

PENSE NISSO, ANTES DE AGIR: UMA ANÁLISE COMPARATIVA ENTRE OS SERVIÇOS DE INTELIGÊNCIA BRASILEIRO, COLOMBIANO E BRITÂNICO (2022–2024)

PRIOR TO ACTING, CONSIDER IT: A COMPARATIVE ANALYSIS BETWEEN BRAZILIAN, COLOMBIAN, AND BRITISH INTELLIGENCE SERVICES (2022–2024)

FERNANDO HENRIQUE CASALUNGA

RESUMO

Com o intuito de verificar como a inteligência pode contribuir com a formulação de estratégias que favoreçam os interesses nacionais de cada um deles, este artigo apresenta uma análise comparativa entre as principais instituições e sistemas responsáveis pelo setor no Brasil, na Colômbia e no Reino Unido. A análise comparativa permite um exame apurado sobre como diferentes Estados abordam os desafios securitários contemporâneos. Porquanto, com o objetivo de identificar os mecanismos que facilitam a atuação assertiva no desempenho de suas atividades, o modelo proposto considera alguns fatores-chave como elementos cruciais para robustecer as operações e a fiúza pública de suas principais agências. Assim, procuro compreender diferenças e similitudes, destacando as intersecções e divergências inerentes a cada uma delas.

PALAVRAS-CHAVE: Ameaças; Ética; Integração Interagências; Inteligência; Técnico-Científico.

ABSTRACT

The main intelligence sector organizations of Brazil, Colombia, and the UK are compared in this article to see how they could aid in the creation of policies that further the goals of each nation. The comparative study allows for a detailed examination of how they address contemporary security concerns. Consequently, the proposed model considers a few key factors as crucial elements to improve the functioning and public trust of their agencies in order to identify the processes that boost the effectiveness of their operations. With a focus on the points of convergence and divergence founded, I seek to understand both parallels and distinctions among each of them.

KEYWORDS: Threats; Ethics; Interagency Integration; Intelligence; Technology.

O AUTOR

Doutor em Ciência Política (UFRGS/2024), Mestre em Ciência Política (UFPE/2020), Bacharel em Ciência Política com ênfase em Relações Internacionais (UFPE/2019), Bacharel e Licenciado em História (UNESP/2010). Realizou instância de investigação doutoral no Instituto Universitário de Lisboa (Portugal). Membro da Associação Brasileira de Estudos de Defesa, Associação Brasileira de Ciência Política e dos grupos de pesquisa do CNPq ‘O Brasil e as Américas’ e ‘Segurança e Política Internacional’. Pesquisador do Núcleo de Estudos Prospectivos do Centro de Estudos Estratégicos do Exército (NEP - CEEEx) no ciclo 2024-2025.



1 INTRODUÇÃO

O presente artigo é o quarto de uma série de cinco produtos que serão desenvolvidos pela linha de pesquisa ‘Inteligência’ do Centro de Estudos Estratégicos do Exército (CEEEx), no âmbito do Núcleo de Estudos Prospectivos (NEP) até 2025¹.

Partindo do pressuposto registrado nos três ensaios apresentados e discutidos no âmbito do Núcleo², nos quais se reforça a significância da atividade de inteligência para a formulação de políticas, estratégias, e planos de segurança mais eficazes, este artigo apresenta uma comparação entre estruturas responsáveis pelo setor no Brasil, Colômbia e Reino Unido.

Dentre as unidades de análise considera-se, no Brasil, a Agencia Brasileira de Inteligência (ABIN) e a Assessoria de Inteligência de Defesa (AIDef) que operam, respectivamente, sob o Ministério da Casa Civil e o comando do Estado-Maior Conjunto das Forças Armadas (EMCFA); na Colômbia, a Direção Nacional de Inteligência (DNI) que opera em estreita relação com agências civis no enfrentamento de ameaças internas associadas ao narcotráfico e à insurgência; e, no Reino Unido, as agências GCHQ, MI5 e MI6 subordinadas ao Gabinete do Primeiro-Ministro britânico.

Ao lançar luz sobre o interesse institucional pelo desenvolvimento de capacidades que permitam confrontar o problema das ameaças securitárias contemporâneas, em particular, das ilícitudes atribuídas ao terrorismo e/ou crime organizado, proponho explorar o argumento de que a eficácia das agências supracitadas depende da combinação adequada de fatores-chave como estrutura organizacional, desenvolvimento técnico-científico, conduta ética, e integração interagências. De tal, a hipótese aventada afirma que as unidades de análise promotoras de uma colaboração fluida e respeitosa, tendem a produzir informações mais relevantes e acionáveis, impactando positivamente o planejamento estratégico.

Logo, a fim de verificar a sua plausibilidade, este artigo aborda não apenas as suas idiossincrasias organizacionais e/ou capacitárias, mas também os mecanismos que permitem a formulação e implementação de estratégias mais eficazes. Dessarte, se acha dividido em três seções que destacam: i) o funcionamento das principais estruturas e sistemas responsáveis pela inteligência no Brasil, Reino Unido e Colômbia, ii) apresenta uma análise comparativa entre elas; iii) discute o seu papel no planejamento estratégico. Por fim, uma breve conclusão sumariza os resultados obtidos pela linha de pesquisa.

2 A INTELIGÊNCIA NO BRASIL, COLÔMBIA, E REINO UNIDO

Nesta seção apresento, brevemente, as estratégias de Brasil, Colômbia, e Reino Unido para lidar com desafios securitários contemporâneos, acentuando aspectos normativos que estruturam e regulam as atividades de suas principais instituições de inteligência.

Sem embargo, no Brasil, a Constituição Federal de 1988, estabelece que o Conselho de Defesa Nacional (CDN) é o órgão responsável por assuntos relacionados à soberania nacional e à defesa do regime democrático (Brasil, 2023a), primazia refletida na Política Nacional de Defesa (PND) que

¹ Os achados e resultados dos produtos desenvolvidos ao longo deste ciclo servirão de base para a construção de um *Policy Paper* que deverá indicar implicações e recomendações ao Exército brasileiro.

² Os ensaios podem ser consultados no sítio eletrônico do Centro de Estudos Estratégicos do Exército (CEEEx). Disponível em: <https://ebrevistas.eb.mil.br/CEEExAE/issue/archive>.

orienta o planejamento das ações.

A estratégia brasileira destaca a importância de uma gestão eficaz da inteligência como fator essencial para apoiar as decisões e promover os interesses nacionais (Brasil, 2020). Por conseguinte, o foco do setor repousa sobre o controle de ameaças e a identificação de oportunidades, buscando atuar de modo assertivo frente aquelas associadas à espionagem, sabotagem, interferência externa, ataques cibernéticos, terrorismo, exfiltração de propriedade intelectual, corrupção e atentados contra a ordem democrática (Brasil, 2016).

Ante a demanda, fontes oficiais destacam a competência do setor em produzir e disseminar conhecimento às autoridades competentes sobre fatos e situações que possam impactar processos decisórios e a segurança do Estado³. Nesse ensejo, sublinham a significância estratégica do Sistema Brasileiro de Inteligência (SISBIN), centro que concatena esforços interagências para defender os interesses do Estado e da sociedade brasileira (Brasil, 2016; 2017)⁴.

A Agência Brasileira de Inteligência (ABIN) representa o órgão civil central deste Sistema, responsável por planejar, executar e coordenar as atividades de inteligência nacional. Sob a Doutrina da Atividade de Inteligência (DAI), monitora grupos envolvidos em atividades ilícitas, buscando neutralizar ações que possam desestabilizar a segurança política, econômica e social⁵. Suas principais atribuições incluem a coleta e análise de informações, proteção de propriedade intelectual e dados sigilosos, avaliação de ameaças ao regime democrático, além da cooperação com estruturas e órgãos de segurança internacionais sempre que necessária (Brasil, 2023b).

A atuação da ABIN se orienta pelo zelo ao bem público, avaliando potenciais impactos sociais e mantendo o compromisso com a produção de informações imparciais e empiricamente verificáveis. Em contrapartida, o controle das atividades é realizado pelos três poderes da República⁶. Ademais, a instituição exige de seus agentes a incorporação de valores éticos como pilares de conduta pessoal (Brasil, 2023b).

No tocante à esfera militar, o SISBIN opera em acordo com as diretrizes do Ministério da Defesa (MD) que orientam as atividades do setor. Dentre as principais estruturas destacam-se: o Sistema de Inteligência de Defesa (SINDE), subordinado ao MD, que por intermédio da Assessoria de Inteligência de Defesa (AIDef) atende ao Estado-Maior Conjunto das Forças Armadas⁷.

³ Documentos basilares que orientam as atividades do setor reforçam o papel da inteligência no monitoramento da conjuntura geopolítica, proteção de infraestruturas críticas e conhecimentos sensíveis, e promoção de uma contra-inteligência efetiva (Brasil, 2016). Ademais, enfatizam a importância das atividades especializadas de produção e disseminação de informações para o planejamento e avaliação das políticas de Estado, reforçando o papel central do sistema de inteligência na orientação dos processos decisórios (Brasil, 2017).

⁴ Criado em 1999, o SISBIN foi idealizado para concatenar esforços de planejamento e execução das competências relativas à inteligência, representa o centro da engenharia institucional responsável por prover informações significativas que ofereçam suporte aos processos decisórios capitaneados pelos líderes civis e/ou militares. Sua funcionalidade é marcada pela capacidade de agregar interesses de diversas instituições, fator que tem efeito positivo sobre a eficácia das atividades de inteligência ao passo em que promove ações conjuntas (Brasil, 2016; 2017).

⁵ A DAI estabelece três regras fundamentais para guiar suas operações: adequabilidade dos meios, escolha apropriada das técnicas e proporcionalidade no uso dos recursos, assegurando que os métodos respeitem os limites legais e a integridade das atividades sigilosas (Brasil, 2023b, p. 29-30).

⁶ Para garantir transparência e legalidade no Legislativo, a Comissão Mista de Controle da Atividade de Inteligência (CCAI), juntamente com o Tribunal de Contas da União (TCU), supervisionam suas atividades; no Executivo, a Câmara de Relações Exteriores e Defesa Nacional, e a Controladoria Geral da União (CGU), acompanham a execução da Política Nacional de Inteligência monitorando os recursos empregados (Brasil, 2017, p. 10).

⁷ O Sistema de Inteligência do Exército (SIEx) faz parte do SINDE e tem como órgão central o Centro de Inteligência do Exército (CIE), sendo estas estruturas responsáveis pelas atividades de inteligência voltadas à defesa de infraestruturas críticas e apoio ao planejamento de ações terrestres.

A defesa considera essencial o aprimoramento das capacidades do SINDE para antecipar cenários adversos e garantir que o Estado esteja preparado para lidar com ameaças complexas no ambiente estratégico. Por esse prisma, aspectos como neutralidade ideológica e objetividade analítica informacional são percebidos como elementos chave (Brasil, 2023c).

Não obstante, na Colômbia, o Plano Nacional de Desenvolvimento 2022-2026 (PND) aponta para o controle institucional e a defesa do território como elementos fundamentais para assegurar a segurança humana e a justiça social⁸. À conta disso, os colombianos priorizam o desenvolvimento sustentável e a proteção ambiental, refletindo uma visão integrada que busca ir além da segurança física tradicional, visando combater organizações criminosas em áreas estratégicas⁹.

O PND prioriza três objetivos fundamentais, a organização do território em torno da água; transformação das estruturas produtivas em direção a economias sustentáveis; e a promoção da equidade e inclusão, que devem ser perseguidos por meio da exploração sustentável de riquezas naturais e da construção de laços entre os setores público e privado. Através da construção de incentivos ao desenvolvimento e redução de desigualdades, as lideranças buscam restaurar a confiança dos cidadãos nas instituições, reafirmando o papel do Estado como promotor do bem-estar e da paz (Colômbia, 2023a).

No tocante à defesa, a Constituição Política da Colômbia de 1991, estabelece o zelo pela soberania, independência, integridade territorial, e a ordem constitucional como missão fundamental das Forças Armadas. Por conseguinte, sua competência para proteger os interesses nacionais contra ameaças internas e externas, sejam estas convencionais ou não, se estende por todos os domínios (Colômbia, 2022).

Neste ensejo, a noção de segurança é compreendida como a percepção de ausência de ameaças que comprometam a existência, propriedade e interesses de um Estado e seus cidadãos¹⁰. Daí, definem o conceito de ameaça como um fenômeno que representa risco aos interesses nacionais e aos propósitos estratégicos do Estado, podendo gerar danos significativos à vida, propriedade, infraestrutura e recursos naturais, dependendo de sua gravidade (Colômbia, 2022)¹¹.

A estrutura de inteligência colombiana é complexa e reflete os desafios de segurança e desenvolvimento enfrentados pelo Estado¹². Em específico, a Direção Nacional de Inteligência

⁸ Este documento foi elaborado a partir de diálogos regionais com diversas comunidades e setores, visando consolidar propostas que fortaleçam o papel do Estado como garantidor de oportunidades de desenvolvimento. Ele propõe a formulação de políticas públicas para enfrentar injustiças históricas e promover transformações nas estruturas produtivas, adequando-as às demandas contemporâneas de integração e proteção socioambiental (Colômbia, 2023a).

⁹ As instituições civis e militares devem promover a noção de segurança humana e o desenvolvimento de capacidades que permitam lidar com ameaças domésticas e/ou transnacionais. Por essa lógica, o conceito de segurança ultrapassa a mera ausência de conflitos armados, englobando também aspectos de violência indireta, como desastres naturais e necessidades sociais básicas (Colômbia, 2023a; 2023b).

¹⁰ A segurança deve ser encarada como um estado no qual a nação se protege contra destruição ou agressão estrangeira, enquanto a defesa é o instrumento que garante a preservação das estruturas políticas, jurídicas e econômicas do Estado, protegendo seu território, população e soberania (Buchan & Mackintosh, 1975, *apud* Colômbia, 2022).

¹¹ Classificados entre Grupos Armados Organizados (GAO) transnacionais, e Grupos Armados Organizados Regionais (GAOR) com foco em atuação local, essas agremiações disputam o monopólio da força em âmbito doméstico, e, por vezes, acabam assumindo funções governamentais, colocando em questão a soberania do Estado (Colômbia, 2022).

¹² Desde a assinatura do Acordo de Paz em 2016, a Colômbia enfrentou novos desafios, incluindo a crescente presença de grupos criminosos que exploraram o vácuo de poder deixado pela extinção das FARC-EP, adotando práticas ilícitas de controle social em várias regiões. As ameaças contemporâneas são caracterizadas pela transformação dos grupos organizados, que agora se dedicam a atividades como tráfico de drogas, extorsão e mineração ilegal. Essa mudança no cenário requer uma resposta mais robusta por parte do governo e das forças de segurança, que devem adaptar suas estratégias para entender a complexidade social, política e econômica dos novos desafios (Colômbia, 2023b).

(DNI), subordinada à Presidência, desempenha papel central na coordenação das atividades do setor (Colômbia, 2023c)¹³. Conquanto, vale frisar que sua competência extrapola as funções tradicionais da defesa, englobando a proteção de direitos civis, e o combate à pobreza e à corrupção (Colômbia 2023b).

As ações da Direção se voltam ao atendimento dos interesses nacionais, em acordo com o Plano Estratégico Setorial e Institucional (PESI) que objetiva aprimorar as capacidades do setor para lidar com grupos armados ilegais e organizações criminosas que ameaçam a soberania estatal. Este documento destaca a integração de informações e a utilização de novas tecnologias como essenciais para antecipar e neutralizar ameaças. Por esse prisma, as instituições securitárias propõem o fortalecimento da infraestrutura tecnológica da DNI como medida assertiva para aprimorar a eficiência na execução de suas funções, assim como a formação contínua dos agentes em novas tecnologias (Colômbia, 2023c).

Num contexto geopolítico distinto do sulamericano, no Reino Unido, a Revisão Integrada (RI), aponta quatro tendências que influenciarão a ordem internacional nos próximos anos: mudanças na distribuição de poder global, competição interestatal sobre a natureza da ordem internacional, rápida evolução tecnológica e o agravamento de desafios transnacionais. Em efeito, num ambiente internacional caracterizado pela transição para um sistema multipolar, fragmentado e contestado, considera *mister* o desenvolvimento de capacidades dissuasórias (Reino Unido, 2023a).

Frente ao cenário prospectivo, a estratégia se estrutura sob quatro pilares principais: moldar o ambiente internacional, dissuadir e competir em todos os domínios, abordar vulnerabilidades por meio da resiliência, e produzir vantagens estratégicas. Conquanto, em que pese se tratar de uma união política entre quatro Estados constituintes -Escócia, Inglaterra, Irlanda e o País de Gales-, possuidores de recursos e capacidades técnicas e humanas avançadas, os britânicos contam com uma estrutura de inteligência robusta.

As principais agências que compõem este sistema são: o Serviço de Segurança (MI5) atuando na gestão de ameaças internas; o Serviço Secreto de Inteligência (SIS/MI6) responsável pelo monitoramento de ameaças externas; e, a Sede de Comunicações do Governo (GCHQ) que protege dados sensíveis e coordena operações do setor (Reino Unido, 2023b).

As atividades de inteligência britânica dão apoio à formulação de estratégias para identificar as capacidades e intenções de adversários, produzir avaliações preditivas, realizar monitoramento de ameaças e aplicar contrainteligência para conter interferências externas. Porquanto, fornecem informações que permitem aos líderes desenvolver uma compreensão abrangente dos cenários de interesse, atendendo tanto às necessidades imediatas quanto aos objetivos de longo prazo (Reino Unido, 2023b)¹⁴.

Por conseguinte, a criação de incentivos à formulação de políticas voltadas para a proteção e armazenamento de grandes volumes de informações é encarada como medida necessária para fortalecer a capacidade das instituições de inteligência (Reino Unido, 2023a). Para alcançar esse objetivo, sublinham importância de dispor de infraestrutura adequada e habilidades específicas, além

¹³ Criado em 2011, o órgão substituiu o Departamento Administrativo de Segurança (DAS) e tem como atribuições principais a supervisão da coleta e análise de informações para lideranças políticas e militares, colaborando estreitamente com a Polícia Nacional.

¹⁴ A abordagem inclui uma análise preditiva e dedutiva para responder mais do que questões como “quem, o que, onde e por que”, antecipando possíveis evoluções do ambiente operacional. Outrossim, têm como objetivo detectar padrões de mudança e tendências emergentes para garantir o controle da iniciativa em crises que exijam respostas rápidas, permitindo a antecipação de cenários e formulação de estratégias assertivas frente às ameaças (Reino Unido, 2023b).

de aderir a princípios fundamentais como objetividade, segurança, continuidade e colaboração¹⁵.

No contexto da defesa, a direção dos esforços de coleta e análise de informações é conduzida pelo comandante e seu estado-maior que apresentam questionamentos específicos a serem respondidos. A aquisição de informações é realizada por instituições competentes, sendo as fontes divididas entre controladas, descontroladas, e casuais, avaliadas conforme a sua confiabilidade. Após a coleta, os dados passam por um processo de depuração rigoroso que utiliza Técnicas de Análise Estruturada (TAEs) para eliminar vieses cognitivos (Reino Unido, 2023b).

Em síntese, as estruturas de inteligência supracitadas refletem abordagens distintas para a segurança nacional, moldadas por seus contextos geopolíticos e desafios particulares. Com base no exposto, a próxima seção apresenta uma análise comparativa destas estruturas, mediante a consideração de fatores essenciais que afetam o seu funcionamento.

3 ANÁLISE COMPARADA ENTRE AS INSTITUIÇÕES DE INTELIGÊNCIA DE BRASIL, COLÔMBIA, E REINO UNIDO

Nesta seção apresento uma comparação entre as instituições de inteligência do Brasil, Colômbia e Reino Unido, com base em uma seleção de fatores chave que realçam as diferenças e similitudes entre as unidades de análise. Tais indicadores servem como parâmetros para que possamos compreender como cada agência opera e se adapta para lidar com diferentes desafios securitários em seus respectivos contextos.

Nesta pesquisa foram considerados os seguintes fatores a) estrutura organizacional; b) desenvolvimento técnico-científico; c) ética e transparência; d) integração interagências. Em resumo, essas categorias avaliam: a) hierarquia e distribuição de responsabilidades entre as instituições de inteligência em cada país, considerando como estão integradas ao governo e as Forças Armadas, bem como as funções específicas atribuídas a cada instituição como coleta de informações, contrainteligência e análise estratégica; b) adoção de novas tecnologias e métodos de análise que potencializam as capacidades operacionais das instituições, refletindo sua adaptação às ameaças contemporâneas; c) como cada Estado percebe a importância da ética nas operações de inteligência, incluindo o respeito aos direitos civis e à necessidade de transparência em suas atividades; e, por fim, d) a colaboração entre diferentes agências de segurança e defesa, bem como a coordenação com entidades internacionais.

Destarte, as estruturas examinadas desempenham papéis cruciais na segurança nacional de seus respectivos Estados. Entretanto, apresentam diferenças significativas que merecem atenção, a primeira a ser destacada reside na estrutura organizacional.

No Brasil, o SISBIN opera sob a Presidência da República, refletindo uma integração direta com a esfera governamental; de modo similar na Colômbia, a DNI assessoria o Presidente e o Conselho de Segurança Nacional, entretanto, adota uma abordagem difusa que borra a linha divisória entre segurança pública e defesa. Em contraste, o Reino Unido possui três agências principais subordinadas ao Gabinete do Primeiro-Ministro, cada uma com um foco específico (Brasil, 2016; Reino Unido, 2023b; Colômbia, 2024).

O Sistema brasileiro conta com uma estrutura mais abrangente que integra diferentes órgãos

¹⁵A flexibilidade e a agilidade são tomadas como elementos chave para que a inteligência se adapte rapidamente às mudanças e ofereça suporte oportuno baseado numa compreensão aprofundada das situações, garantindo a alocação eficiente de recursos e a minimização de incertezas (Reino Unido, 2023b).

civis e militares, priorizando a coleta e análise de informações em uma variedade de contextos e cenários. Enquanto que a Direção colombiana possui função central na coordenação das atividades de inteligência voltadas à segurança interna, combate ao narcotráfico e enfrentamento de grupos insurgentes. Já as agências britânicas focalizam um horizonte mais amplo, com vistas à projeção de poder nacional por intermédio das atividades do setor.

Igualmente, as competências e funções de cada instituição se diferem substancialmente. Embora o SISBIN, no Brasil, e a DNI, na Colômbia, possuam um papel abrangente na coleta e análise de informações para a segurança nacional, integrando as funções de inteligência ao suporte de forças militares e civis, o primeiro aborda uma gama mais ampla de desafios internos e externos, ao passo em que a segunda se concentra no combate às ameaças domésticas. Em contrapartida, as agências britânicas descentralizam atribuições, o que permite tratar dos problemas de modo abrangente em diferentes contextos.

O segundo fator a ser notado trata do desenvolvimento técnico-científico, aspecto onde residem semelhanças entre as unidades de análises. Nesse sentido, podemos considerar ponto pacífico para as instituições examinadas, o reconhecimento da importância estratégica do domínio cibernético para a segurança nacional. Uma vez que infraestruturas e sistemas de informação automatizados desempenham função vital nas sociedades contemporâneas, ataques disruptivos capazes de causar interrupção dos serviços básicos podem produzir efeitos cinéticos e/ou cognitivos significativos (Brasil 2023b; Colômbia, 2023b; Reino Unido, 2023b).

No Brasil, este fator é considerado preponderante para fortalecer as capacidades de projeção de poder nacional, desde a produção de tecnologias de uso dual à proteção das infraestruturas, passando pelo emprego de ferramentas cibernéticas úteis para a defesa (Brasil, 2016; 2017). Ante a demanda, tanto a ABIN quanto a AIDef têm intensificado seus esforços para desenvolver capacidades de monitoramento e neutralização de ameaças, sejam provenientes de atores estatais e/ou não estatais (Brasil, 2020, 2023b).

De modo similar, a evolução dos desafios tecnológicos fez deste tópico central às instituições securitárias colombianas, atentas à importância de proteger suas próprias infraestruturas e dados sensíveis contra ataques disruptivos. Em efeito, sublinham a importância estratégica das tecnologias informacionais para obter uma compreensão abrangente dos riscos e ameaças à segurança nacional (Colômbia, 2023a; 2023b).

Ante a demanda, a DNI tem buscado modernizar suas capacidades para uso efetivo de ferramentas como a inteligência artificial e de vigilância cibernética, apontadas como peças chave na construção de um ambiente de segurança mais robusto e adaptável, preparado para enfrentar adversários em constante transformação. Daí, o aperfeiçoamento de sistemas de segurança e o uso de algoritmos de aprendizado de máquina são apontados como soluções eficazes para detectar e prevenir ações hostis, permitindo análises detalhadas que ajudam, por exemplo, a identificar e mitigar operações de espionagem, sabotagem e/ou infiltração (Colômbia, 2023c)¹⁶.

No Reino Unido, a tecnologia é considerada central para a consecução dos objetivos estratégicos nacionais, pois, se trata de um garantidor da posição de liderança internacional. No campo cibernético, essa realidade se constitui por meio de cinco ferramentas fundamentais: inteligência artificial;

¹⁶A DNI tem implementado tecnologias cibernéticas para fortalecer suas operações e monitorar atividades criminosas. A integração de ferramentas permite à DNI coletar dados relevantes que podem ajudar a prevenir e responder a ameaças. Além disso, a capacidade de interceptar comunicações digitais é vital para desmantelar redes criminosas e obter informações sobre suas operações. De modo que o ciberespaço, portanto, se torna um domínio fulcral na luta contra o crime organizado, proporcionando conhecimentos que antes eram difíceis de alcançar (Colômbia, 2023c).

engenharia biológica; telecomunicações; semicondutores; e computação quântica (Reino Unido, 2023c).

Haja vista que enfrentam ameaças oriundas de diversas fontes, incluindo Estados hostis e grupos extremistas organizados, os britânicos consideram o avanço tecnológico como um elemento de risco securitário difuso. Em outras palavras, o desenvolvimento de novas ferramentas informacionais é interpretado como ambivalente, na medida em que, embora possibilite o fortalecimento da segurança nacional por meio de tecnologias avançadas de monitoramento, análise de dados e defesa cibernética, também amplia as vulnerabilidades estratégicas ao expor infraestruturas críticas e sistemas sensíveis a ataques sofisticados e de difícil previsibilidade.

Sob essa perspectiva, reconhece-se que a emergência de novas arenas de conflito, nas quais as fronteiras entre guerra e paz se tornam progressivamente mais nebulosas, tem facilitado a execução de ataques remotos de forma anônima, empregando armas cibernéticas altamente complexas, as quais desafiam não apenas a segurança doméstica, mas também a estabilidade da ordem internacional (Reino Unido, 2023b; 2023c)

Frente ao cenário, a vigilância e a prevenção de ataques desta natureza, se acham fortemente interligadas com processos de análise de dados digitais e informações de inteligência, cada vez mais complexos. À conta disso, o GCHQ e o MI5 contam com alta capacidade de monitoramento e interceptação de comunicações eletrônicas, permitindo uma resposta rápida e assertiva às ameaças. Por outro ângulo, através de campanhas de reconhecimento e exploração, o MI6 é capaz de reunir informações cruciais tanto para avaliar intenções, quanto comprometer sistemas operacionais de seus adversários (Reino Unido, 2023b).

O terceiro fator comparativo diz respeito à importância da conduta ética e transparente no desempenho das atividades de inteligência. Sob esse aspecto, as unidades de análise enfrentam desafios semelhantes.

A doutrina que orienta as atividades da ABIN enfatiza a necessidade de diretrizes éticas para as operações, que devem atentar aos limites impostos pela legislação nacional (Brasil, 2023b). Contudo, embora estabeleçam diretrizes éticas que valorizam a honra e conduta ilibada, os documentos gerais examinados não abordam o tema com maior profundidade (Brasil, 2016; 2017).

Na Colômbia, em parte devido aos conflitos internos, a implementação de parâmetros éticos para condução das atividades securitárias tem sido particularmente relevante, em razão da necessidade de resgate da fiúza pública nas instituições estatais (Colômbia, 2023a; 2023b). Por esse ângulo, as ações da DNI se orientam por princípios como necessidade, idoneidade e proporcionalidade que orientam a coleta, armazenamento e produção de dados. Tais medidas intentam assegurar que os processos de inteligência estejam em conformidade com os direitos humanos e promovam uma cultura de responsabilidade institucional (Colômbia, 2023c).

Em relação ao Reino Unido, a condução ética das atividades das instituições de inteligência como GCHQ, MI5 e o MI6, é considerada fundamental para manter o apoio da opinião pública. À conta disso, essas estruturas estão sujeitas a uma série de diretrizes rigorosas que impõem limites constitucionais às operações do setor, buscando promover um equilíbrio entre a segurança pública e os direitos civis, fundamental para o regime democrático (Reino Unido, 2023b)¹⁷.

¹⁷ A Lei de Regulamentação de Poderes Investigativos (RPI) estabelece um quadro legal rigoroso que regula as atividades, assegurando que qualquer ação, como vigilância ou uso de fontes humanas, esteja alinhada com os princípios de necessidade e proporcionalidade. Outrossim, o processo de autorização, previsto na Lei dos Poderes Investigativos (LPI) é crucial para as agências de inteligência (Reino Unido, 2023b; 2024).

Por fim, ao considerarmos o nível de integração interagências entre as unidades de análise examinadas, é possível notar uma forte disparidade nas estruturas brasileira e colombiana frente à britânica. A despeito disso, a colaboração é percebida como fator essencial para o sucesso das atividades de inteligência em todos os três casos.

A estrutura integrada do SISBIN prioriza a cooperação interinstitucional e a produção de conhecimento estratégico para orientar o processo decisório em alto nível, a ênfase é dada à proteção da ordem democrática e à neutralização de ameaças. Por esse ângulo, a colaboração com outras agências de segurança é percebida como necessária à implementação de estratégicas mais eficazes, que permitam mitigar riscos e/ou responder rapidamente aos incidentes (Brasil, 2016; 2017).

Já na Colômbia, em atendimento ao conceito de segurança humana, a DNI alinha suas atividades de inteligência e defesa à promoção do desenvolvimento socioeconômico e à proteção dos direitos humanos. Ante o contexto, opera em estreita colaboração com as Forças Armadas e agências de segurança pública no enfrentamento às ameaças representadas por organizações criminosas que atuam em áreas estratégicas, impactando recursos naturais e comunidades vulneráveis (Colômbia, 2023c).

A reafirmação da soberania estatal, questão cara às esferas militar e política, passa pela capacidade de atingir estes objetivos. Para tanto, as lideranças apontam para a construção de mecanismos de gestão eficiente do setor público e a elaboração de projetos estratégicos, com foco no uso responsável dos recursos e na melhoria das condições de vida das populações afetadas, como medida assertiva a ser implementada (Colômbia, 2023a).

Já no Reino Unido, a integração interagências é percebida como fundamental para o aprimoramento das atividades de inteligência britânica, permitindo uma abordagem mais coesa, em conformidade com as diretrizes da Organização do Tratado do Atlântico Norte (OTAN). Outrossim, frisam a necessidade de ação conjunta e do conceito de integração multidomínio, que potencializam a análise e o entendimento das informações coletadas, assegurando uma compreensão abrangente da realidade (Reino Unido 2023b).

A abordagem integrada e interdepartamental, envolvendo administrações locais, serviços de emergência e o setor privado, permite gerenciar riscos com maior acurácia. Em atendimento a demanda, um Ambiente Único de Inteligência (SIntE) foi criado para integrar esforços interagências e interdepartamentais, harmonizando todos os elementos do processo de inteligência, e dando fluidez ao compartilhamento de informações (Reino Unido, 2023a). Igualmente, a criação da Agência de Avaliação de Risco à Segurança Nacional (NSRA) tem por objetivo ajudar a identificar vulnerabilidades e preparar respostas a ameaças como disputas político-econômicas e mudanças climáticas (Reino Unido, 2022b).

As instituições de inteligência britânicas se beneficiam significativamente deste alinhamento, pois, a cooperação amplia o acesso a uma gama de informações e recursos. Em efeito, a partilha de inteligência entre GCHQ, MI5 e MI6, permite uma análise mais abrangente e a identificação de ameaças emergentes de forma mais ágil, tal sinergia não apenas melhora a capacidade de resposta a desafios complexos, mas também fortalece a resiliência das operações de segurança, garantindo que as agências estejam preparadas para enfrentar ameaças que transcendam fronteiras e exijam uma resposta coordenada (Reino Unido, 2023b).

Frente ao exposto, se verifica que cada uma das agências britânicas funciona como um sistema independente e integrado, adaptado à realidade geopolítica, operando num modelo de colaboração intensa, onde a troca de informações é facilitada por um ambiente regulatório que prioriza a agilidade e a eficiência. Em contraste, tanto o DNI quanto o SISBIN, lidam com um ambiente mais

fragmentado, onde a fluidez da cooperação interagências esbarra em limitações infraestruturais. Assim, embora as agências latinas tenham avançado na modernização de suas operações, ainda se encontram aquém da eficiência e a interoperabilidade, observadas no Reino Unido. A Tabela 1 sumariza os resultados.

Tabela 1- Capacidades da Inteligência no Brasil, Colômbia e Reino Unido

Fatores-chave		BRASIL ABIN e AIDef	COLÔMBIA DNI	REINO UNIDO GCHQ, MI5, MI6	
	Estrutura organizacional	Subordinadas à Presidência. Perspectiva ampla, ameaças domésticas e externas	Subordinada à Presidência. Foco no enfrentamento de ameaças domésticas	Subordinadas ao Gabinete do Primeiro-Ministro. Foco em ameaças externas	Distintos
	Integração Interagências	Fragmentada	Fragmentada	Complexa, sistema de resiliência avançado	Semelhantes
	Desenvolvimento técnico-científico	Ferramentas analíticas cibernéticas de uso dual.	Modernização do setor produtivo	Tecnologias informacionais avançadas.	
	Ética e Transparência	Esfera civil regulado pelo poder público, âmbito militar pouco explorado.	Supervisão rigorosa	Supervisão rigorosa	

Fonte: Elaborado pelo autor (2024)

Ao compararmos as estruturas de inteligência é possível notar que existem semelhanças e distinções nas abordagens que buscam aumentar o nível de desempenho das atividades do setor que não podem ser compreendidas sem levarmos em conta a robustez institucional que sustenta cada uma das unidades de análise examinadas.

Os achados indicam que o Brasil, conta com uma estrutura organizacional que integra diversos órgãos, mas ainda enfrenta desafios relacionados à interoperabilidade - sistematização do compartilhamento de informações¹⁸ - e transparência. Por sua vez, a Colômbia, embora tenha uma abordagem centralizada, luta para modernizar suas operações e garantir uma interação eficaz entre suas instituições securitárias. Já o Reino Unido, se destaca pela especialização de suas agências, que operam de forma altamente integrada e focada no desenvolvimento e uso de tecnologias da informação avançadas.

Não obstante, se percebe um padrão entre as unidades de análise no tocante ao interesse por fortalecer a segurança nacional através da inovação e da adaptação aos desafios impostos pelas ameaças contemporâneas. Razão pela qual, se espera que essas agências contribuam para proteger os interesses estratégicos inerentes a cada nação. A próxima seção discute o tema em profundidade.

4 A INTELIGÊNCIA NA FORMULAÇÃO DA ESTRATÉGIA DE SEGURANÇA NACIONAL

As variáveis examinadas na seção anterior fornecem uma base sólida para identificar o funcionamento das estruturas securitárias responsáveis pela inteligência. À conta disso, nesta seção, procuro discutir o papel crucial que elas desempenham na formulação de estratégias de segurança mais eficazes.

Na esfera militar, a inteligência oferece insights sobre as capacidades e intenções de adversários, possibilitando um planejamento mais robusto e alinhado aos objetivos de segurança

¹⁸ Interoperabilidade. Definição: nível de padronização referente à compatibilidade, intercambialidade e comunicabilidade.

nacional. Essa integração entre inteligência e operações militares não apenas aumenta a eficácia das missões, mas também minimiza os riscos e os custos associados a ações inadequadas (Lowenthal, 2017).

Da mesma forma, na esfera civil, a inteligência é vital para a formulação de políticas públicas que abordem questões de segurança interna. A análise de dados e informações relevantes permite que os formuladores de políticas compreendam melhor as dinâmicas sociais e econômicas, identificando tendências e riscos que podem afetar a estabilidade e o bem-estar da população.

Em contextos de crise, como pandemias, desastres naturais, ou ataques às infraestruturas críticas, a inteligência pode fornecer informações cruciais que orientem a implementação de medidas assertivas para assegurar a resiliência das instituições públicas. Por essa lógica, a colaboração entre agências do setor e órgãos governamentais se faz essencial para garantir que as ações sejam baseadas em informações precisas e oportunas, promovendo uma gestão mais eficiente dos recursos e uma melhor proteção dos interesses da sociedade (Treverton, 2009).

Con quanto, é preciso ter em conta que a realidade geopolítica influencia significativamente o funcionamento das estruturas de inteligência, revelando como diferentes contextos regionais moldam suas prioridades e as abordagens.

Neste ensejo, o Brasil, como uma potência emergente na América Latina, enfrenta desafios relacionados à segurança interna, como crime organizado e terrorismo, além de preocupações com a proteção de sua biodiversidade e recursos naturais. Essas questões exigem que a ABIN e a AIDef desenvolvam estratégias que abordem não apenas ameaças imediatas, mas também as complexidades que surgem de sua diversidade cultural e territorial.

No contexto da segurança nacional, a expressão “diversidade cultural” alude à multiplicidade de etnias, crenças, línguas e práticas sociais que caracterizam a população brasileira. Essa pluralidade, longe de ser apenas um aspecto sociológico, acarreta desafios significativos para as políticas públicas, sobretudo no que tange à segurança. As estratégias desenvolvidas pela ABIN e pela AIDef devem, portanto, integrar uma compreensão sensível e adaptativa dessa diversidade, respeitando as especificidades culturais das distintas comunidades, a fim de garantir uma atuação que favoreça a coesão social e a estabilidade nacional.

Já a “diversidade territorial” diz respeito à extensão geográfica e à heterogeneidade dos ecossistemas e das realidades socioeconômicas que compõem o Brasil. Desde as vastas florestas amazônicas até os complexos centros urbanos, o território nacional impõe desafios logísticos e operacionais para a implementação de políticas de segurança. Para uma efetiva resposta às ameaças que permeiam diferentes regiões, é necessário que as agências de inteligência adaptem suas estratégias ao contexto local, levando em consideração as condições ambientais, as particularidades socioeconômicas e a dinâmica política de cada área, assegurando uma ação integrada e eficaz em todo o país.

Por outro lado, a Colômbia vive um contexto mais agudo em termos de segurança nacional, marcada por um histórico de conflitos armados e o narcotráfico. Em efeito, após a assinatura do Acordo de Paz em 2016, o Estado buscou reforçar sua presença modernizando setores produtivos e promovendo o resgate da confiança social nas instituições securitárias, com a DNI desempenhando um papel vital na coordenação de esforços para enfrentar não apenas ameaças tradicionais, mas também novas dinâmicas do crime organizado (Colômbia, 2023a).

A Colômbia, com sua complexa geografia e um histórico de conflitos armados, enfrenta desafios singulares no que diz respeito à diversidade territorial e cultural. O país possui vastas regiões remotas, como a Amazônia e as montanhas dos Andes, que são de difícil acesso, onde grupos criminosos e guerrilheiros ainda operam, aproveitando-se da fragilidade do Estado nessas áreas. Além disso, a

diversidade cultural, marcada por uma pluralidade de etnias e tradições, torna ainda mais desafiadora a implementação de políticas de segurança eficazes. A modernização dos setores produtivos e a busca pelo resgate da confiança social nas instituições, exigem uma atuação sensível a essas particularidades locais, coordenando ações que considerem tanto as ameaças tradicionais, como o narcotráfico, quanto as novas dinâmicas do crime organizado, sempre com respeito às especificidades culturais e territoriais do país.

Ambos os Estados latinos se acham em condições distintas da observada no Reino Unido, onde a geopolítica é marcada por um papel global ativo, no qual a defesa e a segurança são moldadas por relações domésticas e exteriores, especialmente com aliados como os Estados Unidos e a União Europeia. De tal forma, as agências de inteligência britânicas são constantemente desafiadas a se adaptarem aos novos tipos de ameaças, incluindo crises sanitárias globais, espionagem cibernética, e ataques terroristas, capazes de atingir tanto a segurança interna quanto a defesa de seus interesses internacionais (Reino Unido, 2023a).

O Reino Unido, embora possua uma geopolítica de destaque global, também enfrenta desafios internos relacionados à diversidade cultural e territorial, os quais impactam diretamente suas estratégias de segurança. A pluralidade étnica e cultural de sua população, somada à presença de regiões com especificidades políticas, como Escócia e Irlanda do Norte, exige uma adaptação contínua das agências de inteligência, como o MI5 e o GCHQ. Essas entidades precisam enfrentar ameaças externas, com especial atenção à sua potencial influência em dinâmicas internas, onde tensões culturais e regionais podem conduzir à instabilidade securitária.

Em atenção às questões peculiares de cada qual, a adoção de parâmetros necessários à condução assertiva das atividades de inteligência se torna um diferencial para aqueles que intentam promover cursos de ação estratégicos que permitam resolvê-las de modo eficiente e discreto. Razão pela qual, o uso de novas tecnologias se tornou uma prática crescente do setor que, cada vez mais, vem utilizando ferramentas informacionais avançadas para otimizar operações e enfrentar desafios emergentes, como o terrorismo e a espionagem cibernética (Treverton, 2009).

Em razão disto, nos três casos, se verifica que a integração interagências é considerada uma prática essencial para operações de inteligência de alto desempenho, capazes de contribuir de modo substantivo com os processos de tomada de decisão.

No Brasil, em cooperação com a ABIN, a AIDef busca assegurar que as informações circuladas entre as Forças Armadas sejam utilizadas de maneira estratégica para a proteção da soberania e integridade territorial. Já na Colômbia, as diretrizes que regulam as atividades de inteligência e contraespionagem, enfatizam a importância da ação interagências no desempenho de suas competências. Ademais, reforçam a importância da cooperação internacional para assegurar uma resposta coordenada e eficaz aos desafios securitários (Colômbia, 2023c). Entretanto, ambos carecem de um sistema integrado funcional e robusto.

Em contraste, no Reino Unido, as instituições de inteligência são compostas por estruturas sólidas e bem articuladas, por intermédio das quais comandos interconectados permitem uma colaboração mais eficaz, aumentando o nível de desempenho das atividades do setor. Conforme estabelecido oficialmente, é função de inteligência garantir que as atividades de defesa sejam realizadas de maneira harmoniosa, e alinhada às políticas governamentais. Essa integração interagências não apenas facilita a troca de informações, mas também cria um ambiente em que operações internacionais possam correr de maneira flexível, adaptando-se às dinâmicas do contexto global. (Reino Unido, 2023b).

Por este prisma, podemos posicionar o MI5, e o M16, e o GCHQ, como modelos ideais de adaptação a um ambiente de segurança dinâmico e multifacetado. Em contrapartida, tanto no Brasil

quanto na Colômbia, embora as principais estruturas de inteligência busquem tal excelência em matéria de integração, ambos enfrentam desafios relacionados à interoperabilidade institucional.

Sem embargo, se faz *mister* destacar os estágios distintos de desenvolvimento tecnológico em que se encontram as unidades em tela. Posto que, nas últimas décadas, tanto o Brasil quanto a Colômbia tenham investido em capacidades analíticas e cibernéticas, e, ainda que, atualmente, estejam empenhados em modernizar suas forças de inteligência por intermédio da incorporação de novas tecnologias, tais processos distam do que ocorre no Reino Unido.

No contexto sulamericano, as Indústrias 4.0 têm se concentrado na adoção de tecnologias digitais para aumentar a eficiência e a produtividade. Essa fase inclui a automação de processos, o uso de Internet das Coisas (IC) e a análise de grandes volumes de dados. No Brasil, o setor tem enfrentado desafios como a infraestrutura limitada e a necessidade de capacitação profissional, dificultando a plena implementação dos princípios deste modelo (Vanzella e Lima, 2020). Igualmente, na Colômbia, o setor produtivo está se modernizando, mas ainda lida com questões estruturais e socioeconômicas que impedem uma adoção mais ampla e integrada dessas tecnologias (OECD/UN/UNIDO, 2019).

Em contrapartida, a chamada Revolução Industrial 5.0, atualmente em curso no Reino Unido, busca não apenas otimizar processos produtivos por meio da automação e integração de tecnologias avançadas, mas também colocar o ser humano e a sustentabilidade no centro da produção. Essa abordagem faz-se evidente em iniciativas que priorizam a colaboração entre máquinas e humanos, promovendo a personalização em massa e a responsabilidade social. Em efeito, se propõe uma transformação onde a eficiência e a inovação, seguem *pari passu* a medidas de sustentabilidade, resultando num modelo que visa não apenas o lucro, mas também o desenvolvimento social (Alves et al., 2020; Shiyan et al., 2021).

Assim, enquanto o desenvolvimento técnico-científico britânico se encontra na fronteira do conhecimento, as forças produtivas no Brasil e Colômbia permanecem focadas na modernização e na eficiência de processos, refletindo as necessidades e contextos específicos de regiões historicamente dispares, como a latina e a europeia. Contudo, tendo em vista que a promoção da segurança humana constitui elemento central da estratégia colombiana, o modelo colombiano carrega alguma semelhança com o processo que se desenrola no Reino Unido.

A DNI está se modernizando, integrando tecnologias que potencializam suas capacidades operacionais e melhoram a resposta a ameaças, especialmente no combate ao narcotráfico e à insurgência. O uso de ferramentas de inteligência artificial e vigilância cibernética é apontado como chave para reduzir os custos de aquisição, depuração e transmissão de informações, apoiando a tomada de decisões no mais alto nível hierárquico e ampliando a capacidade de ação preventiva do Estado (Colômbia, 2023c).

Já no Reino Unido, a necessidade de incorporar métodos modernos e tecnologicamente avançados para identificar e neutralizar de modo assertivo um espectro mais amplo de atores, fez da capacidade de lidar com grandes volumes de informação um diferencial competitivo. Conforme registram os documentos oficiais, por lá, a automação, inteligência artificial e o aprendizado de máquina já vem sendo empregadas para identificação de riscos e oportunidades, otimizando a coleta e análise de informações que anteriormente eram difíceis de serem tratadas com métodos tradicionais (Reino Unido, 2023b).

Contudo, ao passo em que ampliam a eficácia no desempenho das atividades de inteligência, o uso de novas tecnologias informacionais suscita um importante debate a cerca de seus limites jurisdicionais. Tendo em vista as idiossincrasias contextuais, as instituições do setor enfrentam um

dilema fulcral, até que ponto as suas atividades devem ou não se moldar às demandas das lideranças?

A questão se faz pertinente, uma vez que as esferas política e militar, embora interdependentes, possuem culturas organizacionais distintas que influenciam suas expectativas e objetivos. Nesse sentido, enquanto líderes políticos podem buscar imprimir um caráter personalista às instituições securitárias, promovendo a busca por informações que legitimem seus interesses pessoais, as lideranças militares tendem a demandar a produção de dados que ajudem a maximizar a eficácia operacional das forças para cumprimento de missões designadas.

Destarte, o dilema levanta preocupações sobre a objetividade e a integridade da atividade de inteligência, uma vez que a sua adaptação ao que é solicitado pode comprometer a neutralidade e a capacidade analítica das agências. À vista disso, a necessidade de transparência torna-se um ponto central nesse debate.

Em geral, as agências de inteligência seguem normas que visam garantir que suas operações respeitem os direitos civis e os princípios democráticos. A importância dessas diretrizes é amplamente discutida na literatura que enfatiza que a ética não deve ser um mero complemento às operações de inteligência, mas uma parte integrante de sua cultura organizacional, uma vez que a fiúza pública nas instituições estatais está intimamente ligada à percepção de que as informações são produzidas de forma independente e ética (Miller et al., 2021).

Não obstante, quando as agências se veem pressionadas a atender interesses específicos, pode haver um risco significativo de desvio de suas funções essenciais. Porquanto, a busca por um equilíbrio entre atender às demandas e manter a integridade da atividade de inteligência se constitui como um desafio incontestável aos agentes do setor. Mais do que isso, a transparência nas práticas de inteligência é vista como essencial para mitigar os riscos de abusos de poder e assegurar que as atividades estejam alinhadas com os interesses da sociedade.

No Brasil, o tema se tornou particularmente polêmico, dado o registro recente de mudanças na estrutura de comando das agências de Inteligência, com a transferência da ABIN do Gabinete de Segurança Institucional (GSI) à tutela do Ministério da Casa Civil, em certa medida devido aos atentados orquestrados em 8 de janeiro de 2023, classificados pelo poder público como tentativa de golpe de Estado que colocaram em questão a eficácia das estruturas de inteligência (Verdélío, 2023; Oliveira, 2023).

Já em contextos onde as instituições de segurança têm um histórico de abusos, como na Colômbia, a promoção da ética é crucial para restaurar a confiança social e legitimar a atuação do Estado. Entretanto, recentemente o governo colombiano se tornou alvo de investigação por suposto esquema de espionagem ilegal orquestrado para monitorar membros da Corte Constitucional do país (AFP, 2024).

Tampouco no Reino Unido a discussão se torna trivial, uma vez que as agências de inteligência têm a responsabilidade de manter um equilíbrio delicado entre eficácia operacional e integridade moral, garantindo que as ações respeitem a dignidade humana e os valores democráticos (Omand, 2021).

Entretanto, ao passo em que precisam lidar com ameaças externas que intentam promover o caos através de campanhas de desinformação, ataques cibernéticos e influências políticas, as agências de inteligência tiveram de passar por um árduo processo de robustecimento de suas capacidades (The Economist, 2024). Essa expansão reforçou a importância do compromisso ético, pois, na ausência de sua vigilante observância a identificação de padrões distintivos que as separem de práticas autoritárias seria praticamente impossível.

Ao contrastar as abordagens ocidentais, baseadas na ética e transparência, com as táticas russas, a discussão sobre o controle ético na inteligência ganha relevo, não apenas dada a necessidade de proteção aos direitos civis, mas também em razão de seu potencial para fortalecer alianças internacionais e reduzir a hostilidade global. Em essência, a ética não é apenas uma restrição, mas uma ferramenta estratégica que legitima o uso da inteligência num cenário de ameaças complexas (Ohmand, 2021).

Para além da orientação de práticas operacionais, tais normativas contribuem, também, para assegurar que as atividades do setor tenham maior prestígio e legitimidade fortalecendo a cooperação entre o setor público, privado e a esfera social. Contudo, esses padrões devem ser constantemente revisados para que se mantenham relevantes num cenário de ameaças em constante mudança. Por meio de relatórios públicos e supervisão independente, a transparência nas operações pode ajudar a mitigar os riscos de abusos de poder e garantir que as atividades sejam conduzidas de maneira responsável.

Não obstante, no Brasil, controvérsias recentes, como o caso da “Abin paralela”, demonstram a urgência de estabelecer diretrizes claras que distingam informações estratégicas sigilosas de dados que podem ser compartilhados com a sociedade. Isso porque na ausência de supervisão eficaz e de delimitações precisas, abusos de poder e desvios de conduta podem ocorrer, comprometendo significativamente a confiança pública nas instituições de Estado. Nesse sentido, o fortalecimento de mecanismos de controle é imperativo para assegurar a legitimidade das instituições de segurança e a proteção da democracia (Crisóstomo, 2024).

Por outro lado, informações diretamente vinculadas à segurança nacional, como identidades de agentes, operações em andamento e dados que possam comprometer estratégias de defesa, devem permanecer sigilosas. Esse equilíbrio é crucial para proteger o Estado de ameaças internas e externas, garantindo que a divulgação pública não comprometa a eficiência e a eficácia das operações de inteligência.

Embora na Colômbia a transparência nas atividades de inteligência busque equilibrar a proteção da segurança nacional com a preservação da legitimidade democrática, sendo particularmente relevante em um contexto marcado por histórico de abusos, as práticas de prestação de contas, como relatórios públicos, adotadas pela DNI, contrastam com denúncias recentes de espionagem ilegal que evidenciam a necessidade de fortalecer mecanismos de supervisão, fundamentais para restaurar a fiúza pública e prevenir desvios institucionais (Colômbia, 2024).

Já no Reino Unido, o modelo de transparência nas atividades de inteligência enfatiza a supervisão pública sem comprometer a segurança nacional. Relatórios como o *Disruptive Powers* detalham a aplicação de poderes disruptivos de maneira alinhada a parâmetros legais, garantindo que as operações sejam conduzidas de forma ética e responsável (Reino Unido, 2020). No entanto, informações sensíveis, como dados operacionais e identidades de agentes, permanecem confidenciais, refletindo um equilíbrio entre o sigilo necessário e a responsabilidade democrática.

Desta forma, a discussão sobre transparência no setor de inteligência assume importância central, especialmente diante de crises institucionais e de polarização política. A adoção de práticas inspiradas em modelos como os da Colômbia e do Reino Unido podem facilitar a construção de um equilíbrio entre sigilo e prestação de contas, fortalecendo a confiança da sociedade, promovendo a ética nas operações e consolidando os princípios democráticos nas atividades de inteligência.

Por fim, tendo por base a ampla dimensão dos pontos destacados, se pode razoavelmente afirmar que apesar das diferenças contextuais, a eficiência das instituições securitárias depende da adaptação às inovações tecnológicas, observância ética e transparência das atividades, e a construção

de medidas de fortalecimento mútuo interinstitucional e interdepartamental, aspectos cruciais para lidar com as ameaças contemporâneas.

Ao abordarmos a intersecção entre as esferas civil e militar é importante reforçar o papel da inteligência como uma ferramenta que não apenas fundamenta a segurança nacional, mas também orienta a formulação de políticas públicas. A sinergia entre essas dimensões garante que as respostas a ameaças sejam abrangentes e integradas, refletindo uma abordagem holística que visa fortalecer a segurança e assegurar o bem-estar da população. Num mundo cada vez mais complexo, a capacidade de uma nação de formular e implementar políticas informadas pela inteligência pode ser considerada, portanto, um indicador de sua resiliência e eficácia na gestão de riscos.

Portanto, assumindo o pressuposto de que instituições de inteligência no Brasil, Reino Unido e Colômbia desempenham papéis vitais no planejamento estratégico, é plausível considerar que a integração somada ao uso de novas tecnologias informacionais de modo responsável e transparente reflita a robustez institucional das unidades de análise supracitadas, na busca por obter vantagem estratégica e resiliência diante de ameaças complexas.

Dito de outro modo, a conjunção dos fatores-chave destacados nesta pesquisa tem efeito significativo sobre a capacidade das instituições de inteligência fornecerem suporte confiável e oportunidade às lideranças, garantindo que as decisões estratégicas estejam fundamentadas numa compreensão objetiva dos desafios e oportunidades.

5 CONCLUSÃO

Os achados desta análise comparativa destacam a relevância das estruturas de inteligência no Brasil, na Colômbia e no Reino Unido como pilares estratégicos para a formulação de políticas e a salvaguarda da segurança nacional. A pesquisa revelou que, embora cada qual enfrente desafios e disponha de capacidades singulares, há uma convergência notável em torno da necessidade de integração interagências, do avanço técnico-científico e da observância de preceitos éticos para nortear suas operações. A eficácia das agências analisadas demonstra que a inteligência transcende o caráter meramente operacional, se configurando como um instrumento indispensável para a gestão de riscos em um ambiente global marcado pela crescente complexidade.

No contexto brasileiro, a integração de órgãos civis e militares por meio do SISBIN evidencia um avanço significativo para a gestão de questões de segurança nacional. Entretanto, subsistem desafios relacionados à interoperabilidade entre instituições e à transparência nas operações, que limitam o seu pleno potencial. Nesse sentido, a modernização tecnológica e a adesão aos princípios éticos e legais emergem como elementos cruciais para o fortalecimento da fé pública e ampliação da eficácia operacional das agências de inteligência.

Na Colômbia, a Direção Nacional de Inteligência (DNI) desempenha um papel central no enfrentamento de ameaças internas, como o narcotráfico e as insurgências, ao mesmo tempo em que busca modernizar suas operações tecnológicas e aprimorar sua coordenação interinstitucional. Sua abordagem, que combina elementos de segurança e desenvolvimento socioeconômico, pode ser considerada um modelo promissor para lidar com as dinâmicas contemporâneas, embora ainda necessite de maior consolidação institucional que lhe assegure maior eficácia.

Por outro lado, o Reino Unido destaca-se pelo elevado nível de sofisticação de suas operações de inteligência, refletido na especialização de suas agências e no emprego de tecnologias avançadas. A integração robusta entre suas instituições e a observância rigorosa de normas éticas,

o posicionam como referência na gestão estratégica da segurança nacional. Contudo, mesmo nesse cenário, questões como o equilíbrio entre transparência e sigilo operacional evidenciam a necessidade de constante aprimoramento das práticas, garantindo a legitimidade e a eficácia do setor.

Por conseguinte, a continuidade desta agenda de pesquisa revela-se imperativa para aprofundar os estudos acerca da aplicação estratégica da inteligência no Brasil, especialmente no que tange à sua capacidade de articular os interesses das esferas política e militar. O fortalecimento das capacidades analíticas e operacionais das agências nacionais, aliado a uma maior integração interagências, poderá viabilizar respostas mais assertivas às ameaças contemporâneas. Além disso, o alinhamento da inteligência estratégica às exigências da segurança nacional não apenas subsidiará a formulação de políticas públicas mais robustas, como também contribuirá para a proteção da soberania e o fomento do desenvolvimento sustentável. Nesse contexto, avanços nessa linha de investigação têm o potencial de consolidar a resiliência institucional brasileira, afirmando sua posição como um ator estratégico de relevância no cenário internacional.

REFERÊNCIAS

AFP. Petro Nega Espionagem Ilegal após Denúncia de Magistrado na Colômbia. **EXAME**, jun. 24. 2024. Disponível em: <<https://exame.com/mundo/petro-nega-espionagem-illegal-apos-denuncia-de-magistrados-na-colombia/>>. Acesso em: 22.10.2024.

ALVES, Joel., Lima, Tânia M., Gaspar, Pedro D. Is Industry 5.0 a Human-Centred Approach? A Systematic Review. **Processes** 2023, 11 (1), 1-15, 2023.

BRASIL. **Política Nacional de Inteligência Decreto nº 8.793**. 2016. Presidência da República. Secretaria-Geral Subchefia para Assuntos Jurídicos. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm#:~:text=1%C2%BA%20A%20Pol%C3%ADtica%20Nacional%20de,%20de%20dezembro%20de%201999%20.>. Acesso em: 02.06.2024.

BRASIL. **Estratégia Nacional de Inteligência**. Presidência da República. Gabinete de Segurança Institucional. 2017. Disponível em: <<https://www.gov.br/abin/pt-br/centrais-de-conteudo/politica-nacional-de-inteligencia-1/ENINT.pdf>>. Acesso em: 02.06.2024.

BRASIL. **Política de Defesa Nacional, Estratégia Nacional de Defesa**. Presidência da República Secretaria-Geral. 2020. Disponível em: <<https://legis.senado.leg.br/sdleg-getter/documento?dm=8865685&ts=1614082662204&disposition=inline>>. Acesso em: 25.05.2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Presidência da República. Casa Civil Subchefia para Assuntos Jurídicos. 2023a. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 25. 05.2024.

BRASIL. **Doutrina da Atividade de Inteligência**. Presidência da República Casa Civil Agência Brasileia de Inteligência. 2023b. Disponível em: <<https://www.gov.br/abin/pt-br/centrais-de-conteudo/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023>>. Acesso em: 05.06.2024.

BRASIL. **Estratégia de Inteligência de Defesa**. Ministério da Defesa Estado-Maior Conjunto das Forças Armadas. 2023c. Disponível em: <<https://www.gov.br/defesa/pt-br/assuntos/>>

estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD60E01EstratgiadeIntelignciadeDefesa1Edio2023.pdf>. Acesso em: 05.06.2024.

CRISÓSTOMO, Caio. **PF Liga Tentativa de Golpe e caso da Abin Paralela ao Indiciar Bolsonaro.** Folha de São Paulo. 2024. Disponível em: <<https://www1.folha.uol.com.br/poder/2024/11/pf-liga-tentativa-de-golpe-e-caso-da-abin-paralela-ao-indiciar-bolsonaro.shtml>>. Acesso em: 22.11.2024.

COLÔMBIA. **Estrategia de Defensa Nacional (2022-2032).** Escuela Superior de Guerra. Colombia. 1ºed., Bogotá. Fundación Konrad Adenauer. 2022. Disponível em: <<https://esdeglibros.edu.co/index.php/editorial/catalog/book/161>>. Acesso em: 23 ago. 2024.

COLÔMBIA. **Plan Nacional de Desarrollo 2022-2026: Colombia Potênciam Mundial de la Vida. Departamento Nacional de Planeación.** 2023a. Disponível em: <<https://www.dnp.gov.co/Planificacion/Paginas/Plan-Nacional-de-Desarrollo-2022-2026.aspx>>. Acesso em: 13 ago. 2024.

COLÔMBIA. **Política de Seguridad, Defensa y Convivencia Ciudadana. Garantías Para la Vida y la Paz (2022-2026).** Ministério de Defensa Nacional. 2023b. Disponível em: <https://ddhhcolombia.org.co/wp-content/uploads/2023/05/GARANTIAS-PARA-LA-VIDA-Y-LA-PAZ.pdf>. Acesso em: 28 ago. 2024.

COLÔMBIA. **Plan Estratégico Sectorial / Institucional (2023-2026).** Dirección Nacional de Inteligencia. 2023c. Disponível em: <<https://dni.gov.co/wp-content/uploads/2024/01/PLAN-ESTRATEGICO-DNI-2023-2026.pdf>>. Acesso em: 05 set. 2024.

COLÔMBIA. **Dirección Nacional de Inteligencia: Inteligencia Estratégica al Servicio del País.** Dirección Nacional de Inteligencia. 2024. <https://dni.gov.co/la-entidad/estructura-organica-organigrama/>. Acesso em: 03 set. 2024.

LIU SHYAN., PENGYUE LI., JINFENG WANG., PENG LIU. Toward Industry 5.0: Challenges and Enablers of Intelligent Manufacturing Technology Implementation Under the Perspective of Sustainability. **Helyon**, 10, 1-15, 2024.

LOWENTHAL, M. M. **Intelligence: From Secrets to Policy.** CQ Press. 2017.

MILLER, S. R. M., REGAN, M., WALSH, P. F. **National Security Intelligence and Ethics,** Routledge, 2021, 316 p.

OECD/UN/UNIDO. Transforming Industries: Unleashing the Potential of Industry 4.0 in Colombia, In: **Production Transformation Policy Review of Colombia: Unleashing Productivity**, OECD Publishing, Paris, 2019.

OLIVEIRA, Caroline. Ex-Abin diz que GSI foi Alertado sobre Ameaça de Golpistas no 8/1 ‘em Grupo de Whatsapp’. **Brasil de Fato**, ago. 01. 2023. Disponível em: <<https://www.brasildefato.com.br/2023/08/01/ex-abin-diz-que-gsi-foi-alertada-sobre-ameaca-de-golpistas-no-8-1-em-grupo-de-whatsapp>>. Acesso em: 25.10.2024

OMAND, David. The Ethical Limits We Should Place on Intelligence Gathering as Part of an Integrated CT Strategy. **Terrorism and Political Violence**, 33 (2), 290-301, (2021).

REINO UNIDO. **HM Government Transparency Report: Disruptive Powers 2020.** UK

Government. 2020. Disponível em: < <https://www.gov.uk/government/publications/disruptive-powers-2020/hm-government-transparency-report-disruptive-powers-2020-accessible> >. Acesso em: 22.11.2024.

REINO UNIDO. **The UK Government Resilience Framework.** Cabinet Office. 2022b. Disponível em: <<https://www.gov.uk/government/publications/the-uk-government-resilience-framework/the-uk-government-resilience-framework-html>>. Acesso em: 15.07.2024

REINO UNIDO. **Integrated Review Refresh 2023 Responding to a more contested and volatile world.** Presented to Parliament by the Prime Minister. 2023a. Disponível em: <<https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world>>. Acesso em: 11.07.2024

REINO UNIDO. **Joint Doctrine Publication 2-00 Intelligence, Counter-intelligence and Security Support to Joint Operations.** Ministry of Defence. 2023b. Disponível em: <https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf>. Acesso em: 18.07.2024.

REINO UNIDO. Law, oversight and ethics. **Security Service MI5, 2024.** Disponível em: <<https://www.mi5.gov.uk/how-we-work/law-oversight-and-ethics>>. Acesso em: 15.10.2024.

RENDEIRO, Sérgio Henrique Lopes. A integração das Operações de Informação com a Inteligência Militar Terrestre. 2017. 43 f. **Trabalho de Conclusão de Curso** (Especialização em Ciências Militares). Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2017.

THE ECONOMIST. Vladmimir Putin's spies are plotting global chaos. **International Going Feral**, out. 13. 2024. < <https://www.economist.com/international/2024/10/13/vladimir-putins-spies-are-plotting-global-chaos>>. Acesso em: 25.10.2024.

TREVERTON, G. F. **Intelligence for the 21st Century.** Cambridge University Press. 2009.

VERDÉLIO, Andreia. Governo Transfere Abin do GSI para a Casa Civil. **Agência Brasil**, fev. 03. 2023. Disponível em: <<https://agenciabrasil.ebc.com.br/politica/noticia/2023-03/governo-transfere-abin-do-gsi-para-casa-civil>>. Acesso em: 28.10.202