvimento de estudos sobre o tema, teoricamente mais coesos. Dessa forma, o modelo abre caminho para a construção de trabalhos harmônicos que levem ao desenvolvimento científico desta área ainda pouco explorada.

Está claro que as novas tecnologias de vigilância são bastante invasivas e difíceis de controlar, colocando em risco a legitimidade e a própria existência das instituições democráticas (Prince et al., 2021; Zuboff, 2022). Assim, atentos a esses riscos, diversos países têm buscado estabelecer mecanismos de controle mais robustos das atividades de inteligência, o que implica realizar significativas reformas

nos já existentes. No entanto, para que isso ocorra é preciso produzir bons diagnósticos e explorar alternativas.

O modelo proposto deve auxiliar em ambas as frentes. Por um lado, o seu desenho fornece um mapa detalhado para o diagnóstico das fragilidades no controle externo das atividades de inteligência, classificando-as e indicando de que forma cada uma delas pode afetar a capacidade de controle. Por outro lado, o modelo auxilia na busca de alternativas, já que a padronização das categorias de análise facilita a realização de estudos comparados e a identificação de *benchmarks*.

6.1. Limitações teórico-metodológicas da pesquisa

Este trabalho apresenta limitações teórico-metodológicas, a seguir apresentadas. A principal delas diz respeito ao uso do constructo "capacidade de controle" como *proxy* para avaliar a eficácia do controle externo das atividades de inteligência. Embora a capacidade de controle externo (leia-se Autonomia, Poderes e Meio) seja fundamental, ela não garante, por si só, que o controle em questão seja eficaz. Fatores como independência das instituições de controle, habilidade técnica de seus membros, e vontade política para agir também são determinantes da eficácia do sistema de controle (Born et al., 2015). Além disso, embora a capacidade de controle seja uma variável estrutural muitas vezes mensurável, sua eficácia depende, entre outros, de fatores qualitativos, como o impacto das ações de controle na redução de abusos, a promoção de transparência e prestação de contas — indicadores estes que podem não ser imediatamente visíveis ou quantificáveis (Gill, 2020). Ademais, somando-se a essas limitações, pode-se dizer que mesmo com alta capacidade, instituições de controle podem ser capturadas politicamente ou se tornar ineficazes, devido a conflitos de interesse ou inação deliberada (Caparini, 2016). Assim, a capacidade de controle formal pode não refletir, necessariamente, o funcionamento real da atividade de controle externo.

Uma outra limitação teórico-metodológica desta pesquisa diz respeito ao fato de que o modelo proposto não foi testado empiricamente. Assim, modificações podem ser necessárias à sua configuração atual, quando o modelo for posto em prática. No entanto, é preciso lembrar das dificuldades associadas à pesquisa empírica acerca do controle externo de sistemas nacionais de inteligência (Gioe et al., 2020). Portanto, a testagem do modelo proposto não é iniciativa de fácil implementação.

Ademais, o artigo considerou que as três dimensões principais do modelo proposto — Autonomia, Poderes e Meio — são linearmente independentes, o que pode não ser sempre verdade, podendo haver superposição entre essas dimensões em alguns pontos da avaliação (Child & Rodrigues, 2011).

Não obstante as limitações supracitadas, recomenda-se que o modelo exploratório desenvolvido e ora apresentado seja testado e que, nesse processo, diferentes contextos sejam utilizados, mormente aqueles que não foram abarcados pela revisão de literatura empreendida — com destaque para o Sul Global. Nesse teste, seria importante avaliar a correlação existente entre distintas dimensões e variados elementos e critérios de análise. Assim, um mapa de força dessas correlações seria valioso na avaliação de potenciais estratégias de reforma institucional voltadas para o controle externo das atividades de inteligência.

6.2. Passos futuros

O modelo apresentado se baseia fortemente em literatura científica produzida em países desenvolvidos, como mostrado na Figura 4. Entretanto, o contexto socioeconômico, político e institucional dos países

exerce significativa influência sobre o controle externo das atividades de inteligência (Davison & Martinsons, 2016). De fato, o contexto nacional determina os níveis de *accountability*, transparência e eficácia dos mecanismos de supervisão das agências de inteligência, moldando a maneira como são implementados e aplicados (Caparini, 2016). Ainda assim, o procedimento metodológico adotado se justifica, já que se buscou as boas práticas associadas ao controle externo das atividades de inteligência — o que permite avaliar quão perto ou longe está o Brasil de poder, de forma eficaz, controlar, por via externa, as atividades de inteligência levadas a cabo no país. Em outras palavras, o contexto institucional não muda o modelo proposto, apenas mostra quão fácil ou difícil é controlar, eficazmente, as atividades de inteligência de um país.

Dito isso, pode-se vislumbrar vários passos futuros associados a esta pesquisa, como mostrados a seguir:

i) Testagem empírica do modelo: recomenda-se que o modelo seja testado em diferentes países, tanto em democracias consolidadas quanto em democracias emergentes, e em sistemas de controle variados (Judiciário, Parlamento, Sociedade Civil etc.). Isso ajudaria a confirmar a sua robustez, identificar possíveis ajustes necessários e fornecer dados concretos que possam aprimorar o framework.

ii) Expansão da base geográfica e contextual: embora este artigo reconheça que o modelo proposto se fundamenta em literatura associada ao contexto das democracias ocidentais, seria interessante expandir a análise para incluir mais países do Sul Global — onde os sistemas de controle e as práticas de inteligência podem ser bastante diferentes. A inclusão de países com diferentes regimes políticos e culturais pode contribuir para a criação de um modelo mais global e adaptável, permitindo que o controle das atividades de inteligência seja discutido em uma perspectiva mais inclusiva e diversa.

iii) Ampliação da discussão sobre tecnologias emergentes: o artigo discute a crescente complexidade das tecnologias envolvidas nas atividades de inteligência, como big data, IA e vigilância digital. No entanto, a análise de como a IA e outras ferramentas emergentes podem tanto ajudar quanto dificultar o controle das atividades de inteligência — por meio da automação do monitoramento ou do uso indevido de dados — poderia enriquecer a discussão teórica e prática.

iv) Aprofundamento na questão da autonomia do controlador: o modelo proposto destaca a importância da autonomia do controlador, mas essa dimensão poderia ser futuramente mais explorada, em termos de estratégias específicas para garantir a independência dos órgãos de controle. Além de explorar o papel do Judiciário e do Parlamento, trabalhos futuros poderiam discutir como as relações entre os controladores e os controlados podem ser estruturadas para evitar conflitos de interesse.

v) Desenvolvimento de indicadores operacionalizáveis: a criação de um conjunto de indicadores operacionais ajudaria a transformar o modelo em uma ferramenta prática para pesquisadores, tomadores de decisão e organizações da sociedade civil, objetivando avaliar a eficácia do controle externo das atividades de inteligência.

vi) Interação com a sociedade civil e transparência: o modelo poderia, em trabalhos futuros, ser aprimorado, ao discutir em maior profundidade o papel da sociedade civil no controle

das atividades de inteligência. O uso de canais de denúncia, o monitoramento por ONGs e a transparência por meio da mídia são elementos importantes que podem complementar o controle institucional.

vii) Considerações éticas e de direitos humanos: discutir as implicações éticas do uso de dados pessoais e de práticas invasivas de monitoramento seria uma adição importante a este trabalho, pois as atividades de inteligência frequentemente esbarram em questões delicadas de privacidade e liberdades individuais.

viii) Reflexão crítica sobre o papel do governo: artigos futuros poderiam desenvolver uma reflexão mais crítica sobre o papel do governo no controle das atividades de inteligência. Em muitas democracias, o governo pode ter interesse direto em restringir a transparência ou evitar investigações que possam comprometer sua imagem ou suas políticas.

ix) Submissão a especialistas: o modelo desenvolvido poderia, futuramente, ser submetido ao crivo de especialistas da área de inteligência. Para tal, o uso da abordagem Delphi poderia representar um avanço em termos de validade dos resultados aqui obtidos — especialmente se for possível identificar outros critérios também relevantes para um eficaz controle externo das atividades de inteligência em um país.

Por fim, não obstante os inúmeros passos futuros aqui propostos, espera-se que o estudo apresentado e o modelo proposto possam ser úteis a acadêmicos, praticantes e formuladores de políticas públicas na compreensão e discussão do controle externo das atividades de inteligência, do papel das tecnologias digitais emergentes nesse processo e de todas as implicações daí decorrentes.

REFERÊNCIAS

Abuza, Z. (2016). *Forging peace in Southeast Asia: Insurgencies, peace processes, and reconciliation*. Rowman & Littlefield.

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security*, *132*, 103352. https://doi.org/10.1016/j.cose.2023.103352

American Civil Liberties Union. (2013). *The global principles on national security and the right to information (Tshwane principles)*. Open Society Foundations. https://www.aclu.org/documents/global-principles-national-security-and-right-information-tshwane-principles

Bajpai, D. (2017). The collection without permission: WhatsApp's data sharing policy. *Supremo Amicus, 2*(1), 139. https://heinonline.org/HOL/LandingPage?handle=hein.journals/supami2&div=19

Banisar, D. (2006). The right to information in the age of information. In R. F. Jørgensen (Ed.). *Human rights in the global information society* (pp. 77–89). MIT Press. https://doi.org/10.7551/mitpress/3606.003.0005

Baumeister, R. F., & Leary, M. R. (1997). Writing narrative literature reviews. *Review of General Psychology, 1*(3), 311–320. https://doi.org/10.1037/1089-2680.1.3.311

Berman, E. (2022). Reimagining surveillance law. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4161996

Bihar, A. M. (2020). Uruguay's attempt at intelligence oversight. *International Journal of Intelligence and CounterIntelligence, 33*(2), 214–247. https://doi.org/10.1080/08850607.2019.1663701

Bloch-Wehba, H. (2021). Visible policing: technology, transparency, and democratic control. *California Law Review*, 109(3), 917–978. https://doi.org/10.15779/Z38NSOKZ51

Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. *Security Studies, 26*(3), 452–481. https://doi.org/10.1080/09636412.2017.1306396

Born, H., Johnson, L. K., & Leigh, I. (2005). *Who's watching the spies? Establishing intelligence service accountability*. Potomac Books.

Born, H., Leigh, I., & Wills, A. (2015). *Making international intelligence cooperation accountable*. Printing Office of the Parliament of Norway.

Born, H., & Wetzling, T. (2007). Intelligence accountability: challenges for parliaments and intelligence services. In *Handbook of intelligence studies* (pp. 315–328). Routledge.

Born, H., & Wills, A. (2012). *Overseeing intelligence services: A toolkit*. DCAF.

Brantly, A. F. (2020). When everything becomes intelligence: machine learning and the connected world. In *Developing Intelligence Theory* (pp. 96-107). Routledge.

Broeders, D., Boeke, S., & Georgieva, I. (2019). *Foreign intelligence in the digital age: Navigating a state of "Unpeace"*. SSRN. https://papers.ssrn.com/abstract=3493612

Cahane, A. (2020). Who will watch the watchmen? Oversight of online surveillance in Israel. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3819815

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

Caparini, M. (2007). Domestic regulation: Licensing regimes for the export of military goods and services. In S. Chesterman & C. Lehnardt (Eds.). *From mercenaries to market: the rise and regulation of private military companies* (pp. 158–178). Oxford. https://doi.org/10.1093/acprof:oso/9780199228485.003.0010

Caparini, M. (2016). Controlling and overseeing intelligence services in democratic states. In H. Born & M. Caparini (Eds.), *Democratic control of intelligence services* (pp. 3–24). Routledge. https://doi.org/10.4324/9781315576442

Caparini, M., & Cole, E. (2008). The case for public oversight of the security sector: Concepts and strategies. In *Public oversight of the security sector: A handbook for civil society organizations* (pp. 11–30). DCAF.

Cayford, M., Pieters, W., & Hijzen, C. (2018). Plots, murders, and money: Oversight bodies evaluating the effectiveness of surveillance technology. *Intelligence*

and National Security, 33(7), 999–1021. https://doi.org/10.1080/02684527.2018.1487159

Cepik, M. (2003). Sistemas nacionais de inteligência: origens, lógica de expansão e configuração atual. *Dados, 46*, 75–127. https://doi.org/10.1590/S0011-52582003000100003

Chadegani, A. A., Salehi, H., Yunus, M. M., Farhadi, H., Fooladi, M., Farhadi, M., & Ale Ebrahim, N. (2013). A comparison between two main academic literature collections: Web of Science and Scopus databases. *Asian Social Science*, *9*(5), 18–26. https://doi.org/10.48550/arXiv.1305.0377

Chesterman, S. (2008). We can't spy... if we can't buy!: The privatization of intelligence and the limits of outsourcing "inherently governmental functions". *European Journal of International Law, 19*(5), 10551074. https://doi.org/10.1093/ejil/chn055

Chesterman, S. (2021). *We, the robots?* Cambridge University Press. https://doi.org/10.1017/9781009047081

Child, J., & Rodrigues, S. B. (2011). How Organizations Engage with External Complexity: A Political Action Perspective. *Organization Studies*, 32(6), 803–824. https://doi.org/10.1177/0170840611410825

Cordero, C., Fellow, R. M. G. S. (2019). *Working paper : Enhancing congressional intelligence committee effectiveness*. Center for a New American Security. https://doi.org/10.2139/ssrn.3454315

Davison, R. M., & Martinsons, M. G. (2016). Context is king! Considering particularism in research design and reporting. *Journal of Information Technology, 31*, 241–249. https://doi.org/10.1057/jit.2015.19

Defty, A. (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

Defty, A. (2022). 'Familiar but not intimate': executive oversight of the UK intelligence and security agencies. Intelligence and National Security, 37(1), 57–72. https://doi.org/10.1080/02684527.2021.1959697

Dobson, M. J. (2019). The last forum of accountability? State secrecy, intelligence and freedom of information in the United Kingdom. *The British Journal of Politics and International Relations, 21*(2), 312–329. https://doi.org/10.1177/1369148118806125

Duroy, S. (2022). State compliance with international law in intelligence matters: A behavioral approach. *Journal of International Dispute Settlement, 13*(2), 233–263. https://doi.org/10.1093/jnlids/idab029

Ebell, C., Baeza-Yates, R., Benjamins, R., Cai, H., Coeckelbergh, M., Duarte, T., Hickok, M., Jacquet, A., Kim, A., Krijger, J., MacIntyre, J., Madhamshettiwar, P., Maffeo, L., Matthews, J., Medsker, L., Smith, P., & Thais, S. (2021). Towards intellectual freedom in an AI Ethics Global Community. *AI and Ethics*, *1*, 131–138. https://doi.org/10.1007/s43681-021-00052-5

Ferrari, R. (2015). Writing narrative style literature reviews. *Medical Writing, 24*(4), 230–235. https://doi.org/10.1179/2047480615Z.000000000329

Firmo, M. R. (2022). Limites éticos da atividade de inteligência. *Revista Ciência & Polícia, 8*(2), 36–50. https://doi.org/10.59633/2316-8765.2022.252

Gill, P. (2007). Evaluating intelligence oversight committees: The UK Intelligence and Security Committee and the 'war on terror'. *Intelligence and National Security*, 22(1), 14–37. http://dx.doi.org/10.1080/02684520701200756

Gill, P. (2012). *Policing politics: security intelligence and the liberal democratic state*. Routledge. https://doi.org/10.4324/9780203043776

Gill, P. (2016). *Intelligence governance and democratisation: A comparative analysis of the limits of reform*. Routledge.

Gill, P. (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, P. (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

Gill, P., & Phythian, M. (2013). *Intelligence in an insecure world* (2nd ed.). Wiley.

Gill, P., & Phythian, M. (2018). Developing intelligence theory. *Intelligence and National Security*, *33*(4), 467–471. https://doi.org/10.1080/02684527.2018.1457752

Gioe, D. V., Goodman, M. S., & Stevens, T. (2020). Intelligence in the cyber era: Evolution or revolution? *Political Science Quarterly, 135*(2), 191–224. https://doi.org/10.1002/polq.13031

Gogolewska, A. (2021). Transformation of state security and intelligence services in Poland — A job still unfinished. *Connections: The Quarterly Journal, 20*(1), 9–32. https://doi.org/10.11610/Connections.20.1.01

Gonçalves, J. B. (2010). Quem vigia os vigilantes? O controle da atividade de inteligência no Brasil e o papel do Poder Legislativo. *Revista de Informação Legislativa, 47*(187), 125–136. http://www2.senado.leg.br/bdsf/handle/id/496919

Gonçalves, J. B. (2017). *Atividade de inteligência e legislação correlata* (5th ed.). Impetus.

Gonçalves, J. B. (2019). *Políticos e espiões: O controle da atividade de inteligência* (2nd ed.). Impetus.

Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal, 26*(2), 91–108. https://doi.org/10.1111/j.1471-1842.2009.00848.x

Green, B. N., Johnson, C. D., & Adams, A. (2006). Writing narrative literature reviews for peer-reviewed journals: Secrets of the trade. *Journal of Chiropractic Medicine, 5*(3), 101–117. https://doi.org/10.1016/S0899-3467(07)60142-6

Hegemann, H. (2018). Toward 'normal' politics? Security, parliaments and the politicisation of intelligence oversight in the German Bundestag. *The British Journal of Politics and International Relations*, 20(1), 175–190. https://doi.org/10.1177/1369148117745683

Herman, M. (1996). *Intelligence power in peace and war*. Cambridge University Press. https://doi.org/10.1017/CBO9780511521737

Hillebrand, C. (2012). The role of news media in intelligence oversight. In R. Dover, H. Dylan, & M. S. Goodman (Eds.). A Decade of Intelligence Beyond 9/11: Security, Diplomacy and Human Rights (pp. 689-706). *Intelligence and National Security, 27*(5). https://doi.org/10.1080/02684527.2012.708521

Hillebrand, C. (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

Junior, É., & de Quadros, D. (2021). A constituição como limite para o ativismo do Judiciário. *Revista Brasileira de Teoria Constitucional*, 7(2), 73–88. https://doi.org/10.26668/IndexLawJournals/2525-961X/2021.v7i2.8274

Keane, J. (2009). *The life and death of democracy*. W. W. Norton & Company.

Khan, A., Imam, I., & Azam, A. (2021). Role of Artificial Intelligence in Defence Strategy. *Strategic Studies*, *41*(1), 19–40. https://doi.org/10.53532/ss.041.01.0058

Kinyondo, A., Pelizzo, R., & Umar, A. (2015). A functionalist theory of oversight. *African Politics & Policy, 1*(5), 1–25. https://www.researchgate.net/profile/Riccardo-Pelizzo-2/publication/292227902_A_Functionalist_Theory_of_Oversight/links/56ac376808ae19a385116801/A-Functionalist-Theory-of-Oversight.pdf

Kirchgaessner, S., Cutler, S., Pegg, D., & Sabbagh, D. (2021, July 18). *Revealed: Leak uncovers global abuse of cyber-surveillance weapon*. The Guardian. https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

Klöckner, C. (2023). *A capacidade de controle externo das atividades de inteligência na era digital* [Dissertação de mestrado]. Fundação Getulio Vargas. https://repositorio.fgv.br/items/af86cd33-d297-4465-8d12-4a27634e4899

Kniep, R., Ewert, L., Reyes, B. L., Tréguer, F., Mc Cluskey, E., & Aradau, C. (2024). Towards democratic intelligence oversight: Limits, practices, struggles. *Review of International Studies*, *50*(1), 209–229. https://doi.org/10.1017/S0260210523000013

Korff, D., Brown, I., & Wright, J. (2017). *Boundaries of law: Exploring transparency, accountability, and oversight of government surveillance regimes*. Cambridge Legal Studies Research. https://papers.ssrn.com/abstract=2894490

Krause, G., Lewis, D., & Douglas, J. (2006). Political Appointments, Civil Service Systems, and Bureaucratic Competence: Organizational Balancing and Executive Branch Revenue Forecasts

in the American States. *American Journal of Political Science*, 50(3), 770–787. http://www.jstor.org/stable/3694248

Krivokapić, Đ., Krivokapić, D., Adamović, J., & Stefanović, A. (2021). Comparative analysis of video surveillance regulation in data protection laws in the former Yugoslav states. *Journal of Regional Security, 16*(1), 5-26. https://doi.org/10.5937/jrs16-27170

Langley, A. (1999). Strategies for theorizing from process data. *Academy of Management Review, 24*(4), 691–710. https://doi.org/10.2307/259349

Leigh, I., & Wegge, N. (2018). Intelligence and oversight at the outset of the twenty-first century. In *Intelligence Oversight in the Twenty-First Century* (pp. 7–24). Routledge. https://doi.org/10.4324/9781351188791

Lester, G. (2015). *When should state secrets stay secret?: accountability, democratic governance, and intelligence*. Cambridge University Press. https://doi.org/10.1017/CBO9781107337015

Lester, G., & Rogg, J. (2018). Intelligence and oversight. In I. Leigh & N. Wegge. *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World*. Routledge.

Li, Z. (2024). Ethical frontiers in artificial intelligence: navigating the complexities of bias, privacy, and accountability. *International Journal of Engineering and Management Research*, *14*(3), 109–116. https://doi.org/10.5281/zenodo.12792741

Lopes, A., & Vieira, D. (2023). Between politics and bureaucracy: a systematic literature review on the dynamics of public appointments. *International Journal of Public Sector Management*, 36(2), 152–170. https://doi.org/10.1108/IJPSM-09-2022-0200

Lowenstein, K. (1979). *Teoría de la Constitución* (2nd ed.). Ariel.

Matei, F. C., & Bruneau, T. (2011). Intelligence reform in new democracies: Factors supporting or arresting progress. *Democratization, 18*(3), 602–630. http://dx.doi.org/10.1080/13510347.2011.586257

Matias-Pereira, J. (2022). Governance in the public sector: Emphasis on better management, transparency and society participation. *Brazilian Journal of Development, 8*(9), 63172–63195. https://doi.org/10.34117/bjdv8n9-183

Mayer, J. (2018). Government hacking. *Yale Law Journal, 127*(3), 490–787. https://www.yalelawjournal.org/article/government-hacking

Meirelles, H. L. (2015). *Direito administrativo brasileiro* (42a ed.). Malheiros.

Mershon, C., & Shvetsova, O. (2019). *Formal modeling in social science*. University of Michigan Press.

Minayo, M. C. S. (2017). Amostragem e saturação em pesquisa qualitativa: Consensos e controvérsias. *Revista Pesquisa Qualitativa, 5*(7), 1–12. https://editora.sepq.org.br/rpq/article/view/82

Mongeon, P., & Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: A comparative analysis. *Scientometrics, 106*, 213–228. https://doi.org/10.1007/s11192-015-1765-5

Montasari, R. (2023). Internet of things and artificial intelligence in national security: Applications and issues. In *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity* (pp. 27–56). Springer International Publishing. https://doi.org/10.1007/978-3-031-21920-7_3

Moses, L. (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

Muchwa, A. S. (2021). Intelligence oversight systems in Uganda: Challenges and prospects. *Intelligence and National Security, 36*(5), 696–708. https://doi.org/10.1080/02684527.2021.1888201

Obuobi, P. P. (2018). Evaluating Ghana's intelligence oversight regime. *International Journal of Intelligence and CounterIntelligence, 31*(2), 312–341. https://doi.org/10.1080/08850607.2017.1375841

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1954824

Parsons, C. A. (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

Pătrașcu, P. (2021). Emerging technologies and national security: The impact of IoT in critical infrastructures protection and defence sector. *Land Forces Academy Review*, *26*(4), 423–429. https://doi.org/10.2478/raft-2021-0055

Paul, J., & Criado, A. R. (2020). The art of writing literature review: What do we know and what do we need to know? *International Business Review, 29*(4), 101717. https://doi.org/10.1016/j.ibusrev.2020.101717

Pelizzo, R., & Stapenhurst, F. (2012). *Parliamentary oversight tools: A comparative analysis*. Routledge.

Phythian, M., Gill, P., & Marrin, S. (2008). *Intelligence theory: Key questions and debates*. Routledge.

Pires, F. M., & Andrade, A. L. (2022). Career choices: Adaptation and initial evidence of the Work Volition Scale in Brazil. *Brazilian Business Review, 19*(2), 153–170. https://doi.org/10.15728/bbr.2021.19.2.3

Polido, F. B. P. (2024). Estado, soberania digital e tecnologias emergentes: interações entre direito internacional, segurança cibernética e inteligência artificial. *Revista de Ciências do Estado*, *9*(1), 1–30. https://doi.org/10.35699/2525-8036.2024.53066

Post, C., Sarala, R., Gatrell, C., & Prescott, J. E. (2020). Advancing theory with review articles. *Journal of Management Studies, 57*(2), 351–376. https://doi.org/10.1111/joms.12549

Prince, C., Saxunová, D., & Hanson, L. (2021). Are we living in surveillance societies and is privacy an illusion? An empirical study on privacy literacy and privacy concerns. *IEEE Transactions on Engineering Management, 70*(10), 3553–3570. https://doi.org/10.1109/TEM.2021.3092702

Ribeiro, M. M. (2023). *A atividade de Inteligência de Estado brasileira está em xeque com a promulgação da Emenda Constitucional n. 115/2022?* [Dissertação de mestrado]. Universidade de Brasília.

Roberts, T., Ali, A. M., Farahat, M., Oloyede, R., & Mutung'u, G. (2021). Surveillance Law in Africa: a review of six countries. *Brighton: Institute of Development Studies*. https://doi.org/10.19088/IDS.2021.059

Shoemaker, P., Tankard Jr, J., & Lasorsa, D. (2003). *How to build social science theories*. Sage publications.

Siddaway, A. P., Wood, A. M., & Hedges, L. V. (2019). How to do a systematic review: A best practice guide for conducting and reporting narrative reviews, meta-analyses, and meta-syntheses. *Annual Review of Psychology, 70*(1), 747–770. https://doi.org/10.1146/annurev-psych-010418-102803

Snowden, E. (2019). *Eterna vigilância: Como montei e desvendei o maior sistema de espionagem do mundo*. Planeta.

Theile, C. M., & Beall, A. L. (2024). Narrative reviews of the literature: An overview. *Journal of Dental Hygiene, 98*(1), 1–10. https://jdh.adha.org/content/98/2/51

Thiry-Cherques, H. R. (2009). Saturação em pesquisa qualitativa: estimativa empírica de dimensionamento. *Revista PMKT*, 3(2), 20–27.

União Europeia. (2023). *Relatório A9-0189/2023*. Parlamento Europeu. https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_PT.html

Van Brakel, R. (2021). How to watch the watchers? Democratic oversight of algorithmic police surveillance in Belgium. *Surveillance & Society, 19*(2), 228–240. https://doi.org/10.24908/ss.v19i2.14325

Veletsianos, G., & Shepherson, P. (2016). A systematic analysis and synthesis of the empirical MOOC literature published in 2013-2015. *International Review of Research in Open and Distributed Learning, 17*(2), 198–221. https://doi.org/10.19173/irrodl.v17i2.2448

Vieth, K., & Wetzling, T. (2020). Data-driven intelligence oversight: Recommendations for a system update. *SSRN Electronic Journal*. https://dx.doi.org/10.2139/ssrn.3505906

Walsh, P. F. (2022). Australian intelligence oversight and accountability: Efficacy and contemporary challenges. *Intelligence and National Security, 37*(7), 968–984. https://doi.org/10.1080/02684527.2022.2095602

Wegge, N. (2017). Intelligence Oversight and the Security of the State. *International Journal of Intelligence and CounterIntelligence*, *30*(4), 687–700. https://doi.org/10.1080/08850607.2017.1337445

Weinstein, J. M., Moore, R. J., & Silverman, N. P. (2017). Balancing privacy and public safety in the post-Snowden era. In D. Gray & R. Henderson

(Eds.). *The Cambridge handbook of surveillance law* (pp. 227–247). Cambridge University Press. https://doi.org/10.1017/9781316481127

Wills, A., & Vermeulen, M. (2011). *Parliamentary oversight of security and intelligence agencies in the EU*. European Parliament.

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. M. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems, 22*(1), 45–55. https://doi.org/10.1057/ejis.2011.51

Xu, X. (2021). To Repress or to Co-opt? Authoritarian Control in the Age of Digital Surveillance. *American Journal of Political Science*, *65*(2), 309–325. https://doi.org/10.1111/ajps.12514

Young, M., Katell, M., & Krafft, P. M. (2019). Municipal surveillance regulation and algorithmic accountability. *Big Data & Society, 6*(2), 205395171986849. https://doi.org/10.1177/2053951719868492

Zairi, M. (2010). *Benchmarking for best practice*. Routledge.

Zuboff, S. (2019). Surveillance capitalism and the challenge of collective action. In *New labor forum, 28*(1), 10–29. Sage Publications. https://doi.org/10.1177/1095796018819461

Zuboff, S. (2020). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* PublicAffairs.

Zuboff, S. (2022). Surveillance capitalism or democracy? The death match of institutional orders and the politics of knowledge in our information civilization. *Organization Theory, 3*(3), 26317877221129290. https://doi.org/10.1177/26317877221129290

Conrado Klöckner

Mestre em Administração pela Escola Brasileira de Administração Pública e de Empresas da Fundação Getulio Vargas (FGV EBAPE); Coordenador-geral de bancada na Assembleia Legislativa do Rio Grande do Sul. E-mail: conradoklockner@gmail.com

Luiz Antonio Joia

Professor titular da Escola Brasileira de Administração Pública e de Empresas da Fundação Getulio Vargas (FGV EBAPE). E-mail: luiz.joia@fgv.br

CONTRIBUIÇÃO DOS AUTORES

Conrado Klöckner: Conceituação (Liderança); Curadoria de dados (Liderança); Análise formal (Liderança); Aquisição de financiamento (Liderança); Investigação (Liderança); Metodologia (Liderança); Administração de projeto (Igual); Recursos (Liderança); Software (Liderança); Supervisão (Suporte); Validação (Igual); Visualização (Igual); Escrita – rascunho original (Liderança) Escrita – revisão e edição (Suporte).

Luiz Antonio Joia: Conceituação (Suporte); Curadoria de dados (Suporte); Análise formal (Suporte); Aquisição de financiamento (Suporte); Investigação (Suporte); Metodologia (Suporte); Administração de projeto (Igual); Recursos (Suporte); Software (Suporte); Supervisão (Liderança); Validação (Igual); Visualização (Igual); Escrita - rascunho original (Suporte) Escrita - revisão e edição (Liderança).

DISPONIBILIDADE DE DADOS

Todo o conjunto de dados que dá suporte aos resultados deste estudo foi disponibilizado no FGV Sistema de Bibliotecas e pode ser acessado em:
https://repositorio.fgv.br/items/af86cd33-d297-4465-8d12-4a27634e4899

FINANCIAMENTO

Esta pesquisa foi financiada pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), processo número 304290/2021-1 (L.A.J.) e Escola Brasileira de Administração Pública e de Empresas da Fundação Getulio Vargas (FGV EBAPE), processo número PROPESQUISA 00505100300360 (L.A.J.).