

INTELIGÊNCIA NA DEMOCRACIA

DESAFIOS E PERSPECTIVAS PARA A
AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

**Inteligência na Democracia:
Desafios e perspectivas para a Agência Brasileira de Inteligência**



PRESIDÊNCIA DA REPÚBLICA
CASA CIVIL
AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Inteligência na Democracia:
Desafios e perspectivas para a Agência Brasileira de Inteligência



Brasília/DF
Dezembro de 2024



REPÚBLICA FEDERATIVA DO BRASIL

Presidente Luiz Inácio Lula da Silva

CASA CIVIL

Ministro Rui Costa

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Diretor-Geral Luiz Fernando Corrêa

SECRETARIA DE PLANEJAMENTO E GESTÃO

Secretário Rodrigo de Aquino

ESCOLA DE INTELIGÊNCIA

Diretora Anna Cruz

Coordenação

Coordenação-Geral de Pesquisa

Catálogo Bibliográfico Internacional e Normalização

Divisão de Conhecimento e Memória – DICOM/CGPE/ESINT

Capa

Samuel Tabosa

Editoração Gráfica

Samuel Tabosa

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

SPO Área 5, Quadra 1

CEP: 70610-905 – Brasília/DF

1ª edição: dezembro de 2024

I61 Inteligência na democracia: desafios e perspectivas para a Agência Brasileira de Inteligência. – Brasília: Abin, 2024.

288 p.

ISBN: 978-65-86360-47-9

1. Atividade de Inteligência – História – Brasil. 2. Cenários prospectivos.
I. Agência Brasileira de Inteligência. II. Título.

CDU 355.40(81)



Os capítulos desta obra são de responsabilidade de seus autores. As opiniões emitidas não necessariamente exprimem pontos de vista ou posicionamentos oficiais da Agência Brasileira de Inteligência.



I Sumário

Apresentação	9
---------------------------	----------

Parte I. Inteligência e Democracia: Contexto

Capítulo 01. 25 anos da ABIN: <i>Redirecionamento</i> , Reorganização e Reposicionamento	17
Luiz Fernando Corrêa	

Capítulo 02. Serviços de inteligência, contextos nacionais e regimes políticos: efetividade e legitimidade em perspectiva comparada	43
Júlio C. Rodriguez	

Capítulo 03. Democracia e inteligência estatal: Caminhos para o Controle no Contexto Brasileiro	73
Rodrigo Ribeiro Bedritchuk	

Parte II. Atividade de Inteligência no Brasil: História

Capítulo 04. Uma era de transição: entre o SNI e a ABIN	107
Priscila Carlos Brandão e Samantha Viz Quadrat	

Capítulo 05. Breve Histórico da Cooperação em Inteligência: Dinâmicas atuais para a Reformulação do SISBIN	151
Leonardo Singer Afonso e Cintiene Sandes Monfredo Mendes	

Capítulo 06. A Inteligência como política pública: desafios para a ABIN ..	179
Rodrigo de Aquino	

Parte III. Futuro da Atividade de Inteligência no Brasil: Perspectivas

Capítulo 07. O Papel da Escola de Inteligência da ABIN: uma reflexão ...	213
Anna Cruz e Marco Cepik	

Capítulo 08. A renovação da agenda de inteligência no contexto contemporâneo	239
Ana Ribeiro e Esaú Feitosa	
Capítulo 09. Desafios tecnológicos emergentes: impactos para a Contrainteligência e a resposta a Ameaças Cibernéticas e Interesses adversos	257
Cristina Célia Fonseca Rodrigues e Juliano Rodrigues Ferreira	
Posfácio. Os próximos 25 anos	281
Intelis (União dos Profissionais de Inteligência de Estado da ABIN)	



I Apresentação

Coordenação-Geral de Pesquisa

Escola de Inteligência
Organizadora do livro

Em um cenário de crescentes demandas por transparência e diálogo com a sociedade, a Agência Brasileira de Inteligência (ABIN) enfrenta a missão de consolidar seu papel no contexto democrático brasileiro. Motivada pela efeméride de 25 anos da ABIN e do Sistema Brasileiro de Inteligência (SISBIN), *Inteligência na Democracia: desafios e perspectivas para a Agência Brasileira de Inteligência* é uma obra que reúne a contribuição de acadêmicos e profissionais da inteligência para desmistificar e esclarecer a relevância da Agência na manutenção da segurança nacional e no fortalecimento das instituições democráticas. Ainda que gestores da ABIN estejam entre os autores do livro, ele não se propõe a ser uma história oficial, e suas reflexões não devem ser encaradas como uma visão institucional. Essa obra foi concebida para ser um espaço livre de debate sobre temas relevantes da história e para o futuro da Atividade de Inteligência.

Com nove capítulos divididos em três partes – contexto, história e perspectivas futuras –, o livro oferece uma visão abrangente da atuação da ABIN, mostrando como a Inteligência é uma peça fundamental para a soberania nacional e para a defesa da democracia no Brasil. Ao longo de suas páginas, o leitor é convidado a refletir sobre os avanços, desafios e possibilidades da Atividade de Inteligência no Brasil. O objetivo é estabelecer diálogo com a sociedade para a construção de uma compreensão coletiva sobre essa atividade vital, ainda que pouco conhecida e reconhecida, para o desenvolvimento nacional e para a segurança do Estado e da sociedade em um contexto de transições globais e crescente instabilidade internacional.

A primeira parte do livro é intitulada *Inteligência e Democracia: Contexto*, onde se propõe apresentar a ABIN e seu atual processo de reconfiguração institucional, assim como demonstrar fundamentos da Atividade de Inteligência e os relacionar a princípios democráticos. O capítulo inaugural é escrito pelo Dr. Luiz Fernando Corrêa, Diretor-Geral da ABIN. Delegado aposentado da Polícia Federal, ele tem em seu currículo relevantes experiências na administração pública, tendo ocupado o cargo de Secretário Nacional de Segurança Pública do Ministério da Justiça, entre 2003 e 2007, e o de Diretor-Geral do Departamento de Polícia Federal, entre 2007 e 2011. No ano em que a Agência completa 25 anos, o texto traz o diagnóstico de que é fundamental adequar a ABIN às novas demandas e expectativas da sociedade, buscando construir uma imagem de transparência e comprometimento democrático. O capítulo explora três eixos centrais da gestão de Corrêa na ABIN: redirecionamento, reorganização e posicionamento. Sua análise sublinha as transformações internas da Agência, apontando o compromisso de redirecioná-la para responder às necessidades de um Brasil soberano, de reorganizá-la para garantir maior efetividade e de reposicioná-la frente ao governo e à sociedade, buscando maior legitimidade de atuação.

No segundo capítulo, o professor Júlio Rodriguez, da Universidade Federal de Santa Maria (UFSM), traz uma análise comparativa entre diferentes serviços de Inteligência ao redor do mundo, enfatizando as relações entre efetividade e legitimidade em diferentes regimes políticos. Pesquisador com artigos de referência no campo dos Estudos de Inteligência, Rodriguez examina as peculiaridades e os desafios que os serviços de Inteligência enfrentam para se adequarem aos contextos democráticos e autoritários, revelando como a atuação e o controle sobre essas atividades refletem os valores e as estruturas de cada sociedade. Ao expor essas dinâmicas, o autor convida o leitor a entender as complexidades da Inteligência no Brasil em relação a práticas internacionais, ampliando o debate sobre a legitimidade e o papel da ABIN no fortalecimento da democracia.

O terceiro capítulo, assinado por Rodrigo Ribeiro Bedritichuk, Analista Legislativo do Senado e Secretário da Comissão Mista de Controle das Atividades de Inteligência (CCAI), enfoca a importância do controle externo para que a Inteligência esteja, de fato, adaptada ao regime democrático. Bedritichuk identifica os principais desafios enfrentados pelos parlamentares ao exercerem controle sobre a Inteligência, mostrando que a efetividade deve ser buscada mesmo diante da natural politização das comissões. Para o autor, o caso brasileiro demonstra que, embora importantes passos tenham sido dados na estruturação de um sistema democrático de Inteligência, bem como no seu controle, ainda há lacunas significativas que precisam ser superadas. Sua análise destaca que tornar o controle da Inteligência eficaz é essencial para a consolidação democrática, convidando o autor a refletir sobre os aspectos que legitimam a Inteligência no contexto brasileiro.

A segunda parte do livro, intitulada *Atividade de Inteligência no Brasil: História*, percorre as transformações históricas que moldaram a ABIN, revelando os desafios e conquistas que marcaram sua evolução. No quarto capítulo, Priscila Carlos Brandão, Professora Titular da Universidade Federal de Minas Gerais (UFMG), e Samantha Viz Quadrat, Professora Associada da Universidade Federal Fluminense (UFF), examinam o processo de transição do extinto Serviço Nacional de Informações (SNI) para a ABIN, destacando as mudanças institucionais, culturais e políticas que fizeram parte dessa transição. As duas professoras, pesquisadoras internacionais de referência sobre a história da Atividade de Inteligência, discutem como as práticas de Inteligência evoluíram no Brasil, passando por crises, períodos de repressão e descontinuidades institucionais. Demonstram como a ABIN tem buscado distanciar sua imagem do passado autoritário do SNI, ajudando o leitor a compreender a construção de uma Agência plenamente alinhada aos princípios democráticos.

No quinto capítulo, Leonardo Singer Afonso, Oficial de Inteligência, e Cintiene Sandes Monfredo Mendes, Professora Adjunta da Escola

Superior de Defesa (ESD), apresentam uma análise histórica sobre a cooperação em Inteligência e suas especificidades no caso brasileiro, especialmente a partir de 1999, com a criação do Sistema Brasileiro de Inteligência (SISBIN). Nesse capítulo, a experiência profissional de Singer, inclusive como Diretor de Inteligência Interna durante o processo atual de reformulação do SISBIN em 2023, se junta ao reconhecimento acadêmico de Mendes, especialista em cooperação interagências, para diagnosticar problemas crônicos da cooperação interagências em Inteligência no Brasil. Os autores destacam como a atual reformulação do SISBIN foi motivada pela necessidade de melhorias para otimizar o compartilhamento de dados e informações, aumentar a fluidez na comunicação e estabelecer prioridades coletivas que promovam a segurança nacional.

No sexto capítulo, Rodrigo de Aquino, Oficial de Inteligência e atual Secretário de Planejamento e Gestão, faz um debate sobre os últimos 25 anos da ABIN sob a perspectiva da Inteligência como política pública. Aquino, um dos mais experientes Oficiais de Inteligência na ativa, ingresso do primeiro concurso público para a Atividade de Inteligência em 1994, aborda os estágios do ciclo de políticas públicas (formulação e planejamento, implementação, avaliação e controle) para apresentar ao leitor aspectos relevantes do funcionamento e da atuação da Agência. O autor demonstra as dificuldades da Inteligência brasileira para integrar a agenda política nacional, o que impacta na formulação de diretrizes claras para que a Inteligência possa responder adequadamente às demandas de segurança nacional. Da mesma forma, elucida ao leitor os desafios de implementação da política pública de Inteligência por meio de um sistema de instituições relativamente pouco coesas e com pouco fluxo informacional entre si, assim como aponta os desafios e paradoxos inerentes da avaliação e controle da atividade. Sua análise conclui sobre a importância de uma atuação com equilíbrio entre eficiência, efetividade e legitimidade, visando a construir uma ABIN respeitada e integrada ao cenário institucional brasileiro.

A terceira parte, *Futuro da Atividade de Inteligência no Brasil: Perspectivas*, propõe uma reflexão sobre os rumos da Inteligência no Brasil, considerando o atual cenário internacional de crescente instabilidade securitária e de transições globais, como a climática e tecnológica, com impactos significativos em diferentes esferas da vida humana. Nesse sentido, o sétimo capítulo, de Marco Cepik e Anna Cruz, traz uma reflexão sobre o papel da Escola de Inteligência da ABIN para o futuro da Atividade de Inteligência no Brasil. Cepik, professor titular da Universidade Federal do Rio Grande do Sul (UFRGS) e atual Diretor Adjunto da ABIN, foi diretor da ESINT entre maio de 2023 e janeiro de 2024, enquanto que Anna Cruz, Oficial de Inteligência desde 2008, é a atual diretora da Escola. Os autores destacam o papel da ESINT como local de reflexão crítica sobre a natureza e a cultura da Atividade de Inteligência, assim como espaço de criação de consensos por meio da divergência e convergência de ideias. Entre o binômio sigilo e transparência, apontam que a ESINT tem função de ser um canal efetivo de diálogo com a sociedade. Ao explorar o currículo, as metodologias e os objetivos da Escola, os autores reforçam a importância de preparar profissionais da Inteligência capacitados para lidar com os crescentes desafios contemporâneos e comprometidos com os valores democráticos.

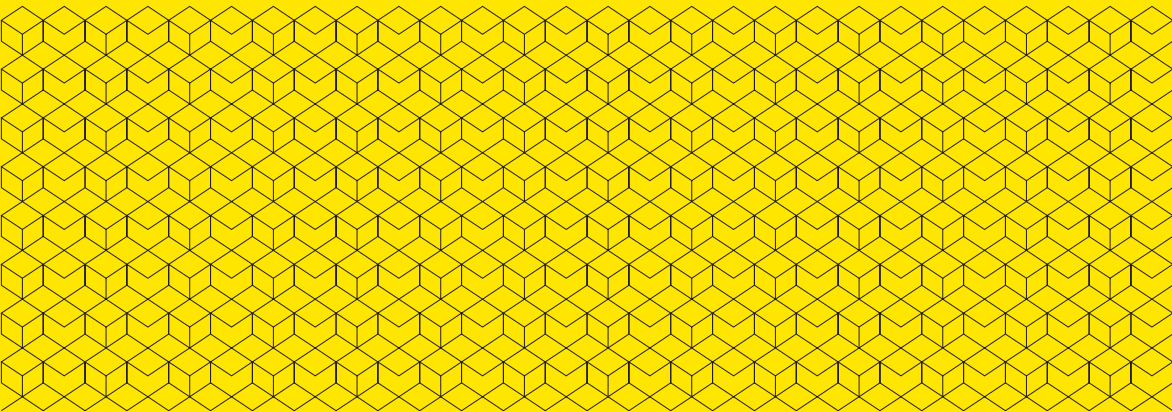
Ana Ribeiro e Esaú Feitosa, respectivamente Diretores de Inteligência Externa e Inteligência Interna, são os autores do oitavo capítulo, que trata da renovação da agenda de Inteligência no contexto contemporâneo. Eles examinam as mudanças na agenda sob a ótica da complexificação dos assuntos de Inteligência, a qual, por um lado, relaciona-se ao alargamento do rol de ameaças percebidas e tratadas como prioritárias pelos Estados e, por outro, refere-se à ampliação dos desafios advindos dos temas tradicionais de Inteligência. Os autores também apresentam ao leitor como a complexificação da agenda traz a necessidade de revisar a forma como se produz e se difunde Inteligência, discutindo aspectos sobre oportunidade e qualidade no assessoramento estratégico. O capítulo, assim, é uma análise fundamental para compreender as novas dinâmicas sobre as temáticas de trabalho da Inteligência.

O livro encerra-se com o nono capítulo, escrito por Cristina Célia Fonseca Rodrigues, diretora de Contrainteligência, e Juliano Ferreira, diretor do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC). Nele, abordam-se os desafios tecnológicos emergentes e seus impactos sobre a contrainteligência. Ao discutir avanços como a computação quântica, computação em nuvem e inteligência artificial, os autores destacam como a segurança cibernética e a contrainteligência precisam evoluir continuamente para lidar com as novas ameaças possibilitadas por essas inovações. Considerando as novas ameaças cibernéticas e o papel da tecnologia na segurança, o capítulo ressalta ao leitor como a criptografia de Estado, um dos principais ativos da ABIN, adquire importância central na segurança de informações sensíveis e infraestruturas críticas do Brasil.

Ao reunir essas reflexões, *Inteligência na Democracia* propõe-se a ampliar o conhecimento e a compreensão pública sobre a importância da Inteligência para o Estado e a democracia brasileira, no sentido de mitigar o desconhecimento e o estigma social que permanecem acerca da Atividade. A obra convida a sociedade civil, a academia e as autoridades brasileiras a participar de um debate fundamental sobre que tipo de Inteligência o Brasil quer e necessita para cumprir suas ambições nacionais em um ambiente internacional e regional incerto e inseguro. Nesse sentido, fica evidenciado, capítulo após capítulo, o engajamento dos profissionais de Inteligência da ABIN para garantir uma organização comprometida com os valores democráticos e empenhada na segurança das pessoas e das instituições, na construção de uma Agência cada vez mais transparente, moderna, eficiente e legitimada pela sociedade.

PARTE I

Inteligência e Democracia: Contexto





25 anos da ABIN: Redirecionamento, Reorganização e Reposicionamento

Luiz Fernando Corrêa
Diretor-Geral da ABIN

Os serviços de Inteligência são realidades na máquina estatal contemporânea da maior parte dos países. Raros são os Estados que dispensam o estabelecimento de uma organização profissional especializada na coleta, análise e disseminação de informações para subsidiar a tomada de decisão das autoridades nacionais. O Brasil, enquanto potência regional da América do Sul, não seria exceção. Como um país continental com desafios geopolíticos, econômicos e sociais expressivos, requer um serviço de inteligência que esteja à altura de suas complexidades. O Presidente da República, legitimamente eleito e nos termos da legislação, deve ter à disposição uma estrutura de inteligência profissional para subsidiá-lo na tomada de decisões. A inexistência ou ineficácia desta estrutura implica riscos e graves danos ao país na execução das políticas públicas.

Criada pela Lei 9.883/1999, a Agência Brasileira de Inteligência (ABIN) é um órgão permanente, apartidário e apolítico, com atuação nacional e representação no exterior. Compete a ela, nos termos da lei, obter e analisar informações para a produção de conhecimento de inteligência a fim de assessorar o Presidente da República, assim como planejar e executar ações de contrainteligência para garantir a proteção de conhecimentos sensíveis (Brasil, 1999). Enquanto órgão central do Sistema Brasileiro de Inteligência (SISBIN), tem a seu cargo planejar,

executar, coordenar, supervisionar e controlar as atividades de inteligência do País. A Atividade de Inteligência, assim, tem como missão o assessoramento especializado aos tomadores de decisão de alto nível para a segurança das pessoas e das instituições – ou, em outras palavras, da sociedade e do Estado.

Desde a criação da ABIN e do SISBIN, o mundo mudou muito, os desafios aumentaram e se tornaram mais complexos. O Brasil sediou e realizou um ciclo de grandes eventos internacionais entre 2007 e 2016 sem incidentes, demonstrando a capacidade dos órgãos de Inteligência e segurança. O país também ampliou a presença comercial e diplomática no mundo, o que exigiu que a Inteligência aumentasse sua capilaridade no exterior. Por outro lado, passamos por uma grave crise na área de segurança pública, agravada pelos impactos negativos de fases persistentes de recessão econômica e de uma pandemia global que encontrou nossa região desarticulada, dividida e desorientada.

A crise mundial de 2008-2009 desencadeou um acentuado aumento global das desigualdades sociais, agravado pelos efeitos desiguais das mudanças climáticas e das transformações tecnológicas, mas também piorado pela crise da governança multilateral e pela crescente desconfiança e falta de cooperação entre as grandes potências. Neste mundo mais complexo, diante do desafio transnacional representado pelo avanço da criminalidade organizada, do extremismo violento e do caos informacional, nosso SISBIN precisa ser reorganizado e nossas instituições civis de inteligência precisam ser fortalecidas.

Diante desses desafios, o Presidente da República reconheceu a necessidade de uma reformulação abrangente da atuação da ABIN e do SISBIN. Essa reformulação foi elaborada em três pilares fundamentais: redirecionamento, reorganização e reposicionamento. O redirecionamento envolve uma revisão dos objetivos estratégicos da Agência, alinhando-os com as novas realidades nacionais e internacionais. A reorganização visa a melhorar a eficiência operacional e a capacida-

de de resposta da ABIN, garantindo que ela possa lidar com as ameaças contemporâneas de maneira mais eficaz e legítima. Já o reposicionamento busca ampliar a integração da Agência com outras áreas do governo e da sociedade, aumentando a transparência e reforçando seu papel como ator central para a segurança nacional.

Esses esforços são essenciais para garantir que a ABIN esteja preparada para os próximos 25 anos de atuação. O mundo está em constante transformação, e a inteligência precisa evoluir junto com ele. O desafio é garantir que a ABIN não apenas acompanhe essas mudanças, mas também seja capaz de antecipá-las, garantindo a segurança e a soberania do Brasil em um cenário global cada vez mais complexo e incerto. Com esse tripé – redirecionamento, reorganização e reposicionamento – a ABIN se prepara para enfrentar os novos desafios do presente e do futuro, adaptando suas estruturas, estratégias e capacidades para proteger o Brasil e suas instituições.

1. Redirecionamento

O cenário internacional impõe grandes desafios à segurança e ao desenvolvimento do Brasil. Transições profundas e globais, especialmente nos âmbitos climático, demográfico e tecnológico, geram tanto riscos quanto oportunidades para os Estados, alterando de maneira transversal, embora desigual, as condições de vida das populações. Essas transformações impõem mudanças à maneira tradicional de conduzir a Atividade de Inteligência, exigindo que ela lide não apenas com atores antagônicos, mas também com fenômenos e óbices complexos.

Simultaneamente, a intensificação da competição entre os Estados que compõem os polos de poder na ordem internacional emergente constrange a criação de soluções conjuntas para os novos problemas, desafiando a produção de inteligência útil e oportuna e renovando desafios clássicos, como os relacionados à contrainteligência. No

âmbito interno, há a transnacionalização de questões como o crime organizado, o extremismo violento e os crimes cibernéticos. Problemas anteriormente tratados como nacionais, como as ameaças às instituições democráticas e ao desenvolvimento nacional, assumiram natureza transnacional, sob influência das transições globais e da competição entre Estados.

Para lidar com esse cenário complexo, foram estabelecidas três tarefas imediatas. A primeira foi a definição de um conjunto de áreas prioritárias para atuação transversal da Agência: crise climática, defesa da democracia e segurança cibernética. A segunda tarefa foi a revisão da Política Nacional de Inteligência, o documento balizador mais importante para a Atividade de Inteligência no Brasil. E, finalmente, a terceira foi a elaboração da Doutrina da Atividade de Inteligência, que estabelece o conjunto de princípios que servem de base para o funcionamento da Atividade de Inteligência na ABIN.

O compromisso firmado com o Presidente da República e confirmado em sabatina perante a Comissão Mista de Controle da Atividade de Inteligência (CCAI) determinava que a ABIN focaria seus esforços em três assuntos caros ao governo democraticamente eleito em 2022 (Brasil, 2023a).

- 1. Impactos das mudanças climáticas sobre a segurança das pessoas e das instituições:** as mudanças climáticas são uma das maiores ameaças à segurança global, exigindo do Estado e da sociedade capacidade de adaptação, mitigação, planejamento e investimentos. A maior frequência de eventos climáticos extremos aumenta os riscos à integridade da população, provoca disrupções nas cadeias produtivas, gera instabilidade social e causa danos a infraestruturas críticas. Efeitos desiguais da crise climática entre Estados e nas populações ameaçam a segurança alimentar e hídrica em diversas regiões, com maior impacto sobre comunidades vulneráveis,

desencadeando crises migratórias e de saúde pública. Além disso, o desequilíbrio climático altera o equilíbrio de poder no sistema internacional, comprometendo a estabilidade econômica, política e social dos países e aumentando o risco de conflitos. Em cenário que demanda transição energética e ecológica, o Brasil tem responsabilidade e papel protagonista como ator na governança climática global.

A ABIN, assim, deve ser capaz de reunir, analisar e conectar informações provenientes de uma ampla gama de fatores que, em conjunto, influenciam cenários interligados de maneira complexa, como a produção de soja, criação de gado, exportação de carne, desmatamento na Amazônia Legal, garimpo ilegal, trabalho escravo, eventos climáticos extremos e a capacidade de geração elétrica em suas diversas matrizes. Ao se tornar eminentemente civil e profissional, a ABIN passou a integrar cada vez mais a análise de riscos e implicações de segurança com o conhecimento científico já produzido por instituições renomadas, como Ibama, ICMBio, Embrapa, Cepagri/Unicamp, IBGE, INPE e INPA.

- 2. Prevenção do extremismo violento ideologicamente motivado:** a transformação na comunicação de massa tem exacerbado as fissuras no tecido social causadas pelas disputas políticas. Com a redução da distância entre produtores e consumidores proporcionada pelas plataformas de redes sociais e aplicativos de mensagens, permitiram a disseminação instantânea de informações e a fragmentação da produção de conteúdo. Esse cenário permitiu a ascensão de novas vozes e a diversificação das perspectivas e fontes de informação, entretanto, também deu espaço a discursos de ódio, intolerância e extremismos. A sociedade brasileira está imersa em tensa disputa política e social, marcada pelo endurecimento de posições e pelo surgimento de formas de atuação que por vezes

ultrapassam os limites da democracia e se manifestam violentamente. Esse enrijecimento político tem gerado divisões profundas, tanto em grandes grupos sociais quanto em famílias e comunidades. Agentes políticos extremistas aproveitam o ambiente de tensão para promover uma retórica agressiva e inflamável, intensificando a intolerância e dificultando a construção de consensos. Para compreender plenamente esse fenômeno, é crucial reconhecer sua dimensão transnacional. Observa-se um crescimento global de narrativas políticas e sociais extremistas, intolerantes e divisivas, que se expandem de maneira organizada e coordenada. Líderes associados a essas narrativas podem ocupar cargos de poder ou buscar ascender a tais posições por meio de processos democráticos, mas frequentemente agem à margem do Estado, utilizando distorções na mídia tradicional e nas redes sociais para espalhar suas mensagens.

A ABIN, nesse contexto, deve atuar para a defesa da democracia, reunindo e analisando informações que possibilitem a identificação e o monitoramento de indivíduos e grupos com ideologias que ameaçam o Estado Democrático de Direito. O foco da análise contínua e especializada deve estar nas motivações, estrutura organizacional e fontes de financiamento desses grupos, permitindo a antecipação de ações que envolvam o uso de violência, mesmo que simbólica, como a disseminação de discursos de ódio, atos de sabotagem e ataques com armas de fogo ou explosivos. A ligação entre interesses ilegais, ideologias extremistas e a imposição violenta de comportamentos predatórios compromete a coesão social e não pode ser subestimada, sob o risco de que os segmentos mais vulneráveis da sociedade continuem a sofrer danos irreparáveis.

- 3. Segurança cibernética:** a segurança cibernética é um desafio complexo para a soberania digital do Brasil, e sua posição

de destaque no cenário global o torna um alvo atraente para ameaças cibernéticas de origem doméstica e internacional. A transição tecnológica mundial e a intensificação dos conflitos entre potências evidenciam a conexão entre a segurança cibernética e a geopolítica, aumentando a necessidade de uma perspectiva estratégica para a contraposição a essas ameaças. Frente ao desafio, a abordagem da segurança cibernética passou por mudanças significativas. Há crescente reconhecimento de que os incidentes cibernéticos são praticamente inevitáveis, transitando o antigo foco de prevenção de ataques para modelo centrado na resiliência cibernética.

A ABIN precisa ser capaz de analisar e atuar preventivamente para neutralizar ameaças cibernéticas (não de crimes cibernéticos, que são atribuição das polícias judiciárias), inclusive tendo capacidade de atribuição de autoria nos casos de ataques em massa de *malware* tecnologicamente sofisticados contra infraestruturas críticas e sistemas de informação dos serviços essenciais (comunicação, energia, finanças). Também deve ter capacidade de realizar o acompanhamento sistemático de conteúdos em mídias sociais que configurem ameaças à estabilidade da sociedade e do Estado Democrático. A capacidade cibernética da ABIN deve ser complementar e sinérgica com as demais arquiteturas institucionais e tecnológicas do governo federal, incluindo as das polícias e das Forças Armadas.

A Atividade de Inteligência no Brasil se organiza em torno de documentos que balizam sua atuação. Revisar esses documentos, para que reflitam uma visão precisa dos desafios atuais, tem sido uma das prioridades da ABIN. A PNI é o principal documento orientador da Atividade de Inteligência no Brasil. Ela estabelece os parâmetros e limites para a atuação dessa atividade e de seus executores, além de definir seus pressupostos, objetivos, instrumentos e diretrizes dentro

do SISBIN (Brasil, 2016). Ao longo de 2024, a ABIN elaborou uma proposta de nova PNI e apresentou-a ao Conselho Consultivo do Sistema Brasileiro de Inteligência (Consisbin). O intuito da ABIN ao propor a revisão da PNI de 2016 é redirecionar a atuação da Atividade de Inteligência frente ao complexo cenário contemporâneo.

A revisão da PNI envolveu a reavaliação de ameaças e oportunidades decorrentes das transformações globais, como a crise climática e a transição tecnológica, além de mudanças no cenário nacional e internacional, como o fortalecimento de movimentos antidemocráticos e o extremismo violento. Primeiramente, reforça a relevância da Atividade de Inteligência, profissional e capacitada, para o apoio ao processo decisório no país e na sociedade brasileira. Em seguida, apresenta conceitos que visam esclarecer como a atividade se organiza e enxerga sua atuação diante da sociedade. Por fim, ela define os objetivos a serem alcançados e oferece diretrizes sobre como o sistema deve atuar para cumpri-los.

A nova PNI traz impacto a todo o Sisbin, orientando esforços para atingir os objetivos definidos e fornecendo diretrizes que viabilizem essa execução. Além disso, funciona como um meio de diálogo com a sociedade, esclarecendo a forma de atuação da Atividade de Inteligência em uma democracia e alinhando-se aos princípios fundamentais da República.

No mesmo sentido de maior interação, comunicação e transparência com a sociedade, reafirmando o papel da Atividade de Inteligência no regime democrático, em dezembro de 2023, a Escola de Inteligência (ESINT) da ABIN lançou a primeira Doutrina da Atividade de Inteligência aberta ao público (Brasil, 2023b). Esse documento, portanto, trata de definir e explicitar para o público os entendimentos que a ABIN tem hoje sobre a Atividade de Inteligência e como ela deve ser praticada pela Agência no Brasil, tendo por parâmetro a Constituição Federal de 1988 (Brasil, 1988) e a legislação vigente.

A Doutrina se refere a um conjunto de princípios que servem de base para educar e orientar as práticas individuais e coletivas da Agência e registra entendimentos conceituais que fornecem uma base prescritiva comum para o agir no tempo e no espaço (Brasil, 2023c). Ela procurou ser elaborada de forma clara, parcimoniosa, autocrítica e revisável, no sentido de que ela seja atualizada e aperfeiçoada de tempos em tempos. Os entendimentos que a ABIN tem sobre a Atividade de Inteligência são resultado de suas próprias experiências desde a criação do órgão em 1999. Resultam também da incorporação de elementos julgados relevantes a partir de outros documentos oficiais brasileiros sobre doutrinas diversas, dos debates públicos travados no Congresso Nacional e no seio da sociedade civil, da produção científica e técnica sobre a Atividade de Inteligência no Brasil e no exterior, e mesmo do conhecimento tácito disponível sobre o tema.

Além de se tratar de um documento de orientação, a Doutrina visa a facilitar a comunicação entre os integrantes da ABIN e desta com a sociedade, incluindo aí os demais organismos responsáveis pelo desenvolvimento de Atividade de Inteligência do país. Nesse sentido, não pretende substituir ou subordinar as doutrinas de inteligência do SISBIN, dos subsistemas e dos demais organismos de inteligência do Brasil, mas sim facilitar o diálogo e a sinergia entre os diversos componentes do sistema.

Em suma, a diretriz para redirecionar a atuação da ABIN no sentido de alinhá-la aos desafios percebidos pelo governo brasileiro, especialmente naqueles que se referem à crise climática, à defesa da democracia e à segurança cibernética, foi materializada na nova PNI e na Doutrina da Atividade de Inteligência. Ao redirecionar os trabalhos da Inteligência brasileira, o País assegura que sua primeira linha de defesa esteja bem orientada para garantir a segurança das pessoas e instituições.

2. Reorganização

Em face aos desafios advindos de um cenário global e nacional complexo, a reorganização do sistema de inteligência e de seu órgão central foi requisito fundamental. Por um lado, era necessário reorganizar o Sistema Brasileiro de Inteligência (SISBIN), que, após 24 anos de sua criação, continuava relativamente disfuncional e desestruturado. Por outro, o órgão central do Sistema, a ABIN, dada a troca de subordinação ministerial do Gabinete de Segurança Institucional para a Casa Civil efetivada pelo Decreto nº 11.426, de 1º de março de 2023, demandava mudanças na arquitetura de governança interna em termos de controle, gestão e produção que garantissem a efetividade e a legitimidade do órgão (Brasil, 2023d).

O SISBIN foi instituído pela Lei nº 9883, de 7 de dezembro de 1999, mesmo instrumento que criou a ABIN e a inseriu como órgão central (Brasil, 1999). O objetivo do Sistema é integrar ações de planejamento e execução das atividades de Inteligência no País, com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional. A organização e funcionamento do SISBIN só veio a ser normatizado quase três anos depois, pelo Decreto nº 4376, de 13 de setembro de 2002 (Brasil, 2002). O arcabouço jurídico criado permitiu a materialização do SISBIN e a sua expansão, que passou de treze membros iniciais para quarenta e oito em 2023.

Ainda que o SISBIN tenha desempenhado satisfatoriamente suas atribuições em momentos críticos, como na integração entre diversos órgãos durante o ciclo de grandes eventos ocorridos no Brasil entre 2007 e 2016 ou na operacionalização de centros de inteligência para crises, ele manteve disfuncionalidades estruturais originadas em seu decreto de criação. A baixa diferenciação de competências entre os órgãos dentro do sistema, a composição heterogênea entre seus membros, os critérios pouco objetivos de ingresso e as dificuldades

crescentes de gestão do conhecimento eram alguns dos problemas persistentemente identificados no Sistema.

Após os ataques extremistas de 08 de janeiro de 2023, o Governo Lula traçou como objetivo a reestruturação do SISBIN. Essa meta foi cumprida com a publicação do Decreto nº 11.963, de 6 de setembro de 2023 (Brasil, 2023e), que substituiu o Decreto nº 4376/2002, promovendo a reorganização do SISBIN baseada nos seguintes pilares: 1. fortalecimento do papel facilitador da ABIN, definido como órgão Central do Sistema; 2. reposicionamento do Conselho Consultivo, tornando-o estrutura consultiva de alto nível; 3. reordenamento dos órgãos a partir da classificação em categorias; e 4. efetiva inclusão das Unidades da Federação.

O novo decreto definiu de forma mais precisa as obrigações da ABIN enquanto órgão central do Sistema e do Consisbin como instância de supervisão da Atividade de Inteligência no Brasil. Para mitigar o déficit de efetividade na gestão, o Sistema foi institucionalizado de forma mais robusta, com normas e regulamentos mais claros para novos ingressos, definindo fluxos e critérios de adesão, além de incentivar a valorização da Atividade de Inteligência nos órgãos que compõem o SISBIN.

Para lidar com a baixa diferenciação de competências e com a alta heterogeneidade de órgãos, foram criadas diferentes categorias de pertencimento ao SISBIN. A classificação em categorias objetivou promover maior organicidade ao Sistema, modulando as expectativas de participação dos membros e as capacidades de contribuição conforme suas próprias características.

Definiu-se, assim, a categoria de órgãos permanentes, o núcleo duro do Sistema, constituído dos representantes das principais expressões do Estado brasileiro em matéria de relações exteriores, defesa externa, segurança interna e governabilidade. Em uma segunda camada são

os órgãos dedicados, composta daquelas entidades do Poder Executivo federal com unidades dedicadas à Atividade de Inteligência e que atuam em assuntos estratégicos relacionados a temas da PNI. Na terceira camada estão os órgãos associados, que são aqueles que lidam com temas relacionados à PNI, mas que não possuem recursos humanos, institucionais e de tecnologia específicos para atuar com Inteligência.

A última camada, por fim, foi criada para endereçar ao problema de como lidar efetivamente com as Unidades da Federação. Os órgãos federados, assim, são órgãos estaduais e municipais que, mediante critérios e procedimentos estabelecidos, podem ser incorporados ao SISBIN. Essa previsão do Decreto denota o reconhecimento da capacidade e do potencial para a Atividade de Inteligência instalados nas unidades federativas, em especial para lidar com ameaças como o crime organizado e o extremismo violento.

O Decreto nº 11.963/2023 estabeleceu uma estratégia digital voltada a aprimorar a qualidade da integração e comunicação entre os órgãos do Sistema em um contexto de transformação digital, com intuito de reforçar a utilidade e, principalmente, a oportunidade do assessoramento estratégico à Presidência da República. Mesmo antes do Decreto, a ABIN já possuía e distribuía aos membros do SISBIN ferramentas para trâmite seguro de documentos classificados. No entanto, a nova estratégia visou aumentar o patamar tecnológico para a viabilizar o compartilhamento seguro de conhecimentos em ambientes virtuais integrados (Brasil, 2024a). Os esforços foram divididos em três frentes: comunicação segura; criptografia de Estado; e Plataforma Sisbin.

A comunicação segura visa à criação de ferramenta de mensageria própria, com interface amigável e usabilidade facilitada ao usuário, para comunicação e troca de arquivos entre membros. A criptografia de Estado, área tradicional de expertise da ABIN por meio do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações

(CEPESC), oferece soluções robustas para proteção de dados armazenados e em trânsito. E a Plataforma Sisbin, cujo desenvolvimento é o núcleo da nova estratégia digital, será um dos principais ativos do Sisbin, ao integrar uma base de dados compartilhada do Sistema com permissões de acesso diferenciadas conforme as categorias do novo Decreto. Além disso, o compartilhamento e troca de informações que ocorrerão na plataforma serão seguros, rastreáveis e auditáveis.

O desenvolvimento dessas soluções tecnológicas está sendo conduzido pela ABIN, que as disponibilizará assim que estiverem finalizadas aos membros do Sisbin conforme critérios legais e técnicos de segurança das informações. A ampla adoção de soluções tecnológicas pelos membros do SISBIN proporcionará ganhos de escala, tornando a plataforma uma ferramenta eficaz de gestão do conhecimento em Inteligência, com o potencial de reposicionar a atividade no Brasil como indispensável para o processo decisório, em padrões comparáveis aos de outros países.

Assim, no novo SISBIN, a ABIN efetivamente assumiu sua função como órgão central, atuando como facilitadora e integradora dos membros do Sistema. À agência cabe consolidar as necessidades de conhecimento e capacidades dos integrantes do SISBIN, estabelecer planos de trabalho e integrar as informações recebidas, com o objetivo de oferecer assessoramento estratégico de alto nível aos responsáveis pela formulação e implementação das políticas públicas.

No âmbito interno, a ABIN passou por mudanças em sua estrutura de controle, gestão e produção para se adaptar à nova subordinação institucional à Casa Civil (Brasil, 2023d). O redesenho de processos, garantindo a rastreabilidade e o exame crítico ao longo da trilha de produção de conhecimentos de inteligência, é algo essencial para a qualificação e legitimação das contribuições que a ABIN pode dar ao processo decisório governamental. Nesse sentido, foram estabelecidas dezenas de novas portarias para aperfeiçoar o controle interno,

com o objetivo de garantir conformidade processual, responsabilização de gestores e segurança aos servidores. Essas portarias também têm o intuito de assegurar a conformidade com os requisitos do controle externo, criando instrumentos para a prestação de contas em todas as ações da Agência. A implementação dessas normativas reflete o compromisso da ABIN com princípios básicos de governança, o que é essencial para a legitimidade e efetividade de sua atuação.

O redesenho dos processos gerenciais e do sistema de gestão de documentos da ABIN foi outro passo crucial na reorganização. O aperfeiçoamento da gestão visou garantir que todos os procedimentos seguissem padrões de auditabilidade, rastreabilidade e conformidade, características indispensáveis em uma Agência que lida com informações sigilosas, sensíveis e estratégicas para o Estado brasileiro. A capacidade de auditar as ações de Inteligência não apenas fortalece a integridade da Agência, mas também oferece garantias ao controle externo, aumentando a confiança do público nas operações da ABIN.

Em paralelo ao redesenho de processos gerenciais, buscou-se a melhoria da qualidade da produção, em especial ao que se refere ao assessoramento ao governo sobre vulnerabilidades, riscos e ameaças para a segurança das pessoas e instituições. O crescimento exponencial de informações nas redes sociais e nas várias camadas da internet demanda uma crescente sofisticação analítica para separar o "joio do trigo", ou seja, aquilo que é ruído irrelevante do que é sinal relevante. A qualificação de produtos analíticos tem sido um esforço permanente, com esforços para reforçar a antecipação de crises (alerta avançado) e a capacidade prospectiva de explicar tendências e construir cenários relevantes para o processo decisório de curto, médio e longo prazos.

Para além desses esforços de reorganização, a Inteligência Civil nacional também precisa que os legisladores repensassem o arcabouço legal que sustenta a atividade no Brasil. Apesar das legislações exis-

tentes, como a Lei 9.883/1999, o quadro normativo carece de maior detalhamento em relação às competências legais, missão e escopo de atuação da ABIN. Para assegurar a eficiência e legitimidade da Agência, é fundamental que seja debatida e aprovada pelas autoridades competentes uma base legal sólida, tanto para garantir a segurança jurídica necessária à atuação de seus servidores quanto para configurar a Inteligência brasileira, dentro dos parâmetros do regime democrático, para lidar com os desafios do século XXI. Mais que isso, tais medidas visam a reduzir riscos de abusos políticos e profissionais, a aumentar a transparência e a legitimidade das atividades de inteligência.

Em síntese, a reorganização da ABIN, amparada pelo novo decreto do SISBIN e por mudanças internas necessárias, representa uma etapa essencial no amadurecimento da inteligência brasileira. Ao promover uma maior integração entre os órgãos do SISBIN, modernizar seus processos internos e garantir a conformidade com o controle externo, a ABIN está se posicionando para operar de maneira mais eficiente, segura e transparente, em benefício do governo e da sociedade.

3. Reposicionamento

O terceiro pilar da reformulação consiste em reposicionar a ABIN frente ao Estado e à sociedade. O reposicionamento em relação ao Estado significa adequar a produção de inteligência às necessidades das autoridades públicas assessoradas pela ABIN, mas sobretudo posicionar e comunicar os produtos da Agência no mercado de ideias e soluções públicas do Poder Executivo Federal. O reposicionamento em relação à sociedade compreende uma série de medidas que abrem a ABIN para o diálogo com setores específicos – tais como as universidades e as comunidades de especialistas – e para a cidadania de forma geral – compartilhando com a sociedade a responsabilidade pelo aprimoramento democrático das concepções e práticas relacionadas à inteligência.

Do ponto de vista do posicionamento na estrutura estatal, a mudança advinda da vinculação à Casa Civil da Presidência da República estabeleceu novos fluxos para os conhecimentos produzidos e incluiu outros atores no ciclo de produção de conhecimentos de inteligência, seja como interlocutores, demandantes ou usuários desses conhecimentos. Nesse contexto, a ABIN priorizou os esforços de adequação da produção de Inteligência às necessidades dos usuários e a comunicação desses produtos de forma a consolidar a imagem da Agência na Esplanada. O objetivo foi otimizar a utilidade, a assertividade e a consistência dos produtos, assim como apresentá-los de forma lógica, sistematizada e estruturada. A Agência estruturou sua produção em três eixos: portfólio de projetos estratégicos; Agenda de Produção de Inteligência; e Carta de Serviços.

O portfólio de projetos estratégicos comporta esforços temporários e transversais que necessitam da mobilização de recursos extraordinários da Agência, tanto recursos humanos e tecnológicos quanto financeiros e organizacionais. Nesse sentido, são projetos cujo escopo e cujos resultados aspiram a contribuir significativamente para o alcance dos objetivos estratégicos da Agência. Como exemplos, podemos citar a atuação da Agência em 2024 no assessoramento em segurança para o Encontro do G-20 no Brasil (Brasil, 2024b), para a aplicação do Concurso Público Nacional Unificado (CPNU) (Brasil, 2024c), para as Eleições de 2024 (Brasil, 2024d) e para a desintrusão da Terra Indígena Yanomami (Brasil, 2024e).

A Agenda de Produção de Inteligência é uma ferramenta de gestão que apresenta de maneira clara e atualizada as áreas de atuação das unidades de produção de conhecimento na ABIN. Ela organiza o planejamento da produção de Inteligência das unidades finalísticas, distribuída em diferentes linhas de análise. Sua elaboração e revisão são baseadas em três pilares: competência legal, capacidade executória e necessidade do usuário. Seguindo esses critérios, todos os resultados, ferramentas, recursos e operações empregados pela ABIN são

claramente fundamentados e podem ser objeto de controle interno e externo.

A Carta de Serviços, por sua vez, detalha as atividades críticas que a ABIN executa em benefício direto do SISBIN, do governo e da sociedade, tornando mais claro seu papel no processo para a segurança das pessoas e das instituições. A ABIN provê uma série de serviços desse tipo, porém até hoje não os tinha arranjado em uma Carta de Serviços de caráter público. Exemplos de serviços de alto valor são as pesquisas de credenciamento de postulantes a cargos no Governo Federal, a criptografia de Estado desenvolvida pelo CEPESC, análise de geointeligência em apoio a projetos estratégicos e inteligência de proteção para altas autoridades da República. Desde o final de 2024, a ABIN conta pela primeira vez com uma Carta de Serviços, validada pela Casa Civil e pela Presidência da República. Tal como as atividades organizadas na Agenda de Produção, todas as ações realizadas no âmbito da Carta de Serviços são auditáveis e seus resultados, ferramentas, recursos e operações são fundamentados.

Entre as medidas de reposicionamento em relação ao Estado, pode-se mencionar ainda a criação da Aliança Sul-Americana de Inteligência Estratégica (Brasil, 2024f). O marco constitutivo da Aliança foi assinado em 5 de outubro de 2023 e a primeira reunião plenária, com aprovação do estatuto da Aliança, ocorreu no dia 2 de julho de 2024 em Brasília. Coube à ABIN a primeira presidência, *pro tempore*, no ano de 2024. A criação da Aliança, além de estabelecer fórum sul-americano de discussão de assuntos de inteligência, com potencial para formulação de entendimentos estratégicos a nível regional, contribui para promover a relevância da ABIN e dos demais serviços membros na comunidade internacional de inteligência. Seguindo tratativas dos chefes de Estado, a Aliança se pauta pelo princípio da integração regional como forma de enfrentar os desafios compartilhados relacionados à crise climática, ameaças à paz e à segurança internacional, pressões sobre as cadeias de alimentos e energia, riscos de novas pandemias,

aumento de desigualdades sociais e ameaças à estabilidade institucional e democrática. Constituem a Aliança os serviços de Argentina, Bolívia, Brasil, Chile, Colômbia, Equador, Guiana, Paraguai, Peru, Suriname e Uruguai.

O reposicionamento em relação à sociedade compreende iniciativas de diálogo e de abertura. Partiu-se do diagnóstico de que, apesar de o Brasil possuir instituições de excelência, a maior parte delas públicas, nas mais diversas áreas do conhecimento, a ABIN não mantinha diálogo sistemático com redes e centros de produção científica. Isso tendia a prejudicar o planejamento da produção, pois sem esse contato é mais difícil permanecer atualizado quanto às abordagens e preocupações mais relevantes para o governo e a sociedade. Ao mesmo tempo, a utilidade da produção também era prejudicada, pois nem sempre é possível se manter a par das perspectivas científicas mais avançadas sem o contato direto e constante com os principais especialistas.

Nessa frente, coordenada pela Escola de Inteligência (Esint) e pelas unidades estaduais, a ABIN tem encontrado grande receptividade por parte de especialistas e contado com sua inestimável colaboração. Notamos que suas maiores motivações costumam ser a generosidade, a confiança no trabalho da Agência e o desejo de colaborar com o processo de assessoramento para a tomada de decisões estratégicas. Outro aspecto muito gratificante dessas interações tem sido o reconhecimento recíproco entre profissionais de inteligência e acadêmicos como brasileiros e servidores públicos com interesses comuns.

As iniciativas de contato, lançadas de forma sistemática em 2023, incluem a promoção de ciclos de palestras e debates, de seminários, participação em eventos científicos e o engajamento de acadêmicos em projetos específicos. As ações são abordadas especificamente no capítulo deste livro sobre a ESINT, porém é importante ressaltar aqui que essas ações são realizadas conforme normativos que regulam as atividades de pesquisa e extensão da ESINT, todos aprovados no iní-

cio de 2024, como parte dos esforços internos de reorganização da ABIN. As superintendências estaduais foram parte fundamental do processo de maior capilaridade com comunidades de especialistas. Em 2023 e 2024, foram realizados seminários temáticos, no âmbito dos Encontros Regionais do Sisbin, em todas as regiões do país, buscando integrar em torno de temas de relevância nacional e regional especialistas acadêmicos, autoridades e a comunidade de inteligência local (Brasil, 2024g).

Dentre as ações de extensão, merece destaque o Seminário Internacional Desafios para a Inteligência Estratégica (Brasil, 2023f), realizado em dezembro de 2023, em comemoração aos 24 anos de fundação da ABIN. Entre os palestrantes, constaram pesquisadores reconhecidos, representantes de outras escolas de inteligência, do Brasil e do exterior, e dirigentes de serviços de inteligência sul-americanos. Além de palestrantes brasileiros, o evento teve palestrantes da Argentina, Colômbia, Equador, Uruguai e Inglaterra.

No Seminário foram discutidos três tópicos muito relevantes e inter-relacionados: a relação entre inteligência e democracia; os desafios da inteligência estratégica; e a profissionalização da inteligência. O diálogo racional de alto nível sobre esses assuntos tem nos auxiliado muito a continuarmos enfrentando os desafios para a reformulação da ABIN com realismo, esperança e perseverança. Além de terem sido convidados para a plateia autoridades e servidores do Sisbin e de outros órgãos públicos e instituições de ensino superior públicas e privadas, totalizando cerca de 400 pessoas, o Seminário teve cobertura da imprensa.

Outro aspecto do reposicionamento envolve justamente a presença pública dos dirigentes da ABIN. Desde 2023, foram várias as entrevistas concedidas a diferentes veículos de comunicação. Além disso, o número de vezes em que o Diretor-Geral da ABIN compareceu à Comissão de Controle das Atividades de Inteligência (CCAI) do Congresso

Nacional é inédito na história da Comissão. Essas são oportunidades valiosas para exercer o controle social e parlamentar da Inteligência, bem como oportunidades para a ABIN, por meio de seus dirigentes, prestar contas, esclarecer dúvidas, dialogar com representantes da sociedade e apontar compromissos públicos para a gestão do órgão.

No caso da CCAI e do Congresso Nacional, permanecem as oportunidades para trabalhar conjuntamente com o objetivo de aperfeiçoar as regulações e processos de controle externo. Lembramos que todas as atividades da ABIN já são fiscalizadas por órgãos de controle externo, como o TCU, a CGU e a CCAI. Mas é importante aprimorar os procedimentos administrativos de autorização, execução e prestação de contas em análises e operações de inteligência também em relação aos demais órgãos do SISBIN.

Após a divulgação da nova Doutrina da Atividade de Inteligência, publicada em novembro de 2023, a ABIN instituiu outras iniciativas de publicações abertas em 2024, com a intenção de mantê-las permanentes entre as atividades da Agência. A primeira dessas iniciativas foi a elaboração e publicação de documento prospectivo denominado *Desafios de Inteligência 2025*. Esse documento é público, disponibilizado livremente no sítio da ABIN, e serve para comunicar os entendimentos básicos sobre o mundo contemporâneo que orientam de forma transversal as análises de inteligência da ABIN e para apontar quais os principais desafios de inteligência projetados para 2025, nos quais a ABIN pretende concentrar esforços.

Desafios 2025 foi produzido em diálogo com especialistas e com atenção aos melhores conhecimentos disponíveis sobre as atuais transições climática, demográfica e tecnológica, assim como às mudanças geopolíticas em curso, e os impactos dessas transformações para os interesses estratégicos brasileiros. Pretendemos instituir a publicação periódica desse documento prospectivo como consolidação do relacionamento com as comunidades de especialistas e, sobretudo,

como contribuição ao Estado e à sociedade brasileiros no sentido de desenvolver capacidades de previsão e planejamento na área de segurança nacional.

A Esint também criou uma série editorial de livros dedicada à memória institucional da ABIN. O objetivo é, para além de registrar episódios relevantes da Agência, abrir mais um canal de diálogo com a sociedade sobre o que faz a Atividade de Inteligência, como faz, por que faz e para que faz. O primeiro livro da série intitula-se “Memórias da Pandemia”, que trata da atuação da ABIN durante a pandemia de COVID-19 em 2020 e 2021. Demonstra como o serviço de inteligência brasileiro esteve à serviço da sociedade e do Estado brasileiro lastreado na ciência e na racionalidade. Ainda, busca-se fomentar o debate sobre novos paradigmas na produção de conhecimento de inteligência, abordando temas que tradicionalmente não eram foco da atividade, como crises epidemiológicas, mas que se tornaram altamente relevantes devido ao seu impacto potencial no tecido social e à sua importância para a gestão do Estado.

O reposicionamento da ABIN em relação ao Estado e à sociedade será atingido com uma combinação de medidas já conhecidas com outras medidas inovadoras. Algumas delas dizem respeito à gestão, em interlocução com atores governamentais; outras exigem articulação internacional; e outras envolvem relacionamento e atuação conjunta com escolas de governo, universidades e imprensa. Há, ainda, uma dimensão promissora de comunicação direta com o público, que pode ser constituído por setores específicos do governo e da sociedade, assim como pela cidadania como um todo, por meio da divulgação de documentos como a Doutrina e o documento prospectivo de Desafios para 2025. A Inteligência pode e deve trabalhar em conjunto com os mais variados setores da sociedade, respeitando-se as diferentes missões e regramentos institucionais, sempre que houver o interesse comum na proteção dos princípios e atingimento dos objetivos constitucionais, no marco do Estado Democrático de Direito.

Conclusão

As mudanças promovidas para o redirecionamento, reorganização e reposicionamento constituem a nossa visão sobre como preparar a ABIN para os próximos 25 anos. Os esforços já realizados não esgotam tudo o que será preciso fazer, mas representam os primeiros passos para a efetivação dessa visão, que já têm produzido resultados concretos. A nosso favor, contamos com as conquistas resultantes do trabalho sério e dedicado do corpo funcional da Agência, um quadro civil, concursado, profissional e especializado, que demonstrou suas qualidades nos trabalhos realizados recentemente em momentos críticos para o Brasil, tais como o ciclo dos grandes eventos de 2007 a 2016, a pandemia de Covid-19 e os ataques extremistas de 8 de janeiro de 2023.

Os desafios que se afiguram a nível global para os próximos anos são muitos. Vivemos transformações profundas nos âmbitos climático, demográfico e tecnológico que afetam todos os países, gerando vulnerabilidades para as pessoas e as instituições. Além disso, o acirramento dos conflitos entre os Estados não apenas dificulta a cooperação internacional, necessária para lidar com essas vulnerabilidades, como também proporciona o surgimento de novas ameaças, resultantes da competição entre os Estados. Nenhum país relevante pode abrir mão de um sistema de inteligência apto a assessorar a tomada de decisões em alto nível e se contrapor de maneira efetiva à atuação adversa de outros Estados.

Nesse contexto, é imperativo promover o fortalecimento institucional da ABIN. Com vistas a atingir esse objetivo, destacam-se as medidas que levam a avanços na profissionalização dos seus quadros, com fortalecimento das carreiras de inteligência de Estado, e medidas que aprimoram o funcionamento do SISBIN, permitindo maior aproveitamento das capacidades estatais existentes na área de inteligência.

Avançando no caminho que já começamos a percorrer, o futuro da ABIN e da Atividade de Inteligência no Brasil passa por (1) efetivar a incorporação da comunicação segura pelo SISBIN e pelo Governo brasileiro (2) concretizar a plataforma segura para gestão de documentos e interações institucionais; (3) incorporar plenamente ciência de dados e inteligência artificial aos processos de produção de Inteligência; (4) consolidar a liderança brasileira em Inteligência na América do Sul e África; e (5) reconstituir pessoal e orçamento, permitindo a adequação de capacidades e controles à importância da missão institucional da ABIN. Com isso, será possível estabelecer uma ABIN legítima, regrada, relevante e ágil no assessoramento sobre riscos e ameaças ao Brasil.

Para isso, desafios imediatos que precisam ser superados dizem respeito a orçamento, pessoal e legislação. É preciso recompor o orçamento da Agência, de modo a permitir o desempenho regular de suas funções, além de conferir margem maior para os necessários investimentos em modernização da infraestrutura, da tecnologia e no desenvolvimento de novos serviços para o SISBIN e o Governo. Além disso, é imprescindível recompor o quadro de pessoal da ABIN, atualmente subdimensionado e com grande índice de vacância entre os cargos previstos. Fazer isso de forma sustentável requer estabelecer mecanismo regular e seguro de recrutamento por concurso público, permitindo planejar e prover formação adequada e progressiva para os servidores, e evitando lacunas geracionais. Por fim, a exemplo do que fizemos em 2023 com a transferência para a Casa Civil e com o decreto de reorganização do SISBIN, é preciso discutir e aprovar legislação que permita à Atividade de Inteligência continuar a se desenvolver e aprimorar. Todas as ações necessárias ao cumprimento das atribuições institucionais da ABIN e do SISBIN, como um todo, devem ser amparadas legalmente e, no caso daquelas protegidas pelo sigilo, devem ser registradas, controladas e justificáveis publicamente sob as leis brasileiras.

Com a continuidade dos processos de redirecionamento, reorganização e reposicionamento, contando com as condições necessárias, teremos uma ABIN e um sistema de Inteligência preparados para servir ao Brasil à altura de suas necessidades e aspirações nos próximos 25 anos.

Referências

BRASIL. **Comissão do Senado aprova indicação de Luiz Fernando Corrêa para diretor-geral da ABIN.** Agência Brasileira de Inteligência, 4 maio 2023a. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/comissao-do-senado-aprova-indicacao-de-luiz-fernando-correa-para-diretor-geral-da-abin>. Acesso em: 16 set. 2024.

_____. **Nova Doutrina da Atividade de Inteligência é lançada.** Agência Brasileira de Inteligência, 8 dez. 2023b. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/nova-doutrina-da-atividade-de-inteligencia-e-lancada>. Acesso em: 16 set. 2024.

_____. Agência Brasileira de Inteligência. **Doutrina da Atividade de Inteligência.** Brasília, DF: ABIN [2023c]. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023>. Acesso em: 16 set. 2024.

_____. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, [1988]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 16 de setembro de 2024.

_____. **Decreto nº 11.426, de 1º de março de 2023.** Altera o Decreto nº 11.327, de 1º de janeiro de 2023, o Decreto nº 11.329, de 1º de janeiro de 2023, o Decreto nº 9.435, de 2 de julho de 2018, e o Decreto nº 4.376, de 13 de setembro de 2002, para integrar a Agência Brasileira de Inteligência à Casa Civil da Presidência da República. Brasília, DF: Presidência da República, [2023d]. Disponível em: http://www.planalto.gov.br/ccivil_03/ato/2023-2026/2023/decreto/D11426.htm. Acesso em: 16 de setembro de 2024.

_____. **Decreto nº 11.693, de 6 setembro de 2023.** Dispõe sobre a organização e funcionamento do Sistema Brasileiro de Inteligência. Brasília, DF: Presidência da República, [2023e]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm. Acesso em: 16 de setembro de 2024.

_____. **Lei nº 9.883, de 7 de dezembro de 1999.** Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências. Brasília, DF: Presidência da República, [1999]. Disponível em: http://planalto.gov.br/CCIVIL_03/LEIS/L9883.htm. Acesso em: 16 de setembro de 2024.

_____. **Decreto nº 4.376, de 13 setembro de 2002.** Dispõe sobre a organização e funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei nº 9.883, de 7 de setembro de 1999, e dá outras providências. Brasília, DF: Presidência da República, [2002]. Disponível em: https://www.planalto.gov.br/CCIVIL_03////decreto/2002/D4376.htm. Acesso em: 16 de setembro de 2024.

_____. **Decreto nº 8.793, de 29 de junho de 2016.** Fixa a Política Nacional de Inteligência. Brasília, DF: Presidência da República, [2016]. Disponível em: https://www.planalto.gov.br/CCiViL_03/_Ato2015-2018/2016/Decreto/D8793.htm. Acesso em: 16 de setembro de 2024.

_____. Agência Brasileira de Inteligência. **ABIN assina primeiro plano de transformação digital com Ministério da Gestão e da Inovação em Serviços Públicos.** Agência Brasil, 25 mar. 2024a. Disponível em: <https://agenciagov.ebc.com.br/noticias/202403/abin-assina-primeiro-plano-de-transformacao-digital-com-ministerio-da-gestao-e-da-inovacao-em-servicos-publicos>. Acesso em: 17 set. 2024.

_____. Agência Brasileira de Inteligência. **ABIN instala Centro de Inteligência para encontro do G20 em São Paulo.** Agência Brasileira de Inteligência, 27 fev. 2024b. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/abin-instala-centro-de-inteligencia-para-encontro-do-g20-em-sao-paulo>. Acesso em: 17 set. 2024.

_____. Agência Brasileira de Inteligência. **ABIN participa de balanço da aplicação das provas do CPNU.** Agência Brasileira de Inteligência, 18 ago. 2024c. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/abin-participa-de-balanco-da-aplicacao-das-provas-do-cpnu>. Acesso em: 17 set. 2024.

_____. Agência Brasileira de Inteligência. **Diretor-geral da ABIN assina os sistemas das eleições de 2024 no TSE.** Agência Brasileira de Inteligência, 11 set. 2024d. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/diretor-geral-da-abin-assina-os-sistemas-das-eleicoes-de-2024-no-tse>. Acesso em: 17 set. 2024.

_____. Planalto. **Decreto institui a Casa de Governo em Roraima para atender os povos indígenas Yanomami.** Agência Brasil, 28 fev. 2024e. Disponível em: <https://agenciagov.ebc.com.br/noticias/202402/decreto-que-institui-a-casa-de-governo-em-roraima-e-publicado-no-diario-oficial>. Acesso em: 17 set. 2024.

_____. Agência Brasileira de Inteligência. **Aliança Sul-Americana de Inteligência Estratégica assina Estatuto.** Agência Brasileira de Inteligência, 03 jul. 2024f. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/alianca-sul-americana-de-inteligencia-estrategica-assina-estatuto>. Acesso em: 17 set. 2024.

_____. Agência Brasileira de Inteligência. **Debates sobre inteligência artificial marcam evento do SISBIN Sudeste.** Agência Brasileira de Inteligência, 12 set. 2024g. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/debates-sobre-inteligencia-artificial-marcam-evento-do-sisbin-sudeste>. Acesso em: 17 set. 2024.

_____. Agência Brasileira de Inteligência. **Seminário internacional discute inteligência estratégica.** Agência Brasileira de Inteligência, 07 dez. 2023f. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/seminario-internacional-discute-inteligencia-estrategica>. Acesso em: 17 set. 2024.



Serviços de inteligência, contextos nacionais e regimes políticos: efetividade e legitimidade em perspectiva comparada

Júlio C. Rodriguez

Professor Associado

Universidade Federal de Santa Maria (UFSM)

Os serviços de informação e de inteligência estão presentes na maioria dos Estados contemporâneos (Gill, 1994; Lowenthal, 2015). Os contextos nacionais, em função dos regimes políticos vigentes, afetam a organização dos serviços, o escopo de atuação, a capacidade de produção de conhecimento, a legitimidade que possuem em cada sociedade e, por fim, sua efetividade enquanto serviço essencial à segurança do Estado.

Os diferentes regimes políticos contemporâneos, que vão, num contínuo, desde os regimes autocráticos de baixa capacidade até os regimes democráticos de alta eficiência (Tilly, 2007), conformam diferentes tipos de serviços de inteligência, com distintas formas de legitimidade e efetividade. Neste contexto, compreender como contextos nacionais distintos em termos de poder e ameaça em função de diferentes regimes políticos produzem serviços de inteligência que vão ter distintas legitimidades e variadas efetividades só é possível por meio de estudos de caso com grande densidade ou por meio comparações (Andregg; Treverton, 2009; Andregg; Gill, 2014; Estevez, 2014).

Assim, neste capítulo, primeiro identificaremos os casos a serem comparados, que foram escolhidos em função dos diferentes contextos de poder e ameaça, mas que possuem variações nos outros objetos da comparação, isto é, regimes, legitimidade e efetividade. Em segundo lugar, identificaremos o papel dos diferentes regimes políticos na formação dos serviços de inteligência, considerando que regimes menos democráticos possuem maior propensão a formar ou reformar serviços de inteligência menos “controláveis”, enquanto regimes mais democráticos tendem a formar serviços de inteligência mais adaptados aos controles democráticos e adaptados aos mecanismos de *accountability* (Borza; Bruneau, 2007). A relação entre esses dois pontos e as consequências sobre efetividade e legitimidade serão abordadas na terceira parte do capítulo. Por fim, será feita uma breve comparação entre os casos e traçadas as semelhanças e diferenças entre os casos.

1. Contextos Distintos, Serviços Distintos

Nas relações internacionais contemporâneas observamos o recrudescimento do uso da força convencional entre os Estados, ao mesmo tempo em que ocorre a consolidação das ameaças não-estatais à segurança dos Estados. Os Estados contemporâneos, portanto, na tentativa de garantir a segurança de suas sociedades, precisam lidar ao mesmo tempo com ameaças do uso da força convencional por inimigos estatais externos e com as ameaças não convencionais, que podem vir das mudanças climáticas aos grupos transnacionais que operam em zonas cinzentas entre o crime organizado e as organizações paramilitares. Neste contexto os serviços de informações ou inteligência passam, por um lado, pela reafirmação de suas funções e, por outro, pela crescente pressão por reforma de seu escopo (Hermann, 2013).

No caso de grandes potências, por exemplo, a disputa estratégica no nível do sistema internacional reafirma para Estados Unidos, Rússia e China que tais serviços são necessários com amplitude de atuação

e institucionalidade profunda. No caso de potências regionais, por exemplo, a disputa estratégica pode estar próxima, e isso remete a uma percepção de ameaça grande, que conduz também à necessidade de eficácia desses serviços. É o caso de atores regionais aliados de grandes potências, tais como Japão, Coreia do Sul, Alemanha, França, Inglaterra, Israel, Turquia e outros que possuem relações diretas, por exemplo, com os Estados Unidos. Atores regionais que estão relativamente distantes das grandes potências ou de regiões de interesse direto delas, como África Austral e América do Sul, não possuem a mesma pressão por eficácia internacional dos serviços de inteligência, em função direta da percepção menor de ameaça convencional. Entretanto, as dinâmicas regionais de segurança e os contextos nacionais afetam decisivamente a construção e atuação dos serviços. São os casos de África do Sul e Brasil, em que os contextos nacionais tiveram um peso maior que o externo na conformação e recentes reformas de tais serviços (Cepik; Ambros, 2014).

Em todos esses casos, contudo, a formação desses serviços estatais é diretamente afetada pela inter-relação entre ameaças externas e contradições internas das sociedades. Mesmo no caso dos EUA, a institucionalização dos serviços de inteligência passou por desafios grandes no âmbito da política nacional, com momentos de maior ou menor controle de suas ações, maior ou menor orçamento, maior e menor efetividade e, mais recentemente, enfrentando crises de legitimidade perante a sociedade norte-americana (Cepik, Rodriguez, 2023). Porém, dado seu posicionamento geopolítico global, as pressões sistêmicas por maior efetividade e capacidade de atuação levou os EUA a construir um serviço complexo, com mecanismos de controle democrático existentes e com capacidade de atuação internacional (Cepik, 2007).

Nos países com menores ameaças externas, mas com contradições internas importantes, isto é, aqueles que passaram pela reconstrução do Estado, por processos revolucionários, transformações culturais

intensas ou, então, cruzaram por regimes políticos diferentes ao longo do século XX, apresentam configurações mais vinculadas a esses processos do que às ameaças externas. Isto não implica ignorar o contexto internacional, mas tais ameaças passam por um filtro interno decisivo.

Dessa forma as semelhanças e diferenças entre casos podem ser apontadas para exemplificar como contextos nacionais distintos levam a resultados distintos, isto é, temos um duplo efeito principal a ser destacado nesta comparação. O principal argumento exposto no presente capítulo é que no atual momento das relações internacionais há aumento da percepção de insegurança internacional por todos os atores, mas ela é percebida de diferentes formas pelos Estados em função de seu poder no sistema internacional e de sua posição regional. Essas ameaças serão também percebidas de formas distintas por cada contexto nacional, ou seja, os diferentes regimes políticos e governos percebem ameaças de forma distinta. Isso implica em resultados institucionais diferentes entre os países. Para esse fim, serão comparados casos em que há variações entre nível de poder global (grandes potências e potências regionais, por exemplo), variações de regimes políticos entre elas (autocracias, democracias e *accountability*) e variações no grau de relevância dos serviços de informação (maior ou menor orçamento destinado, por exemplo). Os casos exemplares que contemplam todos esses elementos são Estados Unidos, China e Brasil.

2. Dados e Mensurações

No sistema internacional da segunda década do novo milênio, em sua configuração mais recente, destacam-se em termos militares e econômicos países diferentes em função do critério utilizado para essa "contabilidade". Ao medir poder pela ótica realista estrutural, podemos considerar o poder militar e econômicos como principais (Waltz, 1979), porém, há diferentes formas de contabilização do poder ma-

material dos Estados. Agregados econômicos e militares são os mais usuais na literatura de relações internacionais (Beckley, 2018), mas tal qual usamos critérios específicos para diferenciar da melhor forma uma autocracia de uma democracia, podemos elencar alguns deles para identificar melhor os casos e seus dados.

No caso das variáveis de poder estrutural, costumam figurar o produto interno bruto do país, seu potencial econômico, isto é, consumo de ferro, aço e energia, além de métricas relativas ao investimento em R&D (Brooks & Wohlforth, 2006). Por essa razão, muitos estudos na área utilizam índices que sintetizam esses fatores em um indicador único, como, por exemplo, o Índice Composto de Capacidades Nacionais (CINC) do "*Correlates of War Program*" da Universidade de Michigan. Mais recentemente, outros autores apontam que métricas de poder agregado econômico permitem identificação mais precisa da quantidade de grandes potências que um dado momento histórico possui, como é o caso da proposta feita por Michael Beckley (2018). Com a mesma lógica de mensurar poder material com alguma fidedignidade e associar a esse poder outros fatores que derivam do poder não material ou brando, o Lowy Institute criou o *Asia Power Index*, que inclui os países da Ásia e aqueles considerados que são banhados pelo Oceano Pacífico, como os Estados Unidos.

Por outro lado, ainda mais específico, outros autores mais voltados para os Estudos Estratégicos optam por identificar capacidades críveis dos Estados, por exemplo, em âmbito militar, no qual possuir capacidade nuclear de segundo ataque é critério importante (Lodal *et al.*, 2010), além de ter em suas capacidades estratégicas a tríade estratégica, isto é, bombardeiros estratégicos, lançadores de mísseis balísticos intercontinentais (ICBM) e submarinos nucleares com capacidade nuclear (Lieber; Press, 2006). Nesse sentido, a cada passo novo na direção da sofisticação do dado a ser usado, mais complexa fica a definição de quais são os atores mais poderosos e qual lugar ocupam os que estão abaixo, as potências médias e regionais. Por essa ra-

zão, os índices são bastante usuais, e faremos uso de dois principais para diferenciar e aproximar os casos. Especificamente, aproximar as grandes potências e diferenciar das potências regionais. Os dados do CINC e do *Asia Power Index* serão usados para demonstrar essas diferenças. Já os dados do *Military Balance* e do *Nuclear Notebook* serão usados para demonstrar o potencial estratégico dos Estados e, conseqüentemente, o quanto são capazes de ameaçar outras grandes potências, vizinhos e potências regionais.

Os dados, então, demonstrarão o papel que desempenham e o quanto são ameaçados ou ameaçam outros Estados. É dessa forma que a primeira variável ficará empiricamente demonstrada. Esses dados serão cotejados com os oriundos dos regimes políticos dos Estados analisados, que são relevantes porque permitem identificar como a ameaça é percebida. Essa percepção pode se dar por um conjunto de instituições democráticas com suas responsabilidades e responsabilizações claras ou por instituições menos transparentes, em que o filtro sobre a vulnerabilidade externa pode estar mais vinculado à percepção de um grupo e de setores específicos da sociedade. Por isso, os dados sobre *accountability* derivados do V-Dem Institute (*Varieties of Democracy*) são os mais indicados.

É importante ressaltar que, assim como o debate sobre mensuração de poder material, no campo das relações internacionais e da política comparada temos distintas formas de medir regimes políticos e suas características (Coppedge, 2020; Munck, 2009; Przeworski, 1999). O debate sobre critérios minimalistas e maximalistas para definir democracia norteia o debate sobre os indicadores principais para identificação de regimes políticos. O V-Dem dialoga com esses dois e nas suas matrizes possui dados agregados sobre regime político em geral e sobre critérios específicos para avaliação da qualidade ou característica de cada regime. Esses dados são relevantes porque permitem avaliar o resultado em termos de gastos em defesa e inteligência conseqüente da ameaça e da interpretação.

Cabe ressaltar que os gastos em defesa serão sempre aproximados e estimados em função das declarações oficiais dos governos e que os gastos com serviços de inteligência são opacos e raramente divulgados com exatidão. Por isso, para fins de comparação entre os casos, este gasto será considerado como uma porcentagem fixa dos gastos em defesa do Estado. Tomando os Estados Unidos como balizador dessa métrica, os dados recentes do Congresso norte-americano sobre os gastos com a comunidade de inteligência apontam que os gastos oscilaram ao longo dos últimos 10 anos de 8% a 10% dos gastos em defesa. Considerando o tamanho do aparato norte-americano de inteligência (número de órgãos vinculados) e suas prerrogativas de ação internacional, podemos considerar os gastos dos EUA como o “teto” de gastos em inteligência. Assim, uma medida não ideal, mas que pode servir para comparação entre os casos, é considerar estimativas que oscilem entre 5% e 10% do gasto em defesa de cada caso.

Ademais, como forma de comparar esses casos exemplares, serão operados dados relativos aos regimes políticos e suas variações recentes, em conjunto com os dados sobre poder material e gastos em inteligência, que permitem identificar se nos momentos em que os gastos se elevam ou diminuem existe coincidência com variações nos regimes. Isso é relevante para identificar cenários possíveis em função das tendências de autocratização ou democratização desses países. O projeto V-Dem possui bancos de dados extensivos sobre os casos e permite a comparação entre eles, contudo, não possui dados sobre transições para democracia ou autocracia. Por isso, os dados principais que permitem identificar capacidade nacional e capacidade de atuação frente à sociedade são sobre poder de atuação do poder executivo.

3. Casos Exemplares

Estados Unidos

a. *Capacidade de Projeção de Poder Global*

Os Estados Unidos possuem grande capacidade de projeção de força nas relações internacionais. Ao considerarmos as métricas agregadas de poder material, figuram no topo dos principais *rankings* de poder. Se considerarmos os atributos de poder militar, teremos os seguintes dados: (1) maior orçamento de defesa (cerca de 905 bilhões de dólares, segundo o *Military Balance 2024*); (2) orçamento maior que a soma dos quinze maiores orçamentos de defesa do mundo; (3) tríade estratégica operacional; (4) domínio do espaço; (5) maior número de porta-aviões, destróieres, corvetas e fragatas; (6) maior número de submarinos estratégicos; (7) maior número de submarinos nucleares não estratégicos; (8) maior número de satélites para IRS (*Intelligence, Reconnaissance and Surveillance*) (The Military Balance, 2020, 2021, 2022, 2023, 2024).

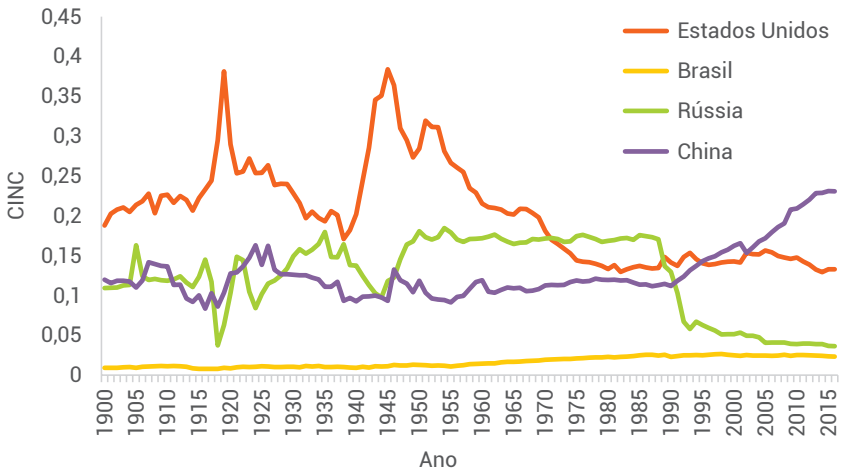
Esses atributos colocam os Estados Unidos, em termos militares, em posição mais alta que os concorrentes. Apenas em alguns aspectos é superado pela China e pela Rússia. Pela China, é superado no tamanho das forças armadas (número de pessoal) e pela Rússia no número de ogivas e mísseis balísticos declarados. Com isso, os Estados Unidos possuem (a) a maior capacidade de defesa do mundo e, ao mesmo tempo, (b) a maior capacidade ofensiva do mundo (Mearns, 2021; Chang, 2023). Isto implica em ser ao mesmo tempo (a) o ator com menor chance de ser atacado por potências rivais e (b) o ator considerado mais ameaçador pelos rivais. Por conseguinte, esses dois fatores afetam decisivamente a demanda por serviços de inteligência eficientes e legitimados dentro do Estado, pois quando o ataque militar real tem sua probabilidade diminuída, dada a capacidade dissuasória do Estado, as ameaças são alternativas e envolvem

ações militares encobertas e não militares que podem produzir danos ao Estado. Por essa razão, as atividades de contrainteligência são essenciais àquele país e integram grande parte do corpo das ações de inteligência norte-americanas.

Ao considerarmos os dados do CINC e do *Asia Power Index*, podemos verificar o posicionamento atual dos EUA frente aos principais rivais estratégicos. Abaixo constam os dados do Índice Composto de Capacidades Nacionais, que demonstra queda do poder relativo dos EUA frente à China, por exemplo. Isto decorre das componentes do índice, que sobrepesam tamanho das forças armadas, tamanho da população e consumo de energia da população (Beckley, 2018), mas subdimensiona os detalhes da capacidade estratégica norte-americana, que pode ser verificada em mais detalhe no *Asia Power Index*.

Gráfico 1

Comparação CINC de 1900 a 2015: Brasil, Estados Unidos, Rússia (União Soviética) e China.



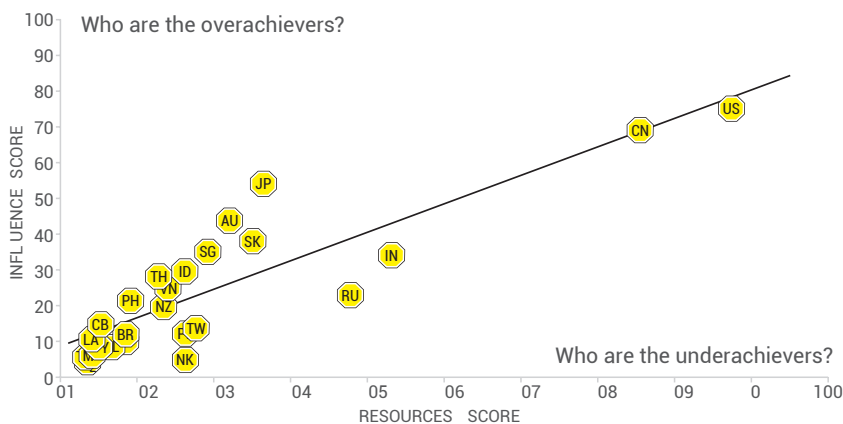
Fonte: Adaptado de Correlates of War, 2016

Esses dados demonstram o crescimento do poder material chinês no início dos anos 2000 e a queda no poder material da Rússia após a dissolução da União Soviética. Também demonstra a estabilização do poder material dos Estados Unidos. Esta é uma métrica de tendência que revela bem a emergência chinesa e a perspectiva de uma redistribuição de poder no sistema internacional, que, por sua vez, pode promover reconfiguração de polaridades. Essa reconfiguração afeta decisivamente as preocupações dos Estados com ameaças externas, pois é neste contexto que o sistema de alianças e confiança mútua se redefine (Walt, 2009).

Ao considerarmos os dados do *Asia Power Index*, especificamente o Índice de Diferença de Poder (*Power Gap*) entre os Estados analisados, os dados apontam para este cenário atual:

Figura 1

Índice de Diferença de Poder



Fonte: Asian Power Index, 2024

A disputa mais importante em termos de poder militar e econômico parece delimitada para os próximos anos, concentrando-se na relação entre China e Estados Unidos, com a Rússia e a Índia como potenciais grandes potências em (re)ascensão. Isso tem implicações im-

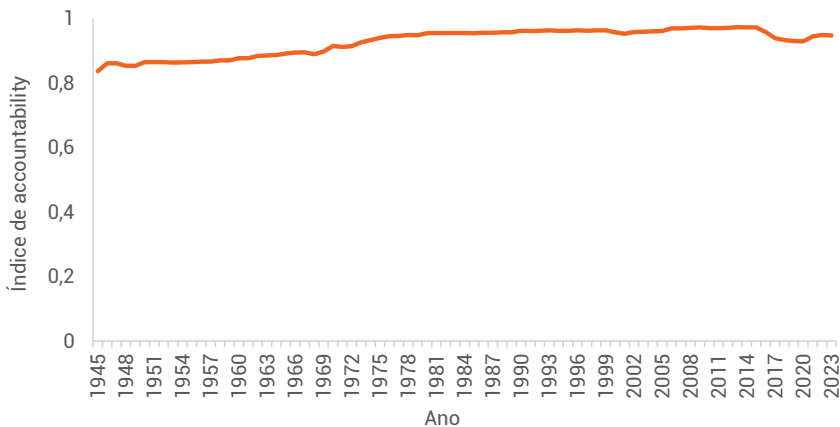
portantes para os serviços de inteligência, ou seja, serão os serviços desses países os que mais demandarão recursos e capacidades de ação nos próximos anos, com continuidade na dotação orçamentária e estrutura institucional no lado norte-americano, e crescimento no lado chinês. Essa conjuntura crítica pode produzir pressões sobre manutenção no controle democrático das ações por parte da sociedade norte-americana, que já vivenciou pressões por “livrar” os serviços de inteligência das amarras institucionais em momentos anteriores de sua história. Por exemplo, na chamada Segunda Guerra Fria, sob comando de Ronald Reagan (1981-1989), que ampliou o poder de atuação da comunidade de inteligência dos Estados Unidos sem que controles democráticos fossem estabelecidos na mesma velocidade (Cepik; Rodriguez, 2023).

b. Regime

Os dados sobre mudança de regime político ou sua estabilidade permitem verificar momentos de crise do regime e momentos em que os mecanismos de controle democrático funcionam com maior efetividade. Entretanto, em democracias consolidadas e que contam com histórico de estabilidade, as variações nos indicadores são pequenas, o que não implica insignificância. Nos índices abaixo, podemos perceber as mudanças no *accountability* nos Estados Unidos, com variações menores mas que se relacionam com contextos específicos, por exemplo, as variações para “baixo” no início dos anos 2000 se referem às ações derivadas da Guerra ao Terror dos EUA, com reformas internas, como a criação do DHS (*Department of Homeland Security*) e o estabelecimento do *Patriot Act*, que ampliou a capacidade de vigilância dos órgãos de segurança da sociedade norte-americana. Também os dados mostram os anos do Governo de Donald Trump, em que as ações na direção de aumentar a margem de manobra do governo sobre temas de segurança foram ampliadas.

Gráfico 2

Índice de accountability dos Estados Unidos

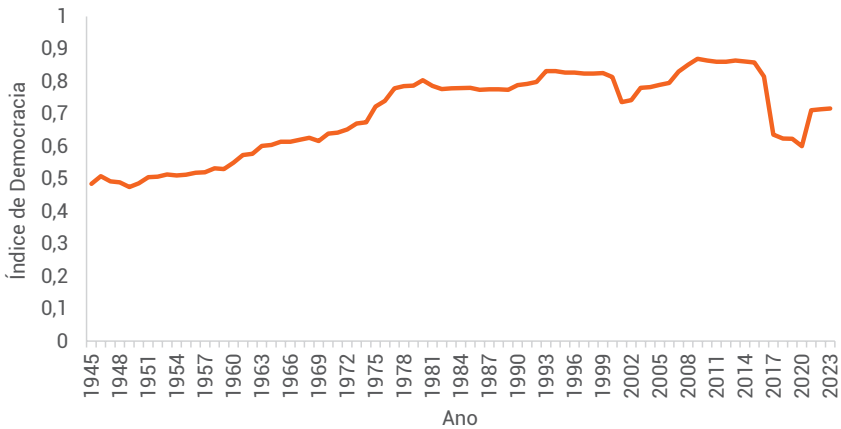


Fonte: Adaptado de V-Dem Institute, 2024

Abaixo estão os dados do *Deliberative Democracy Index*, do V-Dem, que permitem verificar estabilidade ou crise no regime. Quando há quedas no índice, há tendência de desdemocratização, e quando há aumento de valores pode ocorrer democratização ou reforço da democracia. Ademais, neste gráfico chama a atenção a queda nos valores em anos recentes, em que os ataques à democracia foram maiores e a crise chegou ao auge com a tentativa de golpe de Estado, com a tomada do Capitólio por apoiadores de Donald Trump na expectativa de reverter os resultados das eleições.

Gráfico 3

Índice de democracia dos Estados Unidos



Fonte: Adaptado de V-Dem Institute, 2024

Cabe destacar que a queda relativa nos indicadores de democracia e controles democráticos efetivos coincide com as mudanças estruturais reveladas pelo CINC e o *Asia Power Index*. Também coincide com o aumento nos gastos em defesa dos EUA e, conseqüentemente, com os gastos com inteligência, como demonstram os dados na próxima subseção.

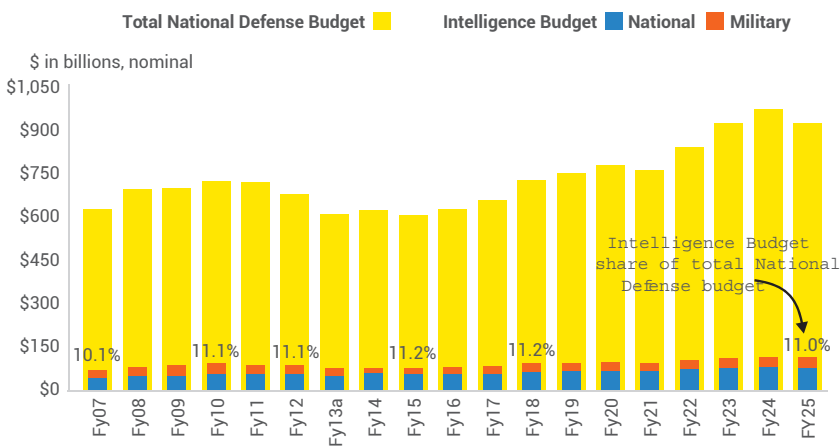
c. Gastos em Inteligência

A comunidade de inteligência dos Estados Unidos conta com investimentos de grande ordem e com continuidade ao longo do tempo. Os relatórios do Congresso e do Escritório do Diretor Nacional de Inteligência (ODNI) divulgam, com certo grau de transparência, o orçamento da comunidade de inteligência do país, que conforme gráfico abaixo, ficam em torno de 10-11% dos gastos em defesa do país, isto é, entre 70 e 100 bilhões de dólares. Como os gastos dos EUA em defesa superam muito os gastos declarados pelos demais países, estes cerca de 10% da defesa em inteligência significam os maiores gastos

em inteligência do mundo. Para ter essa monta superada pelos rivais, o orçamento deveria ser maior do que os gastos totais em defesa da China e Rússia. Isso resulta em grande capacidade de atuação nacional e internacional, embora não implique legitimidade e eficiência.

Figura 2

Comparação entre os gastos com Defesa e Inteligência nos EUA



Fonte: DEVINE; PLAGAKIS, 2024 e ODNI, 2024.

Os dados apresentados revelam os seguintes pontos: (1) os EUA é o ator com maior capacidade militar agregada e maior orçamento de defesa; (2) possui o maior orçamento em inteligência; (3) conta com o regime político mais estável, com alterações pequenas ao longo da série histórica (desde o final da segunda guerra mundial); e (4) apresentaram déficits de *accountability* em momentos em que coincidem pressões externas por maior disputa estratégica ou resposta norte-americana com projetos governamentais de menor comprometimento com controles democráticos sobre as ações do poder executivo, conforme os dados do índice de *accountability*.

China

a. *Capacidade de Projeção de Poder Regional/Global*

A China apresentou a maior ascensão de poder material do milênio. Conforme os dados do CINC na figura abaixo, apresenta poder nacional agregado superior ao dos Estados Unidos, algo contestado pelos estudos de Brooks & Wohlforth (2006) e Beckley (2018), tanto por não mensurar capacidade de investimento em R&D, patentes e potencial de inovação pelos primeiros autores, quanto pelo fato de o CINC sobrepesar renda agregada e potencial latente do Estado, como é o caso da vasta população. Apesar dessas considerações, todos os índices disponíveis de poder material apontam para o crescimento de poder, para o aumento da capacidade chinesa de projetar poder para além de sua região. A capacidade de projeção de força para além da região se vincula a dois pontos principais: (1) ao desenvolvimento de mísseis nucleares de alcance intercontinental, com mobilidade ou instalação em silos próximos à Ásia Central (Kristensen et al., 2024) e (2) aos recentes desenvolvimentos de sua força naval (McDevitt, 2020).

Esses novos contornos do poder militar chinês, associados ao poder econômico crescente, produziram ao longo dos últimos 20 anos o que a literatura de relações internacionais considerou como redistribuição de poder. Mearsheimer (2021) aponta que a rivalidade inevitável veio para moldar o futuro da polaridade do sistema internacional. A partir dessas considerações, podemos identificar que a China possui capacidade de projeção de poder global em crescimento e definitiva capacidade de projeção de força regional. Por isso, é potência que percebe cada vez mais (à medida que cresce) a ameaça norte-americana, motivo pelo qual adota estratégias de *Anti-access/Area Denial* (A2/AD) com efetividade (Biddle; Oerlich, 2016; Beckley, 2017) e projeta seu poder sobre a região, o que afeta a percepção dos vizinhos. A consequência é que a China necessita de serviços de inteligência capazes de fazer contrainteligência no nível sistêmico e de lidar com produção

de conhecimento sensível para tomada de decisão na relação com os vizinhos.

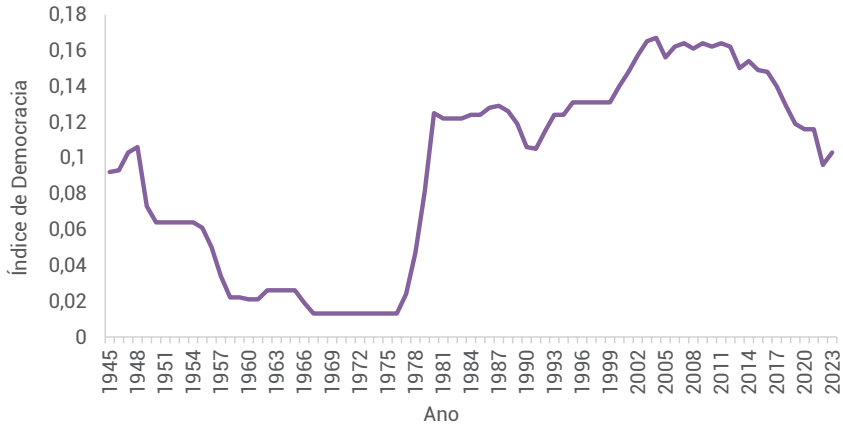
b. Estabilidade do Regime

Após a Revolução Chinesa (1949), a Proclamação da República Popular da China (RPC) vem acompanhada de uma série de processos de centralização política. A radicalização no início do processo de construção da república aparece no gráfico abaixo, em que o Índice de Democracia se altera para um nível ainda mais baixo entre 1949 e o final dos anos 80, que coincidem com o final da Era de Mao Tse-tung à frente da China. Após esse período, a China passa por grandes transformações internas, principalmente econômicas e políticas na base da sociedade, com a diversificação ampla da economia e das contradições sociais. O grande desenvolvimento econômico das últimas três décadas não alterou de forma significativa como o regime é avaliado pelo ocidente, conforme o gráfico abaixo aponta. Cabe destacar que nesse período, apesar das transformações econômicas, não ocorreram mudanças nas características eleitorais do regime, o que para este tipo de índice é indicador crucial.

A grande estabilidade política chinesa é ao mesmo tempo indicador importante sobre tomada de decisão estatal sobre segurança e defesa e indicador de centralidade política autocrática. Na competição interestatal, o tipo de regime diz pouco sobre como os Estados se comportam, segundo, por exemplo, autores realistas (Waltz, 1979). Porém, pode revelar capacidade de manter projetos de força de longo prazo de forma distinta de outras potências emergentes.

Gráfico 4

Índice de democracia da China

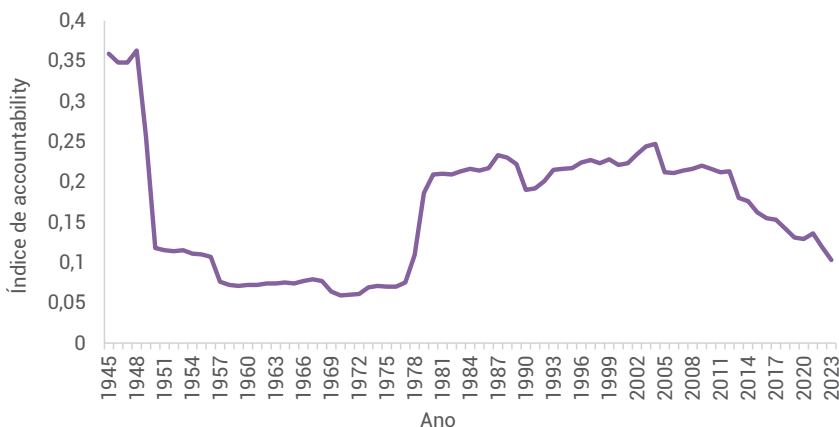


Fonte: Adaptado de V-Dem Institute, 2024

Apesar do centralismo, há variações importantes no índice de *accountability*, que permitem verificar os períodos de menor responsividade do governo, maior capacidade de atuação do executivo sem qualquer mecanismo de controle social (horizontal ou vertical). No gráfico abaixo pode-se perceber que o período da “Era Mao” se caracterizou por níveis muito baixos de *accountability*, que marcaram o endurecimento do regime sob a gestão de Mao Tse-tung. A transição para o período de Deng Xiaoping foi acompanhada de moderação na política interna e reformas que permitiram maior controle social, principalmente pelo Partido Comunista Chinês, e garantiram a seus milhares de membros algum poder decisório. O gráfico também demonstra que o crescimento chinês dos últimos períodos é acompanhado de diminuição dessa capacidade de controle e de aumento do poder do executivo nas decisões.

Gráfico 5

Índice de accountability da China



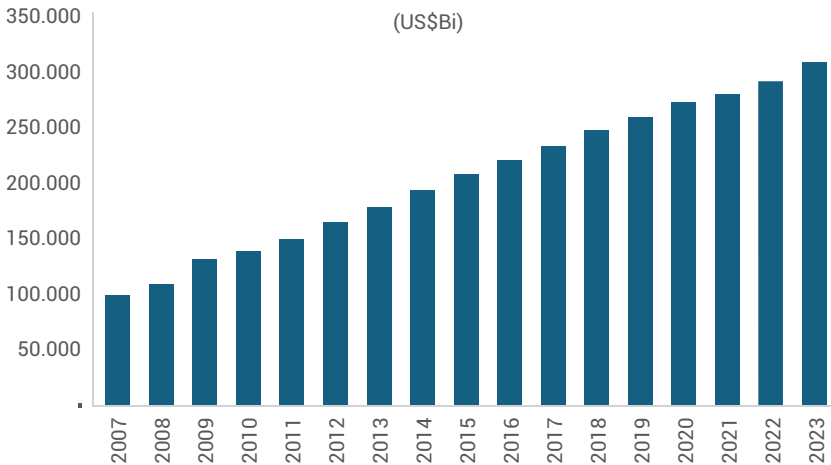
Fonte: V-Dem Institute, 2024

c. Gastos Inteligência

Os dados sobre gastos em inteligência da China não são conhecidos, por isso, neste trabalho, adotamos a medida de porcentagem dos gastos em defesa como métrica aproximada dos gastos em inteligência. Considerando os gastos norte-americanos em cerca de 10% dos gastos em defesa, o orçamento chinês para inteligência seria 1/3 dos gastos norte-americanos, ou seja, entre 20 e 30 bilhões de dólares. Esse orçamento pode conferir, por exemplo, ao Ministério da Segurança do Estado (MSS) grande capacidade de atuação. As reformas pós-Era Mao criaram este ministério com a finalidade de fazer inteligência civil na RPC. Este ministério passou por fases distintas e hoje possui capacidade de atuação compreensiva e proporcional ao *status* de poder da China (Chase & Mulvenon, 2002). Entre os setores que mais recebem recursos estão os ligados à segurança cibernética (Saade, 2020).

Figura 3

Gastos com Defesa da China



Fonte: SIPRI, 2024

Brasil

a. Poder de Projeção de Força Regional e Limitada

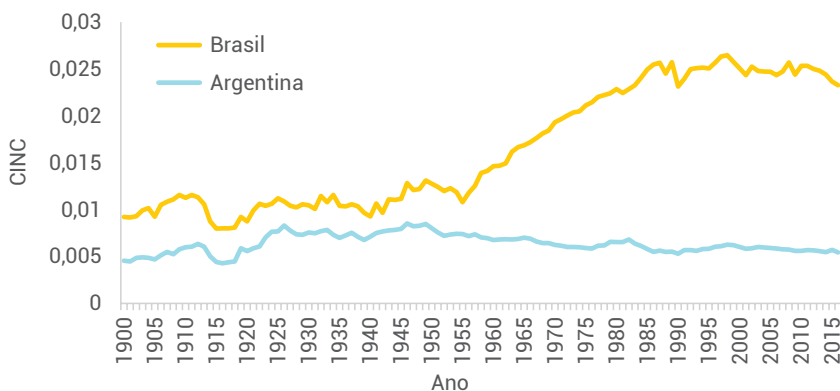
O Brasil apresentou, conforme gráfico abaixo, grande crescimento material, quando comparado com o vizinho com maior potencial da região, a Argentina. Ao comparar com grandes potências, o crescimento é menor e não produz efeitos sistêmicos consideráveis. Por isso, o crescimento do Brasil produz mais efeitos em termos de distribuição de poder e percepção de ameaça na região e entorno estratégico (Atlântico Sul). Desse modo, o país também percebe os atores regionais e hemisféricos com maior peso relativo do que atores com maior distância geopolítica, como China e Rússia. Desta forma, o crescimento de poder material do país está muito ligado ao crescimento econômico e à estabilidade política decorrente. Pouco desse crescimento recente está ligado ao aumento de poder militar. Entretanto, o país tem força suficiente para projetar força regionalmente

em pequena escala. As preocupações regionais são, portanto, as mais importantes para o país e para os serviços de inteligência nacionais.

O gráfico abaixo demonstra o grande crescimento do país durante seu processo de industrialização e posterior período de estabilidade num mesmo patamar do CINC (0,025).

Gráfico 6

Comparação CINC entre Brasil e Argentina (1900-2015)



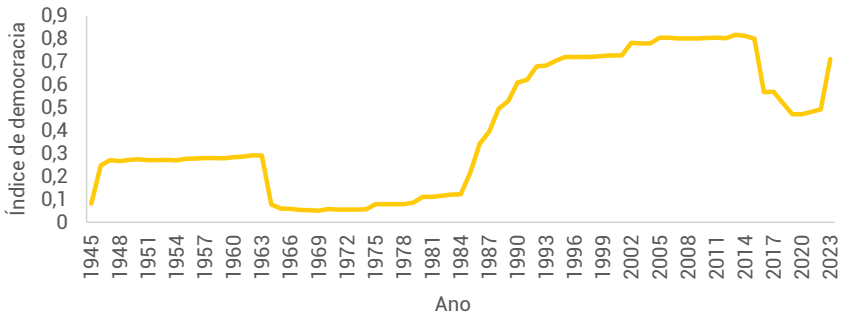
Fonte: Adaptado de Correlates of War, 2024

b. Regime

O Brasil apresentou grandes variações no regime político ao longo do século XX, o que difere crucialmente dos outros países avaliados anteriormente, passando por período longo de ditadura militar (1964-1985), redemocratização e estabilização democrática (1985-2015), crise da democracia (2015-2021) e retomada da democratização (Hunter & Power, 2019). O gráfico abaixo demonstra bem esses períodos, que coincidem com as mudanças também na capacidade de atuação de controles democráticos efetivos e maior força do poder executivo em áreas como segurança pública, forças armadas e inteligência (Rodriguez, 2023).

Gráfico 7

Índice de democracia do Brasil

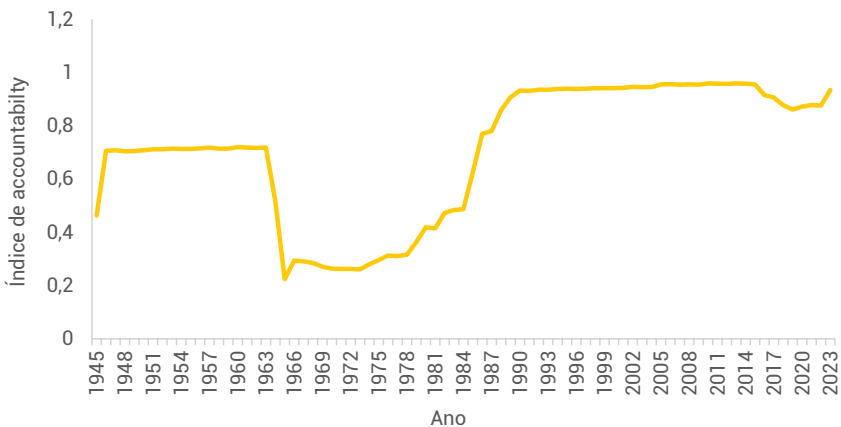


Fonte: Adaptado de V-Dem Institute, 2024

Os dados abaixo demonstram a forte coincidência entre o índice de democracia no Brasil, derivado do V-Dem, e o Índice de *accountability* ou responsividade do governo. As crises recentes envolvendo o SISBIN e os problemas relativos ao respeito aos controles democráticos pelo governo Bolsonaro, por exemplo, ficam identificadas na queda dos anos recente neste indicador.

Gráfico 8

Índice de *accountability* do Brasil



Fonte: Adaptado de V-Dem Institute, 2024

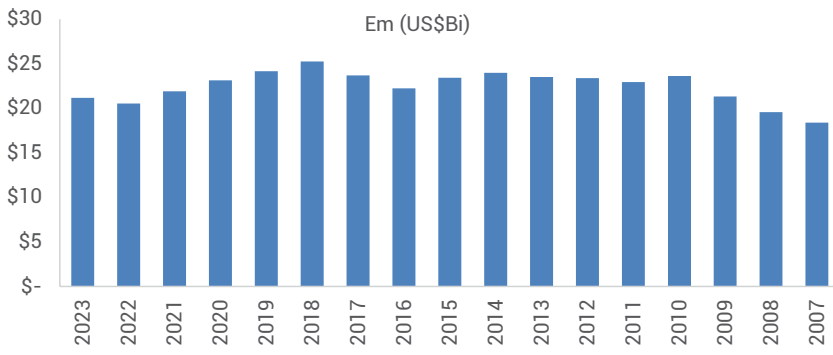
c. Gastos em Inteligência

Os gastos em inteligência do país são ainda mais limitados do que os anteriores, mesmo se considerarmos os gastos na ordem de 10% dos gastos em defesa ou seja, deveriam estar na ordem de 2 a 3 bilhões de dólares. Esse orçamento em Inteligência seria relativo ao SISBIN como um todo, incluindo os órgãos responsáveis por inteligência militar e policial, não se limitando ao orçamento de sua agência central, a ABIN. Mesmo considerando dessa forma, esse orçamento representaria menos de 1/10 do que a China gasta com Inteligência. Esses dados servem para demonstrar a diferença existente entre potência com maior poder, potência competidora em ascensão e potência regional com poder limitado.

A ABIN há anos passa por instabilidade orçamentária. No início de 2024, a previsão de orçamento discricionário daquele ano era R\$127 milhões. Entretanto, após os cortes orçamentários em todo governo federal em agosto, a Agência passou a contar com orçamento de cerca de R\$ 69 milhões, o menor dos últimos sete anos (Megale, 2024). Portanto, se traduz em capacidade bastante reduzida de atuação para prover segurança estatal, o que coloca o Brasil em situação de vulnerabilidade diante da crescente instabilidade internacional advinda da competição estratégica entre grandes potências e de um cenário regional e interno cada vez mais desafiador, com o crescimento de ameaças não tradicionais, como o crime organizado e movimentos antidemocráticos.

Gráfico 9

Gastos em Defesa do Brasil



Fonte: Adaptado de SIPRI, 2024

Considerações Finais: comparando contextos e capacidades

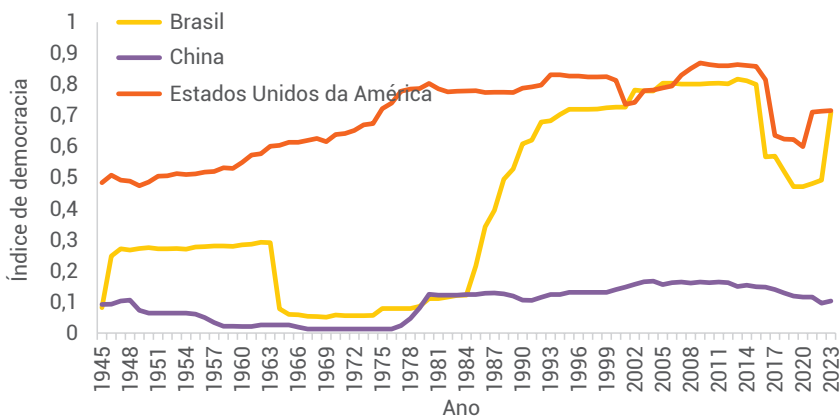
Comparando as três dimensões, podemos apontar que as capacidades são obviamente distintas e, portanto, os desafios também. Além disso, as capacidades de projeção de força, percepção e causa de ameaça são distintas, e enquanto EUA e China projetam força globalmente e regionalmente, o Brasil apenas regionalmente de forma limitada. EUA e China percebem-se como ameaças mútuas, porém, a China percebe os EUA como mais ameaçador devido ao volume de capacidades. Isso produz efeitos diretos sobre a necessidade de serviços de inteligência efetivos, isto é, quanto mais demanda, maior a percepção de necessidade e de utilidade dos serviços para o Estado. A competição interestatal, portanto, tem papel crucial no desenvolvimento e na capacidade desses serviços estatais.

Ademais, os regimes variam muito pouco nos grandes atores e muito no Brasil, o que implica em estabilidade política, mesmo que artificial ou pela força, com algum grau de legitimidade interna. A estabilidade política permite a constituição de serviços que contam com maior capacidade de ação, com ou sem controles democráticos efetivos.

Por fim, o *accountability* desses Estados varia mais do que os outros componentes, o que indica que o poder executivo não necessariamente possui total controle dos setores de segurança. Variam as contradições internas, variam as capacidades de ação com legitimidade interna e, portanto, variam os indicadores de *accountability*. Os gráficos abaixo demonstram bem essas características.

Gráfico 10

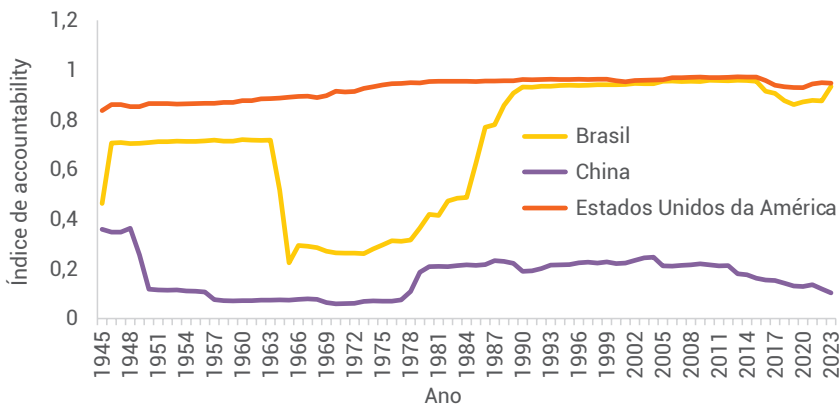
Comparação entre os índices de democracia de Brasil, EUA e China



Fonte: Adaptado de V-Dem Institute, 2024

Gráfico 11

Comparação entre os índices de accountability de Brasil, EUA e China



Fonte: Adaptado de V-Dem Institute, 2024

Os contextos nacionais, portanto, variam externa e internamente, em termos de poder, de regime e de responsividade. As implicações dessas variações não são exaustivas, mas indicam que regimes que variam mais enfrentam maior dificuldade de construção de serviços efetivos e legítimos, pois rupturas e reformas contínuas os afetam. Por outro lado, Estados com maior projeção e desafios organizam serviços maiores e com maior recurso, o que não necessariamente implica em efetividade e legitimidade, pois as crises ocorrem também em momentos cruciais, como foi o caso do 11 de Setembro nos Estados Unidos.

As métricas sobre eficiência, portanto, referem-se mais à capacidade estrita dos serviços, que por sua vez se ligam aos orçamentos, mas não somente. Por outro lado, as métricas de legitimidade referem-se ao quão legítimas são as ações frente à sociedade. Nesse caso, as sociedades muito consolidadas democraticamente ou muito estáveis autocraticamente possuem maior legitimidade, real ou artificial. Enquanto o caso do Brasil demonstrou que variações de regime, crises econômicas e de *accountability* afetam a eficiência e a legitimidade dos serviços. Por se tratar de serviços de segurança do Estado, por fim, estes elementos podem estar ligados mais ao quanto de ameaça sentem e produzem do que por contextos nacionais específicos.

Enfim, isso produz efeitos diretos sobre os investimentos em inteligência de potências regionais como o Brasil. Por não estarem envolvidas diretamente nas disputas estratégicas mais importantes ao nível sistêmico, seus serviços de inteligência, a exemplo da ABIN, podem sofrer perda de capacidades operacionais, perda de relevância e podem não conseguir executar, em função de limitações orçamentárias, os objetivos constitucionais para os quais foram criados. Além disso, podem não conseguir construir legitimidade e efetividade no mesmo patamar dos serviços congêneres das grandes potências.

Referências

AGRELL, W.; TREVERTON, G. F. **National intelligence systems: current research and future prospects**. Cambridge: Cambridge University, 2009.

ANDREGG, M. M.; GILL, P. Comparing the democratization of intelligence. **Intelligence and National Security**. v.29, n.4, p.487-497, 2014.

BECKLEY, M. The emerging military balance in east asia: How china's neighbors can check chinese naval expansion. **International Security**, v.42, n.2, p.78-119, 2017.

BIDDLE, S.; OELRICH, I. Future warfare in the Western Pacific: Chinese antiaccess/area denial, US airsea battle, and command of the commons in East Asia. **International Security**, n.41, v. 1, p.7-48, 2016.

CEPIK, M. **Espionagem e democracia**. Rio de Janeiro: Editora FGV, 2003.

CEPIK, M. Regime político e sistema de inteligência no Brasil: legitimidade e efetividade como desafios institucionais. **DADOS**. v. 48, n. 1, p. 67-113, 2005.

CEPIK, M. Structural change and democratic control of intelligence in Brazil. In: BRUNEAU, T; BORAZ, S. **Reforming intelligence: obstacles to democratic control and effectiveness**. Austin: University of Texas Press, 2007. p. 149-169.

CEPIK, M.; AMBROS, C. Intelligence, crisis and democracy: institutional punctuations in Brazil, Colombia, South Africa and India. **Intelligence and National Security**. v. 29, n. 4, p. 523-551, 2014.

CEPIK, M.; MÖLLER, G. National Intelligence Systems as Networks: Power Distribution and Organizational Risk in Brazil, Russia, India, China, and South Africa. **Brazilian Political Science Review**, v. 11, n. 1, 2017. <https://doi.org/10.1590/1981-3821201700010001>.

CHANG, J. Y. Of Risk and Threat: How the United States Perceives China's Rise, **The Chinese Journal of International Politics**, v.16, n.3, p.357-381, 2023. <https://doi.org/10.1093/cjip/poad010>.

CHASE, M; MULVENON, J. The Decommmercialization of China's Ministry of State Security, International. **Journal of Intelligence and CounterIntelligence**, v. 15, n. 4, p. 481-495, 2002. DOI: 10.1080/08850600290101730.

CORRELATES OF WAR. Composite Indicator of National Capability. National Material Capabilities, 2024. Disponível em: <https://correlatesofwar.org/data-sets/national-material-capabilities/>. Acesso em: 06/11/2024.

DEVINE, M; PLAGAKIS, S. Intelligence Community Spending Trends. **Congressional Research Service**, 2024. Disponível em: <https://crsreports.congress.gov/product/pdf/R/R44381>. Acesso em: 06/11/2024.

ESTÉVEZ, E. Comparing intelligence democratization in Latin America: Argentina, Peru and Ecuador cases. **Intelligence and National Security**. v. 29, n. 4, p. 552-580, 2014.

GILAD, A.; PECHT, E.; TISHLER, A. Intelligence, Cyberspace, and National Security. **Defence and Peace Economics**, v. 32, n. 1, p. 18-45, 2020. <https://doi.org/10.1080/10242694.2020.1778966>.

GILL, P. **Policing politics: security intelligence and the liberal democratic state**. New York: Routledge, 1994.

GILL, P. Evaluating intelligence oversight committees: the UK intelligence and security committee and the 'war on terror'. **Intelligence and National Security**. v. 22, n. 1, p. 14-37, 2007.

GILL, P.; PHYTHIAN, M. What is intelligence studies?. **The International Journal of Intelligence, Security, and Public Affairs**. v. 18, n. 1, p. 05-19, 2016.

HERMAN, M. **Intelligence power in peace and war**. Cambridge: University Press, 1996.

IISS. The Military balance 2020. International Institute for Strategic Studies: 2020.

IISS. The Military balance 2021. International Institute for Strategic Studies: 2021.

IISS. The Military balance 2022. International Institute for Strategic Studies: 2022.

IISS. The Military balance 2023. International Institute for Strategic Studies: 2023.

IISS. The Military balance 2024. International Institute for Strategic Studies: 2024.

JAFFEL, H. B.; LARSSON, S. Why Do We Need a New Research Agenda for the Study of Intelligence?. **International Journal of Intelligence and CounterIntelligence**, v. 37, n. 2, p. 727-750, 2024. DOI: 10.1080/08850607.2023.2222342.

JOHNSON, L.K; SCHEID, K.J. Spending for Spies: Intelligence Budgeting in the Aftermath of the Cold War. **Public Budgeting & Finance**, v. 17, p. 7-27, 1997. <https://doi.org/10.1111/1540-5850.01114>.

KRISTENSEN, H. M.; KORDA, M.; JOHNS, E.; KNIGHT, M. Chinese nuclear weapons. **Bulletin of the Atomic Scientists**, v. 80, n. 1, p. 49–72, 2024. <https://doi.org/10.1080/00963402.2023.2295206>.

LIEBER, K. A.; PRESS, D. G. The end of MAD? The nuclear dimension of US primacy. **International Security**, v. 30, n. 4, p. 7-44, 2006.

LOWENTHAL, M. **Intelligence: from secrets to policy**. Thousand Oaks: CQ Press. Sixth edition, 2015.

MANGER, G. **Unravelling effectiveness in intelligence: a systematic review**, **Intelligence and National Security**, 2024. DOI: 10.1080/02684527.2024.2370132.

MCDEVITT, M. **China as a Twenty-First Century Naval Power. Theory, Practice and Implications**. Annapolis: Naval Institute Press, 2020.

MEARSHEIMER, J. J. The inevitable rivalry: America, China, and the tragedy of great-power politics. **Foreign Affairs**. v.100, n.48, 2021.

MEGALE, B. Cortes no orçamento travam operações da Abin e atuação no G20. **O Globo**. 13 set. 2024. Disponível em: <https://oglobo.globo.com/blogs/bela-megale/post/2024/09/cortes-no-orcamento-travam-operacoes-da-abin-e-atuacao-no-g20.ghtml>. Acesso em: 06/11/2024.

MICHAEL B.; The Power of Nations: Measuring What Matters. **International Security**, v.43, n.2, p.7–44, 2018. https://doi.org/10.1162/isec_a_00328.

ODNI. U.S. Intelligence Community Budget. **DNI, 2024**. Disponível em: <https://www.dni.gov/index.php/what-we-do/ic-budget>. Acesso em: 06/11/2024

PECHT, E.; TISHLER, A. Budget allocation, national security, military intelligence, and human capital: a dynamic model. **Defence and Peace Economics**, v. 28, n. 3, p. 367–399. 2015. <https://doi.org/10.1080/10242694.2015.1101885>.

SIPRI. SIPRI Yearbook 2024. **Stockholm International Peace Research Institute**, 2024. Disponível em: <https://www.sipri.org/yearbook/2024>. Acesso em: 06/11/2024.

V-DEM INSTITUTE. Democracy Report 2024. **Varieties of Democracy**, 2024. Disponível em: https://www.v-dem.net/documents/43/v-dem_dr2024_lowres.pdf. Acesso em: 06/11/2024.

ZEGART, A. B. **Flawed by design: the evolution of the CIA, JCS, and NSC**. Stanford: Stanford University Press, 1999.



Democracia e inteligência estatal: Caminhos para o Controle no Contexto Brasileiro

Rodrigo Ribeiro Bedritichuk

Analista Legislativo do Senado
Secretário da Comissão Mista de Controle
das Atividades de Inteligência (CCAI)

Se a função primordial de todo Estado é a proteção de seus cidadãos, então a Atividade de Inteligência estatal terá sempre relevância, qualquer que seja a época ou o contexto. Obter dados negados, reunir informações e processá-las de modo a auxiliar a decisão dos governantes, antecipar movimentos inimigos – todas essas ações no campo da inteligência sempre foram praticadas onde quer que se ache o poder político.

A inteligência, assim, cumpre quatro funções essenciais de todo Estado, conforme apontado por Born (2004): previne ataques surpresa, confere visão de longo prazo, auxilia o processo decisório e resguarda o sigilo de informações, meios e métodos.

É sobretudo na guerra que a inteligência cresce e se torna um diferencial, um campo de batalha invisível que pode se tornar decisivo. Foi justamente na II Guerra Mundial que os modernos serviços de inteligência estatal foram estruturados. Terminado o conflito armado, entretanto, o mundo se viu dividido num cenário bipolar tensionado de constante conflito por esferas de influência. Na Guerra Fria, batalhas entre soldados, apesar de eclodirem aqui e acolá com o apoio de EUA

e URSS, foram, no mais das vezes, substituídas pela ação da inteligência estatal. Os serviços de inteligência dos países desenvolvidos se tornaram autônomos em relação ao esforço de guerra, tornando-se permanentes (Brandão, 2010).

Espionagem, informação e desinformação, novas técnicas e tecnologias fizeram que a CIA e a KGB entrassem no imaginário popular com certa aura mística. Mas não só elas. Nenhum Estado, seja ele de qualquer dos blocos, pôde prescindir de manter seu próprio aparato de inteligência. Stasi, SNI, MI6, Securitate podiam diferir quanto aos seus inimigos e objetivos finais, mas agiam muitas vezes de modo similar em suas atividades de inteligência. Inteligência estatal, aliás, que também é referida como “serviço secreto”, uma vez que o sigilo das ações é fundamental para garantir seus objetivos.

Mas o segredo atíça a curiosidade. O que um serviço secreto faz ao certo? E se é secreto, como saber se eles estão agindo corretamente? Não à toa, a população encara a inteligência com certa dualidade, ora vendo-a como atividade romântica de espiões e heróis, ora como uma bisbilhotice imoral (Ott, 2003).

Com o fim da Guerra Fria e a dissolução do bloco soviético em 1989, o temor de um conflito global esfriou. Em democracias consolidadas, o resultado foi uma desvalorização do setor de inteligência, com reduções drásticas de orçamento e pessoal (Turner, 2008). Somado a esse fato veio uma nova onda de democratização em vários países com passado autoritário, fazendo que o desmonte do aparelho de inteligência, quase sempre símbolo da repressão estatal, fosse um requisito para a democratização. Nesses casos, também o setor de inteligência foi desprestigiado e quase esquecido pelas novas lideranças políticas.

Os atentados de 11 de setembro em Nova Iorque, porém, marcaram uma inflexão global, fazendo que o mundo abrisse novamente os olhos para a importância de uma inteligência estatal bem aparelhada, além

da necessidade de cooperação internacional (Ott, 2003; Born, 2004). Afinal, para combater inimigos não estatais, como grupos terroristas e o crime organizado, novamente o soldado perde relevância diante do agente de inteligência. Assim é que, em contexto multipolarizado, com ameaças difusas e novas tecnologias, a inteligência reassume papel de relevo no século XXI.

Colocam-se aí dois desafios que os Estados têm à frente. O primeiro é montar um sistema de inteligência eficiente, que cumpre sua missão primordial de garantir a proteção dos cidadãos e se antecipar a ameaças. O segundo é fazer que esse sistema possa agir dentro de uma moldura democrática, respeitando direitos e garantias individuais. Nesse sentido, parece haver uma dicotomia por vezes insolúvel. Muitos dizem que inteligência e democracia são antagônicos, o que faz o desafio ainda maior. Com efeito, até pouco tempo atrás, democracias consolidadas possuíam aparelhos de inteligência que operavam às margens da lei, e escândalos no setor são noticiados pela mídia ainda hoje. Será mesmo possível um controle democrático da inteligência?

O presente trabalho analisa essa questão, enfatizando o controle da inteligência em contextos de transição democrática e analisando o caso do Brasil. Após compulsar a literatura que demonstra as dificuldades em exercer controle efetivo da inteligência depois de um passado autoritário, o trabalho discorre sobre o caso brasileiro. Apesar de importantes passos terem sido dados na estruturação do controle de inteligência, muito ainda falta para que o país possa contar com um controle efetivo e atuante, requisito para a consolidação democrática. Antes, portanto, de discutir a eficiência dos serviços de inteligência no Brasil, é preciso avançar de forma concreta na temática do controle democrático, conforme se verá a seguir.

1. Seguindo o passo de espões

No auge da Guerra Fria, a CIA agia quase sem controle para fazer avançar os interesses americanos mundo afora. No Congresso, muitos parlamentares preferiam a abordagem de “colocar a cabeça em um buraco” e “deixar que honrados homens da CIA fizessem seu trabalho” (Johnson, 2008). A tática tinha também a vantagem de preservar as negativas plausíveis dos parlamentares em caso de insucesso de operações. Mas esse descaso intencional com a inteligência viria a mudar drasticamente com a revelação de um escândalo no jornal *The New York Times*, em setembro de 1974. A reportagem revelava que agências de inteligência tinham se envolvido em operações secretas para manipular eleições no exterior, além de espionar as comunicações de cidadãos americanos sem mandado judicial.

A resposta institucional veio de forma intensa, com a instalação de três comissões para apurar as denúncias. A primeira foi instalada pela própria Presidência da República (a Comissão Rockefeller), a segunda pela Câmara (Comissão Pike) e a terceira pelo Senado (Comissão Church). Cada um dos órgãos trabalhou de forma intensa, reunindo documentos e ouvindo agentes e autoridades. O resultado das investigações foi chocante. A mais célebre das comissões, a Comissão Church, que funcionou no Senado americano entre 1975 e 1976 e foi presidida pelo Senador Frank Church, mostrou à população que as denúncias eram, de fato, pertinentes, e que o nível de ilegalidades cometidas pelas agências de inteligência era um poço profundo envolto em sombras.

Foi comprovado que a CIA havia manipulado eleições no exterior, que promovia a infiltração de agentes em partidos e organizações religiosas e que invadia o correio de cidadãos americanos. O escândalo não se restringia à CIA, e era comum a outros órgãos de inteligência, como o FBI, o qual conduziu mais de 500 mil investigações de “subversivos” entre 1960 e 1974 (Johnson, 2008, p. 201).

O que a comissão concluiu é que, no contexto da Guerra Fria, quando os Estados Unidos se colocavam como defensores da democracia e da liberdade, não fazia sentido vencer a batalha contra a União Soviética e o totalitarismo se tornando um Estado totalitário, com métodos antirrepublicanos que se desenvolviam nas sombras. Abandonar os princípios democráticos, mesmo no campo da inteligência, como parecia ser o caso até ali, faria que o país perdesse sua identidade, bem como o apoio internacional (Johnson, 2008, p. 204). Por isso, o caso marcou um momento de inflexão no setor. A inteligência não poderia operar à margem da lei, sem controle democrático.

Como assinala Born (2004), afinal, toda democracia tem na prestação de contas seu elemento-chave. Os agentes do Estado devem agir às claras e responder à população por suas ações, responsabilizando-se por falhas, incompetência ou mesmo ilícitos cometidos. *Accountability*, transparência e controle fazem parte do *modus operandi* democrático – e, de alguma forma, também o setor de inteligência deve se submeter a esses primados.

Nos anos seguintes ao escândalo revelado pelo *The New York Times*, tanto a Câmara quanto o Senado americano criaram comissões permanentes destinadas a exercer o controle externo sobre a inteligência. A discussão sobre o controle da inteligência se espalhou por outros países. De todo modo, é digno de nota que se trata de um fenômeno recente, mesmo em democracias consolidadas. Se os EUA deram os primeiros passos para o controle externo da inteligência em meados da década de 1970, o Reino Unido, por exemplo, só criou uma comissão parlamentar de controle em 1994. Trata-se, portanto, de um debate ainda vivo e em andamento, com países e analistas compartilhando desenhos institucionais e requisitos para um controle efetivo e democrático da inteligência.

Um consenso formado entre estudiosos é que o controle da inteligência deve desenvolver-se em várias esferas: controle interno (exer-

cido pela própria agência de inteligência), controle do Poder Executivo (supervisão ministerial), controle judicial, controle parlamentar e escrutínio independente (exercido pela mídia e pela sociedade civil) (Gill; Pythin, 2006; Gonçalves, 2019). Para ser efetivo, todas essas formas de controle devem operar de forma adequada, de modo que não se pode prescindir de uma delas (Born, 2004).

Um controle interno operante, por exemplo, tem a vantagem de estar mais perto do dia a dia dos agentes de inteligência, devendo criar uma cultura de cumprimento às regras internas da agência e abrir um canal para denúncias de ordens ilegais (Born; Mesevage, 2012). O controle judicial também é relevante, oferecendo soluções de controle *ex ante* da Atividade de Inteligência para agir preventivamente¹ (Rindskopf Parker; Pate, 2007; Martins Júnior, 2015; Peterson, 2023). Já organizações não governamentais e a mídia muitas vezes se tornam protagonistas do controle ao ajuizar ações judiciais ou revelar desvios do setor de inteligência que levam a amplas discussões na sociedade, ou mesmo a reformas (Kniep *et al.*, 2024).

Mas é o controle exercido pelo parlamento que, certamente, assume maior destaque nas democracias. A ideia de que cabe ao parlamento fornecer a estrutura principal, se não a única, para o controle externo da inteligência, é quase universal (Gill; Pythin, 2006, p. 158), sendo esse tipo de controle também o mais efetivo, ao lado das agências de especialistas externos (Born; Mesevage, 2012). Como legítimos representantes do povo, os parlamentares possuem legitimidade para exercer o controle, não devendo nenhuma área do governo ser uma zona proibida para parlamentares (Born, 2004, p. 5).

¹ Discussões têm sido mantidas sobre a criação de uma vara especializada no Poder Judiciário para tratar de questões de inteligência. Ver em: <https://www.metropoles.com/colunas/guilherme-amado/servidores-da-abin-defendem-justica-especializada-em-inteligencia>. Acesso em 01 nov. 2024.

Em geral, parlamentos se engajam no controle de duas formas: avaliando o cumprimento da lei e das regras pertinentes e a eficácia da inteligência. Parlamentos precisam garantir que os órgãos de inteligência não violem a lei, preservando direitos e garantias individuais, mas também que os recursos públicos sejam utilizados de forma eficiente (Farson, 2012). Ora, parlamentos exercem de forma habitual o controle sobre o governo, mas o desafio é maior quando se trata do controle da inteligência. Além de ser o campo por excelência do "sigilo estatal" (Kniep *et al.*, 2024), a inteligência lida com assuntos sensíveis, que podem comprometer a segurança nacional. Portanto, como pontua Ott (2003), uma coisa é o Congresso exercer controle sobre o Departamento de Energia ou de Agricultura, ou levantar dados sobre construção de casas populares; outra, distinta, é controlar as atividades de inteligência.

Logo, o controle parlamentar deve tanto ter requisitos especiais para se tornar efetivo quanto procedimentos específicos para que o controle não resulte em riscos para a segurança nacional. Em linhas gerais, pode-se falar que a grande dificuldade para o controle parlamentar da inteligência é a assimetria de informações, e o grande risco desse tipo de controle é a politização exagerada do controle. Esses dois pontos serão explorados em mais detalhe abaixo.

Quanto às dificuldades para que o controle se torne efetivo, Gonçalves (2019), analisando a literatura sobre a área, mostra que há um paradoxo, pois, diante do sigilo da Atividade de Inteligência, o controlador depende inteiramente das informações fornecidas pelo controlado. Trata-se, a rigor, de um típico problema de delegação, no qual as perdas por agenciamento, tais como assimetria de informações, risco moral e seleção adversa, se fazem presentes (Kiewiet; McCubbins, 1991). Daí a necessidade de discutir o tema e comparar modelos, a fim de que o arcabouço formal de controle seja adequado para as especificidades da inteligência.

Segundo Born (2004), cinco elementos influenciam a efetividade do controle: atribuições dos órgãos, tipo de órgão, poderes orçamentários, poderes de investigação e acesso a documentos. As *atribuições* podem ser amplas (avaliando legalidade e eficiência dos órgãos) ou restritas (avaliando apenas um desses atributos); podem, também, ser proativas (vetando ações de inteligência) ou reativas (tomando conhecimento a posteriori). O *tipo de órgão* pode ser parlamentar, formado apenas por parlamentares, ou uma agência independente, formada por especialistas, mas geralmente vinculada ao parlamento. Os *poderes orçamentários* consistem na prerrogativa de controlar a apropriação de verbas orçamentárias para agências de inteligência e são um dos principais poderes do parlamento. Os *poderes de investigação* dizem respeito à capacidade do órgão de controle de iniciar investigações. Por fim, o *acesso a documentos* pode ser integral ou parcial, mas o controle efetivo pressupõe o acesso integral.

Sobre esse tema, aliás, a literatura é praticamente unânime em apontar sua centralidade para o controle efetivo da inteligência. Vale dizer que não há controle se não há acesso integral a documentos. Opor o sigilo até mesmo à comissão parlamentar de controle significa esvaziá-la completamente de suas funções. Por esse motivo, o acesso integral a informações e documentos, independente de seu grau de sigilo, é requisito fundamental para o controle da inteligência (Born, 2004; Born; Leigh, 2005; Gill; Pythian, 2006; Bruneau; Matei, 2010; Farson, 2012; Nathan, 2012).

Quanto aos riscos e dificuldades do controle parlamentar da inteligência, sobressaem dois aspectos: a falta de engajamento dos parlamentares, de um lado, e a politização exagerada, de outro. Johnson (2008), falando sobre as comissões permanentes de controle da inteligência na Câmara e no Senado americano, diz que há diversas forças de atração e de repulsa a essas comissões. Primeiro, os parlamentares parecem atraídos para participar e se engajar nessas comissões, porque se envolver com o tema da inteligência passa ao eleitorado a men-

sagem de que o parlamentar se importa com a defesa e a segurança nacional. Além disso, suas reuniões a portas fechadas e as audiências secretas travadas com os diretores da CIA trazem um ar à *la James Bond*, atraindo parlamentares para sua composição.

Por outro lado, Johnson demonstra que o dia a dia do controle envolve atividades rotineiras de análise de diversos documentos e comparecimento a audiências. O trabalho intenso no envolvimento com o controle da inteligência vem com um custo elevado de tempo, ativo precioso na vida parlamentar. Somado a isso, tem-se a impossibilidade de auferir capital político com a atividade, já que o parlamentar não pode tornar público o que faz devido ao sigilo da comissão. Esses dois fatores acabam funcionando como desestímulo a um controle engajado e eficiente. Afinal de contas, "inteligência não dá votos" (Gonçalves, 2019).

Mas se a falta de engajamento é sempre um desafio ao controle parlamentar, outro risco é a sua politização excessiva. Ao levar o controle para o campo político-partidário, corre-se o risco de fazer que a comissão ecoe sensacionalismo e alimente teorias da conspiração. Há, igualmente, o risco do vazamento de informações sensíveis por políticos (Ott, 2003; Gill; Pythian, 2006).

Esses fatores são apontados pela literatura como impeditivos para um controle parlamentar eficiente, seja por sua completa falta de vocação e familiaridade com o tema, seja por sua instrumentalização política. Para contornar esse risco, alguns sugerem a criação de um órgão especializado de controle, formado por especialistas e não políticos, embora seja de algum modo ligado ao parlamento. Esse modelo, de órgão especial independente, é praticado, por exemplo, no Canadá e em Portugal. Outros, por sua vez, sugerem que o controle exercido por parlamentares seja feito de maneira imparcial, técnica, apolítica, de modo a não contaminar o debate.

Embora assista alguma razão a esses argumentos, deve-se, contudo, sopesá-los diante de algumas réplicas. Apresentamos quatro.

Primeiro, como já comprovado em casos práticos, o risco de vazamento de informações pelos parlamentares é baixo, o que desmonta uma das principais críticas contra o controle parlamentar (Ott, 2003; Cluskey; Aradau, 2023).

Segundo, parlamentares são atores com mandato popular, ligados democraticamente ao eleitorado, de modo que sua atuação pode emprestar maior legitimidade ao controle da inteligência, tirando o setor de um viés estritamente técnico, fechado a especialistas, para permitir o controle popular (Born; Leigh, 2005).

Terceiro, mesmo não sendo especialistas, os parlamentares podem se valer de processos de aprendizado institucional. Um modelo institucional adequado, com regras claras de atribuições e responsabilizações, além de sucessivas rodadas de interação com o órgão de inteligência, pode induzir a um processo de aprendizado institucional, fazendo que a comissão parlamentar de controle minimize as perdas por agenciamento (Lupia; McCubbins, 1995).

Por fim, o controle pode ser exercido mesmo em um viés conflitivo, guiado por embates político-partidários. Ora, a “visão consensual” do controle prega que deve haver confiança mútua entre controladores e controlados, isto é, entre a comissão parlamentar e os órgãos de inteligência, e que ambos devem trabalhar de forma imparcial e institucional para o bem do setor. O conflito político-partidário, nessa visão, é nocivo para a efetividade do controle. Porém, como demonstrado por Kniep *et al.* (2024), essa visão consensual de controle traz implícita uma relação hierárquica, na qual a comissão parlamentar, inferior, deve lutar para ganhar a confiança da agência de inteligência, superior; caso contrário, não haverá colaboração entre eles, e o controle será prejudicado pela resistência e falta de cooperação do setor de

inteligência. Além disso, a visão consensual engendra certa visão utópica, como se o político conseguisse trabalhar como político em todas as suas atividades no parlamento, com exceção de uma, o controle da inteligência. Assim, deve-se assumir como natural da democracia, dos parlamentares e da comissão parlamentar, o controle conflitivo da inteligência, sem com isso desmerecê-lo por sua atuação com certo pendor político em vez de estritamente técnico.

O tipo ideal de controlador, o parlamentar supostamente imparcial e técnico, dificilmente é encontrado na prática. Analisando o perfil dos 183 parlamentares americanos que participaram das comissões de controle da inteligência ao longo de mais de três décadas, Johnson (2008) apresenta quatro perfis de atuação. O primeiro seria o "aves-truz", aquele parlamentar que prefere esconder a cabeça na terra e esquecer o setor de inteligência, dedicando-se a outras atividades. O segundo seria o "líder de torcida", aquele parlamentar que defende perante a opinião pública e o Congresso as agências de inteligência, buscando maior orçamento e aprovando suas operações, faltando-lhe olhar crítico. O terceiro seria o "cético", o parlamentar extremamente cético em relação às agências de inteligência, com visão unilateral de que nada do que as agências façam é bom, que elas são imorais, invasivas e incompetentes, e que, afinal, devem ser fechadas. O quarto seria o do "guardião", o parlamentar que é "tanto parceiro quanto crítico", que sabe o valor das agências, mas age com olhar crítico, buscando exercer um bom controle.

Por óbvio, os perfis traçados não são tipos estanques. Igualmente, um parlamentar pode migrar de um tipo para outro ao longo de seu período de atuação (geralmente, um "líder de torcida" acaba se tornando "cético" após a divulgação de algum escândalo ou de alguma comprovação de que a agência mentiu em seus informes ao Congresso). O que importa notar é que os perfis de atuação encontrados por Johnson apresentam uma realidade comum a outros contextos, como no caso brasileiro. Assim, em uma comissão parlamentar de

controle da inteligência, haverá tanto a falta de engajamento na atividade (o parlamentar “avestruz”), quanto o risco de sensacionalismo e oposição exagerada ao órgão de inteligência (o parlamentar “cético”).

Apesar de mecanismos institucionais poderem reforçar o engajamento no controle e minimizar a partidarização exagerada (Gonçalves; Bedritichuk, 2024), o certo é que o controle parlamentar deverá ser exercido mesmo diante de perfis diferentes de parlamentares. Esse controle revela-se ainda mais importante tendo em vista o passado sombrio de alguns países.

2. De polícia política a órgão democrático de inteligência

A maior parte dos estudos sobre inteligência e controle está centrada em democracias consolidadas, especialmente no eixo EUA-Reino Unido. Mesmo nesses países, a discussão sobre controle é relativamente nova, remontando aos anos 1990. Por isso, diz-se que a “parlamentarização” do controle da inteligência é ainda fenômeno recente (Born, 2004).

A discussão, todavia, é ainda mais premente em novas democracias. Se em democracias consolidadas há um grande risco de que serviços de inteligência operem à margem da lei, insulando-se dentro da estrutura administrativa do Estado, esse risco é ainda maior em novas democracias que tenham passado autoritário.

Via de regra, o Estado autoritário utiliza o aparato de inteligência para proteger e perpetuar o regime. Os serviços de inteligência nascem vinculados ao setor militar, em funções sobrepostas com a polícia (Assumpção, 2020). O aparato é utilizado sobretudo domesticamente, com o fim de neutralizar inimigos do regime, sem qualquer consideração sobre a legalidade de sua atuação. Os órgãos de inteligência de Estados autoritários “controlam, intimidam, manipulam, abusam e oprimem inimigos ideológicos, reais ou imaginários, sem respeito por

direitos humanos ou liberdades” (Bruneau; Matei, 2010, p. 4). Trata-se de organismo fundamental desse tipo de governo.

Aos poucos, observa-se o agigantamento desses órgãos, que, de “polícias políticas”, crescem para se transformar em “estados de segurança independentes” (Bruneau; Matei, 2010). Atuando nas sombras e sem qualquer mecanismo institucional de controle, os órgãos crescem em poder e influência dentro do regime. Tornam-se autônomos, como um “poder paralelo” ou um “Estado dentro do Estado”. Não por acaso, vários de seus comandantes tornam-se líderes políticos proeminentes, quando não presidentes. Os abusos dos agentes que atuam sem freios se acumulam e, por não haver mecanismos institucionais de controle, muitas vezes são somente as denúncias veiculadas pela imprensa ou a pressão da sociedade civil que funcionam como limitações ao poder do aparato de inteligência. Ainda assim, apesar do grande poder e da atuação sem limites, nota-se certo improvisado na condução das atividades de inteligência, com falta de profissionalismo, recrutamento por ideologia, falta de gestão e tecnologias desatualizadas (Gill, 2012).

Quando ocorre a ruptura do regime, observa-se um longo processo de consolidação democrática, até que as instituições estatais estejam maduras, os atores políticos mantenham certeza razoável sobre a continuidade democrática e não temam mais um regresso autoritário (Assumpção, 2020). Um ponto costumeiramente negligenciado nesse processo diz respeito ao controle da inteligência, que se insere num escopo mais amplo das relações civis-militares. Trata-se de tema complexo, espinhoso, normalmente um tabu no país em transição, mas que deve ser enfrentado para que a consolidação democrática seja concluída.

Bruneau e Matei (2010) comentam sobre esse difícil processo. Geralmente, as novas estruturas de inteligência convivem com legados autoritários, o que torna a democratização complexa. Primeiro, uma

vez que sistemas de inteligência são construídos sobre as ruínas dos antigos (mantendo estrutura, pessoal, forma de agir), a inteligência carrega um forte estigma por seu passado de transgressões. Segundo, falta aos serviços de inteligência profissionalização (novo pessoal, treinamento, código de ética etc.), de forma que as lacunas são preenchidas por agentes antigos, que preservam hábitos e rotinas da época autoritária. Terceiro, democracias emergentes não têm *expertise* em produzir reformas no setor, já que o foco do processo de transição está em aspectos econômicos e sociais, necessidades mais urgentes do país. Além disso, em casos em que a inteligência era monopólio dos militares (como no Brasil e na Argentina), há maior dificuldade, pois os militares ainda gozam de autonomia e poder nas novas democracias.

A reestruturação do setor de inteligência, com vistas a adequá-lo aos novos parâmetros democráticos, requer, em primeiro lugar, um marco jurídico claro, conferindo institucionalidade ao setor. Outro passo é desenvolver uma "doutrina" de segurança clara e objetiva, para não incorrer na obsessão de perseguir "inimigos internos", voltando a inteligência contra opositores do governo (Gill, 2012).

Além de reestruturar o setor de inteligência, sua democratização envolve a criação de um arcabouço de controle da inteligência, o que é ainda mais significativo em novas democracias, já que o novo arcabouço legal pode conviver com uma subcultura prática de violações de direitos devido ao legado autoritário (Gill; Pythian, 2006). O passo seguinte consiste em efetivar os mecanismos de controle, o que encontra barreiras na forte resistência das agências de inteligência, de segurança e policiais e no controle que elas exercem sobre documentos e informações (Assumpção, 2020; Farson, 2012). Por fim, ao estabelecer um efetivo controle da legalidade, o passo derradeiro para completar o controle democrático consiste em avaliar a efetividade dos órgãos de inteligência, a fim de averiguar se eles cumprem sua missão institucional (Bruneau; Matei, 2010).

Como visto, trata-se de um longo percurso. De um lado, a polícia política transforma-se em Estado paralelo, acostumando-se a atuar sem peias e no desprezo da lei. Por outro lado, é essa mesma polícia política, esse Estado paralelo, que precisa ser domado num contexto democrático, transformando-se em órgão de inteligência que atua com eficiência, mas dentro da legalidade.

Sendo diversos os contextos, cada país percorrerá esse caminho a seu próprio modo.

3. Eu sei o que vocês fizeram...

O Brasil viveu um período autoritário de 1964 a 1985, sendo um dos primeiros atos do novo regime a criação do Serviço Nacional de Informações (SNI), em 13 de junho de 1964, órgão principal do sistema de inteligência do regime militar.

Cabia ao SNI, nos termos da Lei nº 4.341/1964, "superintender e coordenar, em todo o território nacional, as atividades de informação e contra informação, em particular as que interessem à Segurança Nacional" (art. 2º). Seu chefe tinha o *status* de Ministro de Estado, e sua indicação deveria ser aprovada pelo Senado. Além disso, a própria lei dispunha que o SNI estava "isento de quaisquer prescrições que determinem a publicação ou divulgação de sua organização, funcionamentos e efetivos" (art. 4º, § 2º). A lei não previa qualquer espécie de controle institucional sobre os atos do SNI.

O SNI convivia com outros órgãos de inteligência. Por exemplo, cada Força tinha à sua disposição um órgão próprio voltado às atividades de inteligência. O Exército tinha o Centro de Inteligência do Exército (CIE), a Marinha, o Centro de Informações da Marinha (CENIMAR) e a Aeronáutica, o Centro de Informações de Segurança da Aeronáutica (CISA). Havia, portanto, superposição e até competição de funções entre os órgãos de inteligência (Brandão, 2010).

Observou-se no caso brasileiro o mesmo itinerário de órgãos de inteligência em regimes autoritários: o crescimento de uma polícia política até um aparato autônomo e poderoso, como um Estado paralelo. Segundo Brandão, não havia qualquer mecanismo de controle ou freio institucional dos órgãos de inteligência, exceto a preocupação “dos militares em se legitimarem enquanto instituição e enquanto governo” (2010, p. 130). Seus agentes se viam livres para praticarem vigilância, repressão, sequestro e tortura (Assumpção, 2020). A ampla autonomia, a opacidade do sistema, a extensão das ações voltadas à segurança nacional e executadas em todo o país e a falta de controle – tudo isso fez do sistema de inteligência um “quarto serviço militar” ou um “estado dentro do Estado” (Gill, 2012), ou ainda, um “poder paralelo” (Cepik, 2022). Prova disso é que, dos cinco presidentes militares, dois foram diretores do SNI (Emílio Garrastazu Médici e João Baptista Figueiredo).

A transição para a democracia operou-se em um processo longo e gradativo, liderado pelos próprios militares, o que permitiu que eles ditassem o ritmo e, de certa forma, controlassem o processo (Bruneau, 2007). Os agentes de inteligência, em geral, manifestavam-se contrários à abertura política, uma vez que perderiam poder com o regime democrático e temiam investigações e punições por violações aos direitos humanos (Brandão, 2010, p. 131).

A passagem de poder para o primeiro presidente civil em 21 anos foi negociada e realizada por eleição indireta, quando o Congresso Nacional elegeu Tancredo Neves. Um acontecimento fortuito teve grande impacto no aspecto da transição democrática brasileira: Tancredo veio a falecer antes de assumir a presidência, sendo empossado o seu vice, José Sarney. Esse fato assume um relevo importante, já que Sarney não tinha respaldo popular como Tancredo Neves, não sendo também uma liderança política legítima dentro do campo oposicionista. Após o fracasso do plano econômico, Sarney se tornou um Presidente impopular e minoritário (Power, 1998), sendo refém de outros líderes parti-

dários, o que acabou por dar uma sobrevida ao poder militar dentro do governo civil. Os militares ainda mantiveram seis ministros dentro do gabinete (Exército, Marinha, Aeronáutica, Estado-Maior, Casa Militar e SNI), preservando cargos-chave em projetos estratégicos, como na Amazônia e nos projetos nucleares (Brandão, 2010).

Foi apenas com a eleição de Fernando Collor, em 1989, que a transição democrática deu passos mais significativos, com a eleição direta de um civil e a subordinação dos militares aos civis. Nessa linha, Collor extinguiu o SNI no primeiro dia do seu governo, em 15 de março de 1990, passando o setor de inteligência à Secretaria de Assuntos Estratégicos (SAE), vinculada à Presidência da República e chefiada por um civil. Apesar desse movimento, observou-se grande descaso político com a reformulação do setor de inteligência na década de 1990, influenciado pelo estigma do SNI e também pela percepção compartilhada de que o Brasil é um país sem inimigos externos e sem ameaças que justifiquem a existência de um aparato forte de inteligência (Gill, 2012). Como visto, Estados em transição democrática em geral demoram a reformar seus aparatos de inteligência, seja pelo legado autoritário, seja porque o tema vira um tabu, seja, ainda, porque as pautas econômicas e sociais é que ocupam as agendas políticas nesse período.

Quando assumiu o governo em 1995, o Presidente Fernando Henrique Cardoso (FHC) propôs, por medida provisória, a criação de uma agência central de inteligência. A medida não foi bem recebida no parlamento, que pretendia debater os termos da reestruturação. O governo, então, mandou um projeto de lei em 1997, que foi aprovado pelo Congresso Nacional em 1999, consolidando, então, o marco legal do novo sistema brasileiro de inteligência.

A Lei n.º 9.883, de 7 de dezembro de 1999, criou a Agência Brasileira de Inteligência (ABIN), responsável por “planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País”

(art. 3º). Além disso, a legislação criou o Sistema Brasileiro de Inteligência (SISBIN), tendo a ABIN como órgão central e integrado por “órgãos e entidades da Administração Pública Federal que, direta ou indiretamente, possam produzir conhecimentos de interesse das atividades de inteligência”, na forma de ato do Presidente da República (art. 2º). Adotou-se, como em outros países com passado autoritário, um modelo descentralizado; se tal modelo evita o monopólio e a concentração de poderes em um só órgão, também cria certa dispersão da Atividade de Inteligência, com várias agências agindo muitas vezes de forma competitiva (Bruneau; Matei, 2010).

A Lei nº 9.883/1999 também dispôs que o controle externo seria realizado por órgão do Congresso Nacional, integrado pelos líderes da maioria e minoria de cada Casa, bem como pelos Presidentes das Comissões de Relações Exteriores e Defesa Nacional de cada Casa.

Segundo Cepik (2022), a partir da aprovação da Lei nº 9.883/1999, teve início um período de consolidação do sistema de inteligência, concorrendo para tanto a subordinação da ABIN ao Gabinete de Segurança Institucional da Presidência da República, a criação de subsistemas de inteligência e a estruturação do conselho do SISBIN. Avanços recentes na consolidação do sistema estatal de inteligência podem ser vistos, por exemplo, na aprovação da Política Nacional de Inteligência (Decreto nº 8.793/2016), da Estratégia Nacional de Inteligência (Decreto de 15 de dezembro de 2017), bem como na transferência da ABIN para a Casa Civil (Decreto 11.426/2023) e na reformulação do SISBIN (Decreto nº 11.693/2023), com a qualificação dos órgãos integrantes e o detalhamento de sua coordenação.

Entretanto, muitos ainda criticam a legislação de inteligência por seus termos vagos e imprecisos, como Assumpção (2020), Cepik (2007) e Araújo (2022). Outra fonte de críticas é a permanência de agentes do antigo SNI nos quadros da ABIN, perpetuando tanto práticas quanto uma cultura de atuação às margens da lei (Bruneau; Matei, 2010).

Vale notar, entretanto, que esse quadro já foi consideravelmente atenuado, dado que a maior parte dos ex-agentes do SNI já se aposentaram e que o quadro atual da Agência é predominantemente formado por civis recrutados por meio de concursos públicos ocorridos entre 1994 e 2018.

Permanece ainda grande desconfiança entre os agentes de inteligência e a classe política, como se a ABIN fosse, por um lado, inefetiva e desnecessária, e, por outro, apenas um braço de inteligência do governo de situação, utilizado para monitorar a oposição. Vítima do SNI, a ex-Presidente Dilma Rousseff (2011-2016) nunca demonstrou confiar no sistema de inteligência, da mesma forma que o ex-Presidente Jair Bolsonaro (2019-2022) (Assumpção, 2020; Cepik, 2022). Além disso, escândalos divulgados pela imprensa se somam para reforçar a percepção entre a classe política de que a ABIN é um instrumento político e ainda hoje uma ameaça à democracia².

Em resumo, décadas após a aprovação do marco legal da inteligência no Brasil, ainda há muito a percorrer no sentido de sua completa democratização. Primeiro, a legislação ainda é deficiente, carecendo de detalhes sobre a Atividade de Inteligência, de limites e de salvaguardas aos seus agentes. Segundo, paira a percepção de que os serviços da ABIN não são eficientes, criando um clima de desconfiança da comunidade política para com a inteligência. Por fim, ainda é bastante forte o estigma autoritário que remete ao SNI, alimentado por sucessivos escândalos divulgados pela imprensa. Nesse sentido, o

2 Para citar apenas alguns casos: Escândalo da Abin paralela abre crise e expõe atuação nebulosa da agência, **Veja**, 4 jun. 2024. Disponível em: <<https://veja.abril.com.br/brasil/escandalo-da-abin-paralela-abre-crise-e-expoe-atuacao-nebulosa-da-agencia>>; A Abin também espionou adversários no governo Lula, **Veja**, 7 mai. 2024. Disponível em: <<https://veja.abril.com.br/politica/a-abin-tambem-espionou-adversarios-no-governo-lula>>; Quais são os limites? Maior escândalo da Abin reabre discussão sobre as atividades de inteligência, **O Globo**, 4 fev. 2024. Disponível em: <<https://oglobo.globo.com/politica/noticia/2024/02/04/quais-sao-os-limites-maior-escandalo-da-abin-reabre-discussao-sobre-as-atividades-de-inteligencia.ghtml>>.

caminho ainda é longo para que o sistema de inteligência no Brasil seja, a um só tempo, eficiente e controlado democraticamente.

4. Um longo caminho a percorrer

O caminho fácil é colocar toda a culpa na ineficácia do controle parlamentar de inteligência no Brasil. Mas em assunto tão delicado, não se pode pegar atalhos. Deve-se percorrer toda a estrada, ainda que longa.

O Brasil adotou um modelo de controle externo da inteligência baseado em uma comissão parlamentar, focada em garantir o controle legal das atividades de inteligência e evitar abusos. A comissão incumbida do controle externo da inteligência é a Comissão Mista de Controle das Atividades de Inteligência (CCAI), formada por 12 parlamentares, seis senadores e seis deputados. Desde sua primeira reunião, em 2000, até 2013, a CCAI teve atuação esporádica e reativa. Em 2013, após longo debate entre os parlamentares engajados no controle, o Congresso aprovou a Resolução nº 1, de 2013, do Congresso Nacional, norma que institucionalizou o órgão, delineando melhor suas atribuições, composição e atuação. Porém, mesmo com esse importante avanço institucional, o padrão de atuação da CCAI não se alterou, sendo marcado pela reatividade (Gonçalves; Bedritichuk, 2024).

Com efeito, o histórico de atividades da comissão pode ser contado com base no histórico de escândalos envolvendo a ABIN. A instalação da comissão em novembro de 2000 foi motivada por denúncias de espionagem ilegal pela ABIN contra agentes públicos, refletindo seu padrão reativo (Brandão, 2010, p. 152). Em 2005, ano de maior movimento da comissão, a CCAI foi impulsionada pela denúncia de que suposto relatório da ABIN comprovaria que o PT teria recebido doação das FARC. Já em 2008, foi a *Operação Satiagraha*, conduzida pela Polícia Federal, o mote que movimentou a comissão, apurando denúncias de diversas interceptações telefônicas de agentes públicos

feitas ilegalmente. Em 2023, por sua vez, a *Operação Última Milha*, também conduzida pela PF, investigou a compra e utilização de *software* de georreferenciamento que supostamente teria sido utilizado para monitorar opositores ao governo no escândalo conhecido como "Abin Paralela". Em todos esses anos, a CCAI foi cobrada a atuar mais firmemente, e o tema da inteligência e de seu respectivo controle esteve na agenda nacional.

Sem dúvida, há espaço para aprimoramento institucional da comissão parlamentar de controle no Brasil. Gonçalves e Bedritichuk (2024), por exemplo, mostram que alterações regimentais podem conferir à CCAI instrumentos mais claros e adequados para o exercício do controle, além de favorecer a especialização dos membros e minimizar, tanto quanto possível, o embate político-partidário dentro do qual as reuniões costumam ocorrer.

Porém, independente disso, cabe registrar que o controlador técnico e imparcial, idealizado por diversos trabalhos na área, simplesmente não será a maioria em uma comissão parlamentar de controle. Ao contrário, convivem no colegiado parlamentares de diferentes perfis, conforme demonstrado por Johnson (2008). Dessa forma, o comportamento da CCAI no Brasil não destoa muito do esperado para um controle parlamentar da inteligência, observando-se tanto a falta de engajamento quanto a politização exagerada em alguns momentos.

A partir do quadro descrito, questiona-se como se pode avançar no controle para torná-lo efetivo, contribuindo para a eficiência e transparência do sistema de inteligência. Farson (2012), ao enumerar as dificuldades inerentes ao controle da inteligência no contexto de países democráticos, menciona aquelas conhecidas, como falta de especialização, falta de engajamento, partidarismo exagerado e recursos inadequados. Porém, o impedimento mais importante para o controle efetivo, segundo ele, é a limitação de acesso a informações e documentos. Sem acessar os documentos de inteligência, parlamentares

vão simplesmente dar crédito às informações obtidas por outras fontes, em geral os escândalos veiculados pela imprensa, o que contribui ainda mais para o desprestígio da Atividade de Inteligência, levando a um ciclo vicioso de opacidade e desconfiança mútua.

Em contextos de transição democrática, onde as agências de inteligência buscam se consolidar institucionalmente no novo regime, com mais recursos e profissionalização de seus serviços, há uma resistência natural ao controle. Segundo Bruneau e Matei (2010), muitos agentes não querem se submeter a “amadores” na área, ou seja, aos políticos, vendo-os como atores que não se importam e não entendem o tema da inteligência, sendo, portanto, empecilhos ao pleno desenvolvimento da atividade. Dentro dessa linha de raciocínio, a inteligência seria mais efetiva se os órgãos estivessem livres do controle, o que retoma o passado autoritário, de quando as agências atuavam sem amarras institucionais.

Gill e Pythian (2006) lembram que o fator determinante para que o controle da inteligência seja efetivo ou meramente simbólico é o acesso integral às informações. Assim, por mais que a estrutura formal de controle preveja o acesso integral a documentos, na prática o quadro muitas vezes é diverso, com as agências se negando sistematicamente a cooperar com o controle, demandando um processo contínuo de aprimoramento institucional, bem como de mudanças de práticas, segundo os autores.

No caso brasileiro, observa-se essa dicotomia entre previsões legais e a prática do controle. A Política Nacional de Inteligência (Decreto nº 8.793/2016) lista como um dos instrumentos essenciais da inteligência nacional o controle interno e externo da Atividade de Inteligência. A Estratégia Nacional de Inteligência (Decreto s/n de 15 de dezembro de 2017) detalha melhor a questão, consignando expressamente a CCAI como órgão por excelência do controle externo, cabendo à comissão parlamentar “influir permanentemente para atingir as mudanças

desejadas, emanando recomendações e buscando estimular as condutas e atitudes adequadas". A Estratégia Nacional de Inteligência também traz como princípio orientador a "ampliação da interação com a sociedade, órgãos representativos e com o Poder Legislativo".

Apesar dessas previsões normativas que valorizam o controle da inteligência, indaga-se como concretizá-las. Vale dizer: como tornar efetiva a "ampliação da interação" com o Poder Legislativo a partir de ações da própria comunidade de inteligência?

A solução começa, certamente, pela pavimentação de um diálogo contínuo e aberto com o parlamento, mas não pode ter como objetivo último apenas constituir uma assessoria parlamentar para pleitear por emendas orçamentárias. Uma possibilidade, comum em diversos países, é o envio anual de relatórios à comissão parlamentar de controle pelos órgãos de inteligência, indicando suas prioridades, ações em andamento, orçamento e programas (Nathan, 2012) – e isso de forma espontânea e não provocada.

Outra possibilidade é reforçar a transparência ativa, colocando em prática um dos valores norteadores da Doutrina da Atividade de Inteligência, publicada em 2023. Sabe-se que o princípio da transparência – princípio constitucional (CF, art. 5º, XXXIII) regulado pela Lei de Acesso à Informação, a conhecida LAI (Lei nº 12.527/2011) – deve ser a regra balizadora de todo o Estado, devendo os órgãos estatais agir proativamente, independente de solicitações, para colocar esse princípio em prática. Por óbvio, a Atividade de Inteligência está protegida legalmente pelo sigilo, constituindo-se como exceção a esse princípio.

Assim, deve-se achar um equilíbrio fino no tocante a esse ponto. Por isso mesmo a Doutrina da Atividade de Inteligência assevera como fundamental que, no que for possível, os órgãos de inteligência "disponibilizem de forma proativa informações de interesse público, cuja

publicação ofereça pouco prejuízo à condução de suas atividades". O princípio da transparência ativa deve, portanto, ser colocado em prática, a fim de que a ABIN e outros órgãos de inteligência possam sair das sombras e perfilar-se junto a outros órgãos estatais no que for possível. Do contrário, se a inteligência estatal se fecha no completo sigilo, como uma caixa-preta imune à *accountability* democrática, ainda que resguardada pela lei, pode entrar num caminho perigoso de insulamento, com o risco de desvios e instrumentalização política.

Outro ponto nevrálgico que merece atenção é a controvérsia com relação à possibilidade de "sigilo eterno" das informações de inteligência. Isso porque a LAI, ao trazer parâmetros objetivos para excepcionalizar o princípio constitucional da transparência, seria, numa linha interpretativa, a única norma federal aplicável sobre transparência e sigilo, revogando tacitamente as leis anteriores. Segundo a LAI, documentos que comprometem a Atividade de Inteligência podem ser classificados³ em uma das três categorias de sigilo previstas, cada qual com limite temporal de restrição de acesso, quais sejam: reservado (5 anos), secreto (15 anos) e ultrassecreto (25 anos), sendo que apenas o prazo de restrição dos documentos ultrassecretos pode ser renovado. Vencido o prazo de sigilo, qualquer que seja ele, "a informação tornar-se-á, automaticamente, de acesso público" (art. 24, § 4º).

Tomando a LAI como único parâmetro, o sigilo inerente às atividades de inteligência será apenas temporário, trazendo um equilíbrio adequado entre transparência e sigilo. Nessa toada, Vilar-Lopes (2017), por exemplo, analisa a quantidade de documentos classificados e desclassificados segundo a LAI no âmbito público federal e conclui

3 Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:

(...)

VIII – comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

pela compatibilidade entre democracia e sigilo ao demonstrar que os órgãos publicam a quantidade de documentos classificados, que a ABIN não possuía nenhum documento classificado como ultras-secreto e que, portanto, o sigilo seria apenas temporário no curto e médio prazos.

Há, contudo, uma armadilha hermenêutica no caso. Outra linha de interpretação argumenta que a própria LAI não exclui outras hipóteses legais de sigilo (art. 22), tais como o segredo de justiça e o segredo industrial, e que o sigilo das atividades de inteligência não tem por parâmetro a LAI, e sim a Lei nº 9.883/1999, mais especificamente seus artigos 9º e 9º-A. Tais dispositivos afirmam que informações sobre as atividades de inteligência serão mantidas em sigilo, sem dispor nada sobre a autoridade classificadora e o prazo de desclassificação.

Tal interpretação abre a possibilidade de um documento, ao ser protegido do acesso público com base na Lei nº 9.883/1999, poder ficar indefinidamente sob sigilo, sem prazo, ao contrário do prazo temporal de sigilo previsto pela LAI, hipótese que abriria a possibilidade de haver no Brasil o "sigilo eterno" das informações de inteligência.

Tal controvérsia pode ser visualizada na divergência de pareceres das consultorias jurídicas dos órgãos públicos. O Parecer Referencial da Controladoria-Geral da União (CGU), publicado em fevereiro de 2023, cita essa controvérsia interpretativa sobre o sigilo dos documentos de inteligência. O Parecer Referencial da CGU mostra que o Gabinete de Segurança Institucional (GSI) diversas vezes tem negado, em casos concretos⁴, o acesso a informações de inteligência, mesmo vencido o prazo de restrição de acesso previsto na LAI, sob o argumento de que "a divulgação do conteúdo dos documentos de inteligência pode

4 Por exemplo, nos pedidos de acesso a informações desclassificadas com os seguintes números de protocolo: 00077.000925/2012-17, 00077.002138/2019-78, 00077.002141/2019-91 e 00077.002142/2019-36.

continuar ensejando riscos para o Estado e a sociedade", uma vez que "o art. 9º-A da referida Lei configura uma hipótese de sigilo legal autônomo". Segundo o Parecer nº 224/2016/EVS/AJUR-ABIN/CGU/AGU, a Assessoria Jurídica da ABIN conclui pela interpretação que considera os arts. 9º e 9º-A da Lei nº 9.883/1999 como hipóteses de sigilo autônomo, que não se submetem aos parâmetros fixados pela LAI.

Alegando não haver mais no Brasil a hipótese de sigilo eterno após a publicação da LAI, o Parecer Referencial da CGU indica que esse é um tema que deverá ser enfrentado no futuro a fim de concretizar o equilíbrio entre transparência e sigilo alcançado pela LAI, com prazos definidos e procedimentos específicos. Trata-se, portanto, de um dos desafios prementes para aumentar a transparência e o controle da inteligência no Brasil.

A possibilidade de "sigilo eterno" se soma à tendência à sobreclassificação de documentos de inteligência como um entrave no caminho da maior transparência da inteligência estatal. Estudos mostram que órgãos de inteligência tendem a sobreclassificar documentos e informações (Bruneau; Matei, 2010). Geralmente, esses órgãos utilizam o termo "segurança nacional" como base para a classificação de documentos, expressão essa elástica e ambígua (Nathan, 2012). Segundo estimativa de Johnson (2018) no contexto norte-americano, 85% dos documentos de inteligência e defesa são classificados desnecessariamente, e os riscos de sua divulgação são exagerados. Essa tendência de sobreclassificação de documentos por órgãos de inteligência, conjugada com a hipótese de que as informações de inteligência possuem previsão legal autônoma de sigilo no Brasil, pode levar a um quadro de falta de transparência.

O problema se torna ainda mais evidente quando todo esse arcabouço de sigilo, protegido por interpretação legal singular, é utilizado para se esquivar do controle externo. Ora, é patente pela legislação pertinente (Lei nº 9.883/1999, art. 6º; Resolução nº 2/2013-CN, art.

2º, § 4º) o direito de acesso integral que a comissão parlamentar de controle externo no Brasil tem a documentos de inteligência, independente do grau de sigilo. Inclusive, a própria Doutrina Nacional de Inteligência assinala que “a CCAI goza de poderes para realizar inspeções em áreas e instalações dos organismos integrantes do SISBIN, com direito de acesso a documentos e arquivos”.

Todavia, mesmo diante dessa garantia legal, por vezes esse acesso tem sido dificultado⁵ ou mesmo negado⁶ em casos concretos, não apenas pela ABIN, mas também por outros órgãos que lidam com Atividade de Inteligência, como a Polícia Federal (PF). Assim, ainda que estruturado oficialmente, o sistema de controle da inteligência no Brasil ainda incorre nas dificuldades citadas pela doutrina como comuns em casos de transição democrática ainda não concluída, como a resistência dos órgãos de inteligência ao controle, a negativa de acesso a documentos sigilosos e a convivência de uma estrutura formal de controle contrariada por uma subcultura prática (Assumpção, 2020; Cepik, 2022).

Conclusão

Em conclusão, vê-se que o horizonte à frente ainda é amplo, e diversos passos devem ser dados para que o sistema de inteligência no Brasil possa finalmente se inserir num contexto democrático, cumprindo sua missão institucional. Não se pode negar que diversos passos importantes já foram dados ao longo do tempo, como o marco legal das atividades de inteligência, a crescente profissionalização do setor, a nova estruturação do Sistema Brasileiro de Inteligência a partir de 2023 e a criação da comissão parlamentar de controle externo.

5 Senador quer investigar ABIN, PF e CGU por 'abuso de autoridade'. **Veja**, 7 mai. 2024. Disponível em <<https://veja.abril.com.br/politica/senador-quer-investigar-abin-pf-e-cgu-por-abuso-de-autoridade>>

6 Ver, por exemplo, os Requerimentos nºs 13 e 18/2023-CCAI.

Contudo, muito ainda há por percorrer. Pode-se elencar a deficiência da legislação ou de recursos, a divulgação frequente de escândalos na área da inteligência, a desconfiança dos tomadores de decisão quanto aos serviços de inteligência, questionando mesmo sua eficiência e relevância, e, por fim, a ineficácia do controle, foco deste trabalho.

Bruneau e Matei (2010) argumentam que, em processos de democratização, a primeira etapa do controle da inteligência consiste em avaliar se ela é exercida em conformidade com a lei, respeitando direitos e garantias individuais. Após o país se estruturar nesse ponto, as atenções voltam-se à segunda etapa, quando o controle passa a se preocupar não apenas com a legalidade das atividades de inteligência, mas também sua eficiência.

Como apontado neste trabalho, a falta de transparência ativa, a sobreclassificação de documentos e a possibilidade de "sigilo eterno", além da resistência ao controle externo, constituem dificuldades nesse aspecto que devem ser superadas, cabendo aos órgãos de inteligência envidar esforços nesse sentido. Para além da ABIN, os setores de inteligência das Forças Armadas e das forças policiais também precisam se engajar em iniciativas de aperfeiçoamento dos mecanismos de controle.

O controle democrático da inteligência não é apenas um requisito para a transparência governamental, é um pilar indispensável para a legitimidade de qualquer democracia que aspira proteger os direitos de seus cidadãos. Assim, torna-se urgente uma reavaliação da legislação e das práticas institucionais que envolvem a inteligência estatal no Brasil. Para tanto, futuras pesquisas devem aprofundar a análise dos mecanismos de controle, explorando modelos bem-sucedidos que conciliem segurança e transparência em contextos de transição democrática, apontando para aprimoramentos do arcabouço e das práticas de controle.

Somente com esse compromisso contínuo é que o Brasil poderá consolidar um sistema de inteligência verdadeiramente compatível com os ideais democráticos. Afinal, a única forma de compatibilizar serviços de inteligência em contextos democráticos é por meio de um controle eficiente.

Referências

ARAÚJO, John. Quem Espia os Espiões? O Papel dos Serviços de Inteligência em Estados Democráticos. **Revista Brasileira de Inteligência**. Brasília: Abin, n.º 17, dez. 2022.

ASSUMPÇÃO, Clara Ribeiro. Intelligence Oversight and Effectiveness in New Democracies: The Case of Brazil. **POLITIKON: The IAPSS Journal of Political Science**, v. 45, jun. 2020.

BORN, Hans. Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices. **Connections**, v. 3, n. 4, p. 1-12, dez. 2004.

_____; MESEVAGE, Gabriel Geisler. Tool 1: Introducing Intelligence Oversight. In: BORN, Hans; WILLS, Aidan. **Overseeing Intelligence Services**. Genebra: DCAF, 2012.

_____; WILLS, Aidan. **Overseeing Intelligence Services**. Genebra: DCAF, 2012.

BRANDÃO, Priscila Carlos. **Serviços secretos e democracia no cone sul: premissas para uma convivência legítima, eficiente e profissional**. Niterói, RJ: Impetus, 2010.

BRASIL. **Lei nº 9.883, de 7 de dezembro de 1999**. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências. Brasília, 1999.

_____. **Lei nº 12.257, 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, 2011.

_____. **Decreto nº 8.793, de 29 de junho de 2016.** Fixa a Política Nacional de Inteligência (PNI). Brasília, 2016.

_____. **Decreto de 15 de dezembro de 2017.** Aprova a Estratégia Nacional de Inteligência. Brasília, 2017.

_____. **Decreto nº 11.426, de 1º de março de 2023.** Altera o Decreto nº 11.327, de 1º de janeiro de 2023, o Decreto nº 11.329, de 1º de janeiro de 2023, o Decreto nº 9.435, de 2 de julho de 2018, e o Decreto nº 4.376, de 13 de setembro de 2002, para integrar a Agência Brasileira de Inteligência à Casa Civil da Presidência da República. Brasília, 2023.

_____. **Decreto nº 11.693, de 6 de setembro de 2023.** Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência. Brasília, 2023.

_____. **Controladoria-Geral da União.** Parecer sobre Acesso à Informação para Atender ao Despacho Presidencial de 1º de Janeiro de 2023. Brasília, fev. 2023.

BRUNEAU, Thomas. Intelligence Reforms in Brazil: Contemporary Challenges and the Legacy of the Past. **Strategic Insights**, v. VI, n. 3, mai. 2007.

_____; MATEI, Florina. Intelligence in the developing democracies: the quest for transparency and effectiveness. In: JOHNSON, Lock (ed.). **The Oxford Handbook of National Security Intelligence**, 2010.

CEPIK, Marco. Structural Change and Democratic Control of Intelligence in Brazil. In: BRUNEAU, Thomas; BORAZ, Steven (eds.). **Reforming Intelligence**. Austin: Texas, 2007.

_____. Brazil. In: MATEI, Florina C.; HALLADAY, Carolyn; ESTÉVEZ, Eduardo E. (eds.). **The Handbook of Latin American and Caribbean Intelligence Cultures**. Maryland: Rowman & Littlefield, 2022.

CLUSKEY, Emma. M.; ARADAU, Claudia. From abuse to trust and back again: Intelligence scandals and the quest for oversight. In: BIGO, Didier et al (eds.). **Intelligence Oversight in Times of Transnational Impunity: Who Will Watch the Watchers?** Londres: Routledge, 2023.

FARSON, Stuart. Tool 2: Establishing Effective Intelligence Oversight Systems. In: BORN, Hans; WILLS, Aidan. **Overseeing Intelligence Services**. Genebra: DCAF, 2012.

GILL, Peter. Alguns aspectos da reforma da inteligência na América Latina. **Vária História**, Belo Horizonte, v. 28, n. 47, p.101-120, jan/jun 2012.

_____; PHYTHIAN, Mark. **Intelligence in an Unsecure World**. Cambridge: Polity Press, 2006.

GONÇALVES, Joanisval Brito. **Políticos e Espiões: o controle da Atividade de Inteligência**. Niterói, RJ: Impetus, 2019.

_____; BEDRITICHUK, Rodrigo Ribeiro. **Controle parlamentar da inteligência no Brasil: Análise e propostas de mudanças na CCAI**. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/Senado, Julho 2024 (Texto para Discussão nº 331).

JOHNSON, Loch K. The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability. **Intelligence and National Security**, v. 23, n. 2, p. 198-225, 2008.

_____. **Spy Watching: Intelligence Accountability in the United States**. Oxford, UK: Oxford University Press, 2018.

KIEWIET, D. Roderick; MCCUBBINS, Matheus. **The Logic of Delegation: congressional parties and the appropriations process**. Chicago: The University of Chicago Press, 1991.

KNIEP, R., EWERT, L., REYES, B. L., TRÉGUER, F., Cluskey, E. M., Aradau, C. Towards democratic intelligence oversight: Limits, practices, struggles. **Review of International Studies**, n. 50, p. 209-229, 2024.

LUPIA, Arthur; MCCUBBINS, Matthew. Who Controls? Information and the Structure of Legislative Decision Making. In: SHEPSLE, K.; WEINGAST, B. (eds.) **Positive Theories of Congressional Institutions**. Michigan: Michigan University Press, 1995.

MARTINS JÚNIOR, Ayrton Figueiredo. Atividade de Inteligência : uma proposta de controle judicial. 2015. 30 f. Dissertação (Mestrado em Ciências Criminais) – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2015.

OTT, Marvin. Partisanship and the Decline of Intelligence Oversight. **International Journal of Intelligence and CounterIntelligence**, n. 16, v. 1, p. 69-94, 2003.

PETERSON, Samuel. Unblindfold the Watchdog! The Judiciary's Opportunity to Strengthened Intelligence Collection Oversight. **UMKC L. Rev.**, v. 92, p. 449, 2023

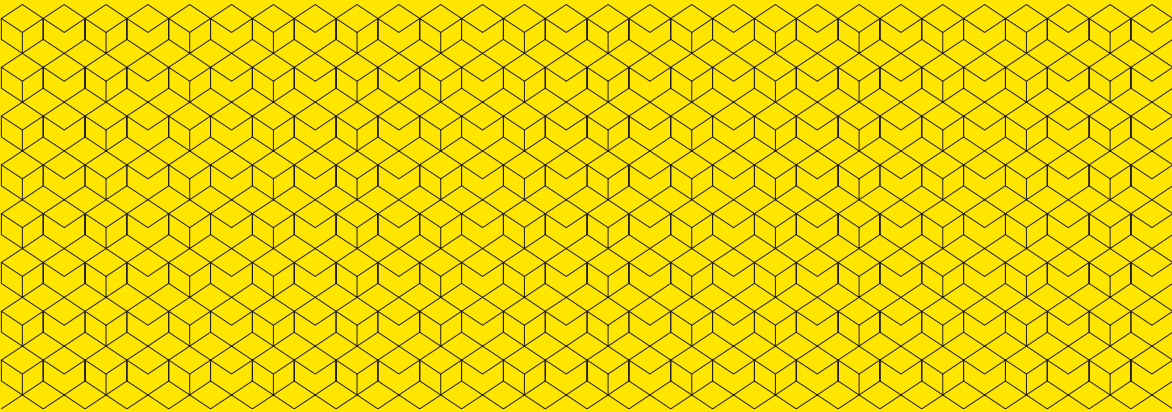
TURNER, Stansfield. **Queime antes de ler: presidentes, diretores da CIA e espionagem internacional**. Rio de Janeiro: Record, 2008.

RINDSKOPF PARKER, Elizabeth; PATE, Bryan. rethinking judicial oversight of intelligence. In: **Reforming Intelligence: Obstacles to Democratic Control and Effectiveness**. University of Texas Press, 2007. p. 51-72.

VILAR-LOPES, Gill. Quando o Segredo é a Regra: Atividade de Inteligência e Acesso à Informação no Brasil. **Revista Brasileira de Inteligência**. Brasília: Abin, n. 12, dez. 2017.

PARTE II

Atividade de Inteligência no Brasil: História





Uma era de transição: entre o SNI e a ABIN

Priscila Brandão

Professora Titular
Universidade Federal de Minas Gerais (UFMG e UFF)

Samantha Quadrat

Professora Associada
Universidade Federal Fluminense (UFMG e UFF)

Neste texto discutimos aspectos do desenvolvimento dos serviços de informações e de inteligência no Brasil desde 1920 até 2023, quase um século de história. Considerando todo o período e as limitações de espaço, priorizamos as considerações sobre aspectos como profissionalização, cultura política, inserção nas estruturas de governo e compatibilidade com os valores democráticos.

A história dos serviços de informações ou, mais recentemente, de inteligência, desperta a curiosidade e o interesse do público justamente por seu caráter confidencial ou sigiloso. Romantizadas por filmes nacionais e estrangeiros, essas atividades têm atraído também a atenção de pesquisadores que buscam fazer uma história institucional desde a sua criação, passando pela formação dos agentes, da criação de sua estrutura e de sua atuação em tempos democráticos e/ou ditatoriais. Procuramos oferecer uma perspectiva crítica enquanto historiadoras e pesquisadoras que acompanham o tema há anos.

1. Uma longa construção (1922-1964)

Até os anos 2000, datava-se a arquitetura de um sistema de informações¹ no Brasil a partir da criação do Serviço Federal de Informações e Contrainformações (SFICI), instituído por meio do decreto nº 9.775-A, em 6 de setembro de 1946, durante a presidência de Eurico Gaspar Dutra. A pressão diante do mundo dividido entre Estados Unidos e União Soviética, com o início da Guerra Fria, incentivava os governos a criarem e/ou reestruturarem atividades de inteligência nos países. A própria *Central Intelligence Agency* (CIA) estadunidense foi criada em 26 de julho de 1947, na esteira da elaboração da Lei de Segurança Nacional, promulgada durante a presidência de Harry Truman, com o intuito de dar conta das novas demandas surgidas após a Segunda Guerra Mundial (Cepik; Rodriguez, 2022).

No entanto, dado o avanço da pesquisa histórica, atualmente é possível questionar tal efeméride. O primeiro ponto diz respeito à própria criação do SFICI, pois, embora data de 1946, o órgão só se estrutura e passa a agir a partir de 1956, já durante a presidência de Juscelino Kubitschek, e por intensa pressão dos Estados Unidos, por meio do seu secretário de Estado John Foster Dulles, que via emergir na região grupos e movimentos sociais simpáticos ao socialismo e ao comunismo (Figueiredo, 2005). O segundo questionamento diz respeito ao ineditismo do SFICI. Pesquisas recentes apontam que a atividade de informações no Brasil tem origem, principalmente no âmbito civil, na Primeira República.

1 Diferentemente dos modelos anglo-saxões e de muitos modelos latino-americanos, o Brasil adotou a expressão informações para referir-se ao que a teoria política define como órgãos de inteligência. Esta expressão passa a ser utilizada no país apenas a partir de 1990, quando o desgaste produzido por esses órgãos durante a ditadura militar, em função da violência por eles desenvolvida, faz que adotem o termo inteligência como forma de se deslocarem dessa memória de violência. Dessa maneira, quando estivermos nos referindo a órgãos ou ao sistema responsável pela produção de conhecimento no país no período anterior a 1990, usaremos a expressão informações e, posterior a 1990, inteligência.

Foi durante a presidência de Epitácio Pessoa (1919-1922) que foi criada a Inspetoria de Investigação e Segurança Pública (Brito, 2011). Era uma estrutura civil que começou a funcionar em 1920, dividida em duas áreas principais, a saber: uma social, voltada para reprimir os movimentos resultantes do crescimento do trabalho urbano, da imigração de estrangeiros que chegavam ao país em grande número, do anarquismo e da própria criação do Partido Comunista Brasileiro em 1922; e outra política, encarregada de gerenciar as rivalidades entre as oligarquias que disputavam o poder.

Em 1922, seu primeiro ano na presidência, Artur Bernardes expandiu aquela estrutura, transformando-a na 4ª Delegacia Auxiliar. Igualmente à Inspetoria, a 4ª Delegacia monitorava políticos da oposição e reprimia trabalhadores, movimento que vinha crescendo em função da urbanização e industrialização do país (Brito, 2011). No que diz respeito ao setor militar, foi criado em 1927 o Conselho de Defesa Nacional (CDN). Embora o CDN não fosse exatamente um órgão de informações, sua função era estudar e coordenar dados sobre “todas as questões de ordem financeira, econômica, bélica e moral, relativas à defesa da Pátria” (Antunes, 2002, p. 43). Ele passaria por diversas mudanças de nome, mas só ganharia maior importância no período imediatamente anterior à Segunda Guerra Mundial (Ferreira, 2007).

Toda essa estrutura que começou a ser montada no início do século XX teve uma marca: trabalhava com a informação, mas também com a violência política bastante característica da época (Brito, 2011). Tal violência foi adensada durante os anos do Estado Novo (1937-1945), sob a presidência de Getúlio Vargas, mas iniciada ainda em 1930, a partir do momento em que ele chegou ao poder e nomeou interventores. Nesse sentido, podemos afirmar que foi com a criação da Delegacia Especial de Segurança Pública e Social (DESPS) que a violência política ganhou novos contornos, como, por exemplo, a ação contra o Levante Comunista em 1935 e durante o golpe do Estado Novo. Os anos Vargas, embora muitas vezes analisados pelo âmbito das polí-

ticas públicas e dos direitos, especialmente trabalhistas, acumulou um alto índice de violência política, que levou até mesmo à pressão pela extinção da DESPS, tendo em vista a participação brasileira na Segunda Guerra, que lutou ao lado dos aliados em defesa da democracia (Cancelli, 1994).

Em um recuo estratégico, Vargas extinguiu a DESPS e criou o Departamento Federal de Segurança Pública (DFSP), herdeiro das informações acumuladas pelo governo federal desde os anos 1920. Eram documentos sobre inimigos potenciais dos governos, líderes sindicais, listas de possíveis comunistas, entre outros. A partir da Segunda Guerra Mundial, o setor de informações brasileiro passou a operar em duas frentes mais definidas: uma civil, centrada no DFSP, e outra militar, sob a responsabilidade da Secretaria Geral do Conselho de Segurança Nacional (SG-CSN), ambas focadas no combate ao inimigo interno, já sob a influência da Doutrina de Segurança Nacional, deixando o Estado vulnerável às ameaças externas (Brandão, 2010). Entre os anos 1950 e início dos anos 1960, ocorreu um movimento sutil por parte dos militares que, em vez de transformar o novo DFSP (após a construção de Brasília) em sucessor do antigo DFSP (sediado no Rio de Janeiro, até então capital federal), transferiu todo o acervo informacional do DFSP carioca para as forças armadas (Brandão, 2019), esvaziando o poder do antigo órgão civil federal e marcando o início de uma característica do sistema de informações brasileiro: o protagonismo dos militares.

Nesse processo, a documentação do DFSP foi transferida para a Secretaria Geral Segurança Nacional (SG-CSN) e, posteriormente, para o Serviço Federal de Informações e Contrainformações (SFICI), citado logo no início deste capítulo.

Embora criado no governo Dutra, foi somente durante o governo JK que o Serviço Federal de Informações e Contrainformações (SFICI) passou a atuar de fato, conforme dito anteriormente. Dessa maneira, por meio do Decreto n.º 44.489-A, de 15 de setembro de 1958, o

governo o estruturou como órgão central de informações no Brasil, responsável por coordenar as atividades de interesse da segurança nacional, tendo, além da chefia, as subseções do exterior, do interior, da segurança e das operações. Meses depois, por meio do decreto nº 45.040, de 6 de dezembro de 1958, o regulamento da Secretaria Geral do Conselho de Segurança Nacional, de onde era oriundo seu orçamento e ao qual estava subordinado, foi aprovado. Nele estava a Junta Coordenadora de Informações (JCI), onde tinham assento o chefe do SFICI, além dos representantes dos Estados-Maiores das Forças Armadas, do Exército, da Marinha e da Aeronáutica e das Seções de Segurança dos Ministérios Cíveis.

Na visão da época, a formação do SFICI veio preencher uma lacuna, pois até então não havia um órgão central de informações no âmbito federal que assessorasse diretamente a Presidência da República. No entanto, o que ocorreu na prática foi a construção de uma agência que viria a desempenhar um papel ativo no golpe militar de 31 março de 1964.

Além disso, com o SFICI começamos a acompanhar um investimento maior na formação dos homens e mesmo das mulheres, ainda que de maneira minoritária e progressiva, que atuavam no campo de informações, com cursos no Brasil, principalmente o ofertado pela Escola Superior de Guerra (ESG), no Rio de Janeiro, e no exterior, com destaque para países como Estados Unidos, França e Inglaterra. No caso daqueles países, havia ainda o interesse em adquirir/conhecer a tecnologia, os equipamentos e fortalecer os contatos internacionais. O intercâmbio com países da América Latina também foi aprofundado, com relações mais próximas com Argentina, Chile, Paraguai e Uruguai (Quadrat, 2012). Tais relações seriam fundamentais a partir de 1964, quando os países do Cone Sul enfrentam sucessivos golpes e ditaduras que duraram até o início dos anos 1990, como é o caso chileno.

2. A criação do Serviço Nacional de Informações (1964-1974)

Com o golpe de 31 de março de 1964, que levou à deposição do presidente João Goulart, a estrutura do SFICI, que já era bastante criticada pela ausência de orçamento próprio, a falta de pessoal especializado e de bons equipamentos, foi considerada incapaz de dar conta da nova realidade do país. Os militares, que vinham participando ativamente dos debates, instituições e ações, avaliaram que era necessário reestruturar todo o sistema. Nesse sentido, embora a proposta de criação do Serviço Nacional de Informações (SNI) tenha sido idealizada pelo general Golbery do Couto e Silva em seu livro "Planejamento Estratégico" (1955), a implementação só ocorreu em 13 de junho de 1964, por meio da lei nº 4.341 (Quadrat, 2000). Não por acaso, o general foi seu primeiro chefe e responsável por toda a sua estruturação. Além disso, Golbery, às vésperas do golpe, atuava no Instituto de Pesquisas e Estudos Sociais (IPES), o qual, junto com o Instituto Brasileiro de Ação Democrática (IBAD), forneceu documentos e criou um extenso fichário com informações das principais lideranças políticas, sindicais e empresariais, bem como atuou fortemente na articulação da intervenção civil-militar de 1964.

O SNI era a estrutura central do Sistema Nacional de Informações, o SISNI, e responsável pela criação do Plano Nacional de Informações (PNI). Com isso, surgiu nos anos seguintes uma complexa e gigante estrutura que coordenava as atividades de informações e a repressão aos opositores do regime.

O SISNI era composto por todos os órgãos responsáveis pelo serviço de informação e contrainformação do país em todos os níveis de governo (federal, estadual e municipal) que já existiam ou foram sendo criados durante a ditadura. Assim, compunham o SISNI os seguintes órgãos (os quais em sua maioria também faziam parte do Sistema de Segurança Interna – SISSEGIN, conforme veremos): o SNI (Serviço

Nacional de Informações), as DSI (Divisões de Segurança e Informações), as ASI (Assessorias de Segurança e Informações), o CIEEx (Centro de Informações do Exterior do ministério de Relações Exteriores), FA-2 (segunda seção do EMFA), os E-2 (serviços secretos do Exército), os M-2 (serviços secretos da Marinha), as A-2 (serviços secretos da Aeronáutica), as S-2 (segundas seções dos três ministérios, distribuídas em cada organização militar), o CIE (Centro de Informações do Exército), os adidos do Exército (ADIEEx), o CISA (Centro de Informações da Aeronáutica), os adidos aeronáuticos (ADIAer), o CENIMAR (Centro de Informações da Marinha), os adidos navais (ADIDAL), os serviços secretos da Polícia Federal, os DEOPS (Departamento de Ordem Política e Social) e as P-2 (serviços secretos da Polícia Militar), os CODIs e os DOIs (Centro de Operações de Defesa Interna e Destacamentos de Operações Internas) e, em cada município, a Divisão Municipal (DM), subordinada ao DOPS (Quadrat, 2000). Embora chamada de comunidade de informações, as disputas por verbas, *status* e poder foram uma constante durante toda a ditadura.

Somando-se a essa estrutura, foi criado também o Sistema de Segurança Interna (SISSEGIN) que, a partir de 1970, na presidência do general Emílio Garrastazu Médici, sob coordenação do Ministro do Exército, Orlando Geisel, elaborou dois importantes documentos para a estruturação da perseguição aos oponentes políticos. Trata-se dos documentos intitulados Diretriz para Política de Segurança Interna e Plano de Segurança Interna. O SISSEGIN, após as mudanças legais asseguradas pelo Ato Institucional nº 5, de 13 de dezembro de 1968, coordenava os DOI-CODIs no território nacional, onde ocorreram os principais casos de mortes e desaparecimentos forçados nos anos 1970 no país.

Ao alocar a responsabilidade de coordenação do combate à subversão no Ministério do Exército, seu funcionamento passou a depender do bom ou mau relacionamento dos respectivos comandantes militares das três forças. A coordenação do ministro do Exército sobre a

direção das ações se dava em nível dos Estados-Maiores. Isso quer dizer que tanto o CISA quanto o CENIMAR, oficialmente, não tinham obrigação perante o SISSEGIN, pois na medida em que se subordinavam diretamente aos seus ministros ficavam acima desse sistema. Na prática, portanto, o sistema criado para centralizar as ações apenas conseguia fazê-lo quando havia colaboração dos devidos comandantes. De forma paralela à cadeia de comando, os serviços de informações da Aeronáutica e da Marinha mantinham, nos ministérios, ampla margem de ação, agiam normalmente com o conhecimento de seus comandos, colaborando com o sistema de acordo com os interesses de cada pasta ou do próprio órgão. Apenas o CIE, devido à subordinação direta ao Ministro do Exército, tinha obrigações para com o SISSEGIN (Antunes, 2002, p. 80).

A despeito dessa arquitetura, percebe-se que o funcionamento do sistema estava geralmente baseado nas relações pessoais entre os ministros militares, entre os comandantes de áreas e entre seus respectivos serviços de informações. No nível interno de cada força, ele ainda dependia das relações entre os comandantes, os chefes dos serviços de informações e seus respectivos ministros.

Sem problemas de hierarquia interna, o SNI também não enfrentava restrições orçamentárias. Ao contrário do antigo SFICI, o SNI nunca teve problemas de verbas, seu orçamento era um dos maiores do governo federal. Ainda que não fosse um ministério, seu chefe tinha cargo equivalente ao de ministro. Não por acaso, dois dos seus chefes foram presidentes durante a ditadura, Emilio Garrastazu Médici e João Baptista Figueiredo. Segundo Antunes (2002), o órgão passaria por duas grandes expansões: a primeira em 1967, com o endurecimento do regime e o surgimento da luta revolucionária, e a segunda no início do governo Figueiredo, quando a comunidade de segurança ainda tinha esperanças de eleger o chefe do SNI, general Otávio Medeiros, para a presidência e, com isso, conter o processo de transição iniciado em 1974.

O SNI teve ampla autonomia e grande contingente de pessoas que atuava diretamente na Agência Central, em Brasília, ou nas agências estaduais subordinadas. Sua estrutura era composta por uma Chefia, Seção de Informações Estratégicas, Seção de Segurança Interna e Seção de Operações Especiais. Com grande capilaridade, o SNI tinha ainda as Assessorias de Segurança e Informações (ASI) e as Divisões de Segurança Nacional (DSI). A primeira era o órgão de informações das entidades vinculadas a cada ministério – como empresas estatais e autarquias – e a segunda, o órgão central de informações em um ministério civil.

Na Agência Central funcionava um moderno estande subterrâneo de tiros, projetado e fabricado nos Estados Unidos, além do setor de tecnologia da agência. Nos anos 1980 houve crescimento substancial do órgão, quando montou um serviço médico próprio para aumentar sua autonomia frente às forças armadas, foi criada uma tropa de operações especiais, além de um setor policial em Brasília. Também foi desenvolvido o Projeto Prólogo, de onde surgiu o Centro de Pesquisa de Segurança de Informações (CEPESC), que naquela época mantinha estreita ligação com o Ministério das Relações Exteriores (Antunes, 2002, p. 58).

Como instituição central do SISNI, o SNI acumulou poder e ficou responsável pela formação de militares e civis que atuariam na área de informações. Nesse sentido, em 31 de março de 1971, quando a ditadura completava sete anos no poder, foi criada a Escola Nacional de Informações (EsNI – decreto nº 68.448), em Brasília, que, com o intuito de centralizar e padronizar as atividades, teria o monopólio da formação dos profissionais do setor no país. De acordo com o decreto de criação, os objetivos da EsNI eram: “preparar civis e militares para o atendimento das necessidades e informações e contrainformações do Sistema Nacional de Informações; cooperar no desenvolvimento da doutrina nacional de informações e realizar pesquisas em proveito do melhor rendimento das atividades do Sistema Nacional de Infor-

mações”. A EsNI absorveu, um ano depois, o antigo curso de informações oferecido até então no país pela Escola Superior de Guerra, inclusive parte do seu acervo e professores. Outros órgãos, como as Segundas Seções e o Centro de Estudos e Pessoal do Exército (CEPE), também tiveram parte do seu pessoal recrutado para a EsNI (Quadrat, 2022). A principal diferença apontada é o curso da ESG ser visto como muito teórico para o momento que o país vivia, em função do crescimento da luta revolucionária, enquanto o da EsNI seria mais prático. Para tal mudança, o grupo fundador da EsNI foi convidado a realizar cursos no exterior, mais precisamente no Estados Unidos, Alemanha, Israel, França e Inglaterra.

O grupo de trabalho para a criação da Escola foi instalado em 1º de março de 1971, e foram realizadas apenas seis reuniões sob a coordenação do general Ênio Pinheiro, contando com a presença de representantes da Presidência Da República, do Estado-Maior das Forças Armadas, dos ministérios da Aeronáutica, do Exército, da Marinha, da Justiça, das Relações Exteriores e do Planejamento e Coordenação Geral. O prazo para a apresentação do projeto era de 60 dias. Ênio Pinheiro informou logo de início que a escola seria em Brasília, que atenderia as necessidades do SISNI e que havia recursos orçamentários para sua criação. Houve concordância sobre os cursos, e ficou decidida a criação de três subgrupos de trabalhos, a saber: o que redigiria o decreto de criação e a exposição de motivos, o que faria o regulamento da escola e o que decidiria sobre as suas instalações físicas e orçamentos. Em seguida debateram-se os currículos e regimento (D’Araujo, Castro e Soares, 1994b).

A criação da EsNI envolveu ainda a construção de um espaço onde as atividades seriam desenvolvidas. Toda a obra no Setor Policial Sul de Brasília foi executada sob sigilo pela empresa Novacap, a mesma que havia construído a cidade. Na época havia a preocupação de uma possível infiltração no grupo de trabalhadores envolvidos na construção. Todos foram investigados. O sigilo exigido dificultava o trabalho de

quem atuava na obra, como engenheiros e arquitetos, que não podiam ter cópias das plantas e muitas vezes não tinham acesso a toda a informação sobre a construção dos prédios. Nesse sentido, em vez de um prédio apenas, foram construídos blocos independentes, afastados uns dos outros, com fins diferentes e controle de circulação do pessoal. No complexo havia um auditório para conferências, espaços para a simulação de ações, salas de aula, biblioteca, arquivo, acomodações para os alunos, refeitórios, salas de informática, estrutura desportiva, circuito interno de TV, estúdio de gravações, entre outros espaços.

Segundo Ana Lagôa (1983, p. 64), a EsNI foi aberta em maio de 1972 de maneira discreta, mas não sem uma cerimônia, com uma aula inaugural do então chefe do SNI, o general Carlos Alberto da Fontoura. Sem a presença da imprensa, em sua aula de cerca de 40 minutos, Fontoura afirmou que não se tratava da criação de uma escola de espíões, mas da formação de pessoal técnico que pudesse atuar de acordo com o Plano Nacional de Informações. O sistema havia crescido, e era chegada a hora de profissionalizar quem nele atuava.

A EsNI oferecia cursos tanto para civis quanto para militares, assim como recebia alunos brasileiros e estrangeiros, em sua maioria de países latino-americanos. A seleção das turmas acontecia a partir da abertura das vagas e da indicação dos chefes de possíveis alunos, pessoas consideradas de confiança e capacitadas para reforçar os laços da comunidade de informações. Além disso, de maneira inovadora para a época, a EsNI recebia mulheres em seus cursos, tanto como alunas quanto como funcionárias, em grande parte no setor de psicologia. A inscrição era feita mediante requerimento próprio e após a checagem da idoneidade e adesão ao regime, para saber se o candidato estava apto a frequentar os cursos da escola (Quadrat, 2022).

Dessa maneira, na EsNI existiam três cursos de níveis diferentes. O curso A (altos estudos) era destinado a militares e civis que ocupariam funções de chefia e de analistas. O recrutamento era feito entre

os oficiais superiores das forças armadas possuidores do Curso de Comando e Estado-Maior, e entre civis com nível superior. Considerado uma espécie de pós-graduação, o curso era realizado em 41 semanas e abrangia dois módulos, A e B. Aqueles que realizavam o curso B, estavam dispensados do módulo A. No currículo encontramos aulas sobre temas da realidade brasileira, análise de conjuntura e estudos de casos. Já o curso B (fundamentos) era destinado a civis e militares que ocupariam as funções de informações de nível médio ou de chefias em escalões intermediários do Sistema Nacional de Informações. Este curso era realizado em 20 semanas, e os recrutados eram majores ou capitães e civis com nível equivalente. O currículo do curso estava centrado em aulas de sociologia, história e ciência política. Era no curso B que se concentrava a formação de quem manejaria os informes e redigiria as informações. Nesse sentido, havia uma preocupação de disciplinar a escrita, de ensinar redação clara e objetiva, sem emitir opiniões. Pelo que podemos aferir da documentação disponível no Arquivo Nacional, o nível mais baixo era o curso C (operações), que compreendia dois subcursos: C1 e C2. O C1 era destinado a capitães e tenentes. O C2 era voltado para os sargentos. Portanto, existiam cursos para todos os níveis hierárquicos das forças armadas brasileiras. O objetivo era formar quadros para as chefias das seções de informações, bem como o planejamento e a direção de operações de informações. Os sargentos, por sua vez, seriam os agentes de informações. Nesse sentido, formavam os agentes que iriam às ruas. O currículo incluía técnicas de vigilância e interrogatório, escutas, gravações, disfarces, infiltração etc. (Quadrat, 2022).

Além dos cursos, a EsNI oferecia estágios de diferentes tipos, como de informações, contrainformações e operações. Eram oferecidos cursos de línguas estrangeiras (inglês, alemão, francês, holandês, espanhol, russo, chinês, italiano e árabe) de todos os níveis com aulas em modernas cabines individuais e teleaulas (com livros e fitas cassetes). Todos os alunos, com maior ou menor exigência, deveriam praticar atividades físicas e treinamento de tiro (Quadrat, 2022).

Chefe do SNI entre 1969 e 1974, nos anos mais repressivos da ditadura, o general Carlos Alberto da Fontoura, afirmou em entrevista que cerca de ¾ dos alunos eram civis e que no decorrer de um ano eram formados cerca de 120 alunos. Foram cerca de mil alunos em 10 anos. Como pudemos observar no acervo do SNI disponível para consulta no Arquivo Nacional, o sistema conseguiu produzir grande volume de documentação sobre os mais diversos setores da sociedade brasileira, como, por exemplo, as universidades públicas (Motta, 2014), movimentos pela anistia política em fins dos anos 1970 (Resende, 2015), entre outros.

3. Da transição à extinção do SNI (1974-1990)

O longo processo de distensão teve início quando o presidente Ernesto Geisel anunciou, em 1974, a “abertura lenta, gradual e segura”. Essa ação afetou particularmente os serviços de informações e repressão, tanto civis quanto militares. Ao longo de toda a ditadura, tais instituições haviam acumulado poder, gratificações e visibilidade política e social. O retorno à vida democrática poderia significar a perda de todo o capital acumulado. Além disso, era tempo de “arrumar a casa” para as incertezas da transição e o futuro do país. Foi naquele período que o SNI abrigou conhecidos militares associados a órgãos de repressão, como Carlos Brilhante Ustra, chefe do DOI-CODI de São Paulo, que, a partir de 1976, passou a comandar na EsNI um módulo nos cursos A, B, C1 e C2, para os quais escreveu a apostila “Cobertura de pontos e neutralização de aparelhos”. Ustra utilizou exemplos reais durante sua participação na linha de frente da perseguição aos oponentes políticos para ensinar como espionar, perseguir e prender a oposição, ou seja, ensinava as táticas e técnicas do DOI-CODI de São Paulo para os futuros agentes que, em princípio, não deveriam participar de tais ações. No entanto, Ustra não chegou sozinho ao SNI. Dois anos depois foi a vez de Freddie Perdigão Pereira, homem forte da repressão do Exército, ser acolhido juntamente com o seu grupo.

Além disso, como órgão principal do SISNI, o SNI forneceu informações que resultaram na captura de oponentes políticos do regime, alguns deles mortos ou desaparecidos. O SNI era também o principal contato com seus similares na América Latina e ativo diretamente no Plano Condor, a perseguição sem fronteiras a oponentes políticos das ditaduras do Cone Sul, que culminou na captura de estrangeiros no país, especialmente argentinos que nunca mais foram vistos (Quadrat, 2005).

Nesse sentido, devemos ressaltar que, diante das denúncias de violações dos direitos humanos e da identificação de espaços da repressão, bastante vinculadas às forças armadas, fomentou-se uma memória sobre o SNI quase que exclusivamente associada a sua atuação como órgão de espionagem, como se a instituição estivesse pouco associada à violência política que caracterizou a ditadura brasileira. A existência de tal narrativa ficou explícita no robusto levantamento historiográfico realizado pelo professor Carlos Fico, um dos maiores nomes da historiografia brasileira relativa à ditadura militar. Na obra "Além do golpe: versões e controvérsias sobre 1964 e a Ditadura Militar" (2004), o professor Fico fez uma pesquisa minuciosa sobre o SISNI e o SISSEGINT e sobre a produção de textos e depoimentos existente sobre os dois sistemas. Embora não ignore o impacto das informações repassadas para o sistema de segurança como um todo, e que o SNI também tenha se envolvido em diferentes casos de violência, o autor demonstra claramente a diferença de ênfase nas narrativas sobre os dois sistemas e como o SNI provocava medo muito mais pelas perseguições no âmbito das burocracias civis, pelas inviabilizações de emprego que poderia provocar, pelas demissões, em termos de entendimento cotidiano, do que por seu vínculo com a violência. Isso sem falar da narrativa militar sobre o tema. A própria Comissão Nacional da Verdade (2014) afirmou, em seu relatório final, que "dentro da chamada comunidade de informações, o SNI revelou-se o único organismo a ter as funções definidas, que eram coletar, armazenar, analisar, proteger e difundir informações sobre os opositores do

regime". No entanto, no mesmo Relatório Final, a Comissão apontou para a presença de agentes do SNI em locais onde ocorreram graves violações dos direitos humanos, como nos DOI-CODI.

O SNI era, na verdade, a face mais conhecida da repressão na ditadura, tendo em vista a publicização de sua existência, com seus chefes conhecidos e algumas atividades, como a criação da EsNI citada anteriormente, fatos divulgados pela imprensa, que muitas vezes estava presente. Muitas histórias foram contadas à época sobre possíveis fichas de políticos, informações que poderiam destruir carreiras e vidas pessoais. Sua complexidade, dimensão e poder levaram Golbery do Couto e Silva a afirmar que havia criado um monstro.

A perspectiva da democratização e o temor pela extinção do órgão, como demonstrou Sá (2024), fizeram que os principais dirigentes do SNI, além de vários outros militares, realizassem um forte *lobby* na Constituinte de 1988 e se aproximassem de parlamentares mais simpáticos às suas atividades. Também houve denúncias de espionagem sobre as atividades dos constituintes. Efetivamente, os militares asseguraram ao SNI alguns anos de sobrevida.

Existem várias posições, a maioria expressa por militares, para tentar explicar o processo que culminou no fim do SNI. Segundo a reportagem de Guiomar Campelo, por exemplo, divulgada no Correio Brasileiro em 18 de outubro de 1987, a medida já seria cogitada antes mesmo do fim da Constituição de 1988, uma vez que durante a presidência de José Sarney, o então ministro do Exército, general Leônidas Pires Gonçalves, defendeu não só sua extinção, como também a do Estado-Maior das Forças Armadas e do Gabinete Militar. Admitir que esses órgãos eram dispensáveis e caros seria a contribuição das forças armadas à reforma ministerial e administrativa que o presidente faria em 1987. Para Leônidas, os então ministérios do Exército, da Marinha e da Aeronáutica poderiam fazer as mesmas funções dos demais órgãos e ainda seria uma ação que deixaria o governo federal

bem-visto pela população naquele momento, dada a opinião pública negativa sobre o SNI (Campelo, 18 de outubro de 1987).

Se não estivéssemos falando do mesmo general que passava pelos corredores da Assembleia Constituinte, junto com seus companheiros, coibindo a ação dos parlamentares, sobretudo daqueles que tentavam propor temas progressistas na subcomissão relativa aos assuntos de Defesa, assegurando dessa forma a permanência do SNI, a não criação do Ministério da Defesa e a função de manutenção da responsabilidade das forças armadas pela lei e pela ordem (Brandão, *et. al.* 2023), talvez esta versão da história ganhasse alguma credibilidade.

Com um discurso um pouco distinto da falácia do general Leônidas, o general Ivan Souza Mendes, chefe do SNI no governo Sarney, apontava, ao final da década de 1980, uma redução de quadros e áreas de atuação do órgão, embora reconhecendo que não tenha havido necessariamente um corte no tipo de ações que vinham sendo desenvolvidas. Segundo o depoimento do general, ele havia procurado “dosar adequadamente o emprego dos meios que eu tinha para a atividade de informações e dei maior importância às informações externas” (Antunes, 2002, p. 63). Haveria naquele período o chamado “Projeto SNI”, que buscava, nas palavras de Mendes, redirecionar o órgão para alvos no exterior. Teria sido em função de tal projeto que Sarney transformou a Secretaria Geral do Conselho de Segurança Nacional em Secretaria de Assessoramento de Defesa Nacional (SADEN), da mesma forma que foi aprovado um novo regulamento para o SNI, quando foi inserida uma referência ao *habeas data*. O general afirmou que criou, no fim do mandato Sarney, um Grupo de Trabalho “com a função de estudar as novas necessidades da agência, organizacionais e estruturais, com o objetivo de propor novas medidas que permitissem a adaptação da agência à nova realidade política do país” (Antunes, 2002, p. 64). A reforma mesma não houve, pois o SNI foi extinto antes.

Um terceiro argumento, e o que mais se sobressai entre os militares (Antunes, 2002), relata que, durante sua campanha à Presidência, Collor teria solicitado uma audiência com o general Mendes, quem lhe teria dado um “chá de cadeira” de horas, e que, por vingança, Collor extinguiu o órgão.

Outra causa, talvez menos idiossincrática, diria respeito à política econômica neoliberal implementada pelo então presidente. Da mesma forma que acabou com o SNI, Collor extinguiu a Coordenação de Aperfeiçoamento de Pessoal Superior (CAPES), a Embrafilme e outros órgãos, evidenciando, como já havia proposto o general Leônidas, uma linha de ação administrativa que visava agradar seus apoiadores, no contexto do chamado enxugamento do serviço público, especialmente naquelas anos em que o Brasil enfrentava forte crise econômica e se consolidava o neoliberalismo no país (Almeida, 2024).

Seja qual for o peso específico de cada fator que levou à extinção do SNI, de modo geral é possível afirmar que, no tocante à memória dos anos de ditadura no Brasil, o começo dos anos 1990 contribuiu para que o SNI nunca se constituísse em um monstro similar àqueles conhecidos como “porões da ditadura”. Porões de onde figuras de torturadores ainda invadem a lembrança de quem vivenciou, de algum modo, a violência, ou mesmo o imaginário de quem possui uma mínima consciência sobre o que ocorreu naquele período. O SNI imprimia medo à vida do cidadão comum, mas também era um local a que muitas pessoas recorriam para fazer denúncias, seja por medos políticos ou vinganças pessoais.

Na memória de muitos protagonistas do regime, conforme registros em entrevistas e documentos, tratar-se-ia de uma agência que lidava com informações. Note-se que sequer se discutia a “legalidade” de como elas eram obtidas, ou a consequência de seu uso pela comunidade de informações e segurança, para perseguir, prender, torturar e matar oponentes políticos. Seus agentes, à exceção do último

chefe, o general Newton Cruz, que posteriormente foi inocentado no caso do assassinato do jornalista e informante do SNI Alexandre von Baumgarten, nunca foram responsabilizados por nenhuma das ações realizadas durante a ditadura.

Mesmo sem uma explicação definitiva para as razões da extinção do órgão, e tendo de lidar com as ambiguidades da memória nacional a respeito de sua trajetória institucional, o ano de 1990 inaugurou uma nova conjuntura crítica na história dos serviços de informação brasileiros.

4. O sistema de inteligência e a expectativa democrática (1990-1999)

A reorganização do sistema de inteligência brasileiro teve início com a posse do presidente Fernando Collor de Melo, marcada pela extinção do Serviço Nacional de Informações (SNI), juntamente com a extinção da Secretaria de Assuntos de Defesa Nacional (SADEN), em março de 1990, por meio da Medida Provisória nº 150.

Em que pesem as abordagens levantadas anteriormente, inclusive a antipatia do presidente em relação aos militares, a extinção do SNI não foi apenas reativa. A Medida Provisória nº 150 criou, no lugar do SNI e da SADEN, a Secretaria de Assuntos Estratégicos (SAE), que comportava um pequeno Departamento de Inteligência (DI/SAE). Não obstante tal perda imediata de *status* hierárquico, o Poder Executivo enviou para o Congresso o Projeto de Lei nº 1.862, de 1991, propondo a criação de um novo órgão federal de inteligência.

De todo modo, o DI/SAE foi o herdeiro imediato do espólio do SNI. Parte do pessoal do SNI, mantido no DI, procurou evitar que a extinção ocorresse na prática ou tentou trabalhar para que ela fosse revertida. Segundo o general Carlos Tinoco, ex-ministro do Exército no governo Collor, a alternativa a recriar o SNI teria sido a de preservar “algumas

de suas estruturas e o *modus operandi* dentro da SAE" (Antunes, 2002, p.112), mesmo com funções restritas à proteção de assuntos e documentos sigilosos, em nível nacional. Na prática, conforme a documentação disponível no Arquivo Nacional, as funções do DI/SAE não eram tão restritas e inercialmente mantinham o mesmo escopo, embora com recursos e autoridade reduzidos, do antigo SNI.

Cabe esclarecimento acerca da documentação oficial da época. Em 2005 o presidente Lula assinou decreto (nº 5.584) determinando que todos os documentos finalísticos de inteligência produzidos durante a época da ditadura militar deveriam ser recolhidos ao Arquivo Nacional, para depois serem disponibilizados ao público. Naquela época, já sob a responsabilidade da Agência Brasileira de Inteligência (ABIN), que seria criada oficialmente em 1999, encontravam-se documentos produzidos pelo Conselho de Segurança Nacional (CSN), pela Comissão Geral de Investigações (CGI) e pelo Serviço Nacional de Informações (SNI). Conforme determinado pelo decreto nº 5.584, de 2005, a documentação relativa às atividades finalísticas daqueles órgãos foi recolhida ao Arquivo Nacional (Arquivos do Regime, 18 de novembro de 2005). Também foram incluídos documentos relativos aos anos 1990.

Uma análise de parte daquela documentação nos permite afirmar que, no começo dos anos 1990, continuava ocorrendo espionagem a antigos oponentes políticos, com a presença de agentes em eventos universitários, em sedes de partidos e movimentos sociais. O formato do informe, os termos e expressões utilizados também não haviam mudado. Isso se deu porque não houve, naquele momento histórico, nenhuma nova doutrina ou mudança profunda na formação de quadros. Gerações de agentes formados pela ditadura, ainda que em número reduzido se comparado ao que o SNI fora um dia, seguiram trabalhando no DI/SAE e em outros órgãos da área no governo federal e dos Estados. Ademais, a estrutura seguiu militarizada durante algum tempo, o que não era esperado ou desejado em tempos democráticos, mas que deixou claro, juntamente com outras ações, como a anistia

aos servidores públicos civis e militares envolvidos com graves violações dos direitos humanos, como tais continuidades prejudicaram a transição à democracia no Brasil.

Apesar de tais permanências, seria ilógico e inconsequente afirmar que o poder do órgão civil federal de inteligência se manteve no mesmo patamar do antigo SNI. Houve, sem dúvida, já nos anos 1990, redução do poder militar, na medida em que o *status* de Departamento era baixo em meio às hierarquias estatais, em especial considerando as antigas prerrogativas que o SNI comportava. Collor também atingiu o calcanhar de Aquiles dos militares quando definiu que todas as chefias do Departamento, tanto a do órgão central quanto das Regionais, deveriam ser compostas por civis. De fato, foi ensaiada uma reforma do setor civil de inteligência quando o Executivo submeteu ao Congresso Nacional o Projeto de Lei nº 1.862, que tratava especificamente do monitoramento e redirecionamento da Atividade de Inteligência para o exterior:

sua atividade compreenderia a execução de ações direcionadas para a obtenção de dados e a avaliação de situações externas que pudessem implicar ameaças externas, veladas ou dissimuladas, e que fossem capazes de dificultar ou impedir a consecução dos interesses estratégicos do Brasil na cena internacional.

O projeto que redirecionava a atuação da inteligência para o exterior foi bem aceito por muitos atores políticos, mas não todos, a exemplo do ministro das Relações Exteriores, Francisco Rezek, que sustentou à época que o Itamaraty já possuía capacidades próprias para desempenhar tais função (Antunes, 2001, p. 122).

Desde a posse, a política do presidente Fernando Collor foi pautada por enfrentamentos com os militares. Não obstante, ao se sentir ameaçado diante das denúncias que corroeram seu governo, procurou uma nova abordagem, no sentido de angariar a simpatia da caserna. Retirou o PL 1.862 e o substituiu por outro, que procurava ampliar a

participação militar na esfera da inteligência. Retirava a Atividade de Inteligência da esfera da SAE e propunha a criação do Centro Federal de Inteligência (CFI)². O centro proposto seria responsável por "planejar, coordenar e executar as atividades civis de inteligência do governo federal; salvaguardar segredos de interesse do Estado; desenvolver programas e projetos de formação e aperfeiçoamento de recursos humanos na área de inteligência". O projeto não fazia nenhuma referência à formação de comissões mistas de controle, à supervisão congressual da atividade e ao controle orçamentário que não fosse exercido pelo Poder Executivo, a exemplo do que havia ocorrido com o projeto anterior. Tratava-se de uma forma de reduzir a intervenção civil em uma área considerada ainda estratégica para o setor militar. Não obstante, o movimento tardio de Collor não alcançou seus objetivos, e os conturbados acontecimentos políticos do ano de 1992, culminando na renúncia do presidente em 29 de dezembro, fizeram que o Poder Executivo retirasse o projeto da pauta política.

Com a saída de Collor, o vice-presidente Itamar Franco assumiu e deu nova organização à estrutura da Presidência da República, tratando de se cercar de militares nas mais distintas esferas, sendo a Polícia Federal e o DI exemplos daquele movimento. Itamar também reformulou a SAE, elevando seu secretário à categoria de ministro e nomeando para chefiá-la o almirante Mário César Flores. O presidente também transformou o Departamento de Inteligência em Subsecretaria de Inteligência (SSI)³, convidando para dirigi-la o coronel do Exército Wilson Romão, que teria passagem rápida pela SSI. Considerado amigo de Itamar, Romão seria logo nomeado Diretor Geral da Polícia Federal, gerando profundo descontentamento por parte dos policiais federais, sobretudo dos delegados, e desencadeando enorme crise dentro da Polícia Federal, bem como a primeira greve na história da instituição (Brandão, 2022, p. 292).

2 Projeto de lei 3.031-A de 29 de junho de 1992.

3 Lei nº 8.490 de 19 de novembro de 1992.

Quanto à SSI, é preciso destacar que a ela ficara subordinado o novo Centro Federal de Aperfeiçoamento de Recursos Humanos (CEFARH), considerado organização herdeira da EsNI, na segunda linha organizacional abaixo da SAE. Embora sob comando de um militar, a Subsecretaria de Inteligência continuaria sem acesso direto ao Presidente da República, subordinando-se ao ministro-chefe da SAE. Para fins de regulamentação, o então ministro Mário César Flores apresentou sua estrutura regimental, aprovada por meio do Decreto nº 782, de 25 de março de 1993.

Portanto, a extinção do SNI reduziu o poder castrense no centro de governo, inclusive simbolicamente, mas não o destruiu. Diversos agentes foram demitidos, muitos militares retornaram para suas forças de origem, muitos foram para a reserva, mas diferentes funções do SNI migraram para e continuaram ativas no Centro de Inteligência do Exército⁴. O *modus operandi* do SNI também permaneceu na Subsecretaria de Inteligência (SSI), fosse como legado institucional ou modo de resistência à desarticulação da antiga comunidade de informações (Antunes, 2002, p. 112).

Do ponto de vista de diretrizes da Presidência da República, a ausência de evidências sobre sua existência nos leva a concluir que, nos governos de Fernando Collor e de Itamar Franco, a relevância atribuída à inteligência era mínima e problemática, pois a falta de interesse permitia atuação bastante autônoma. Não havia tampouco orientações da SAE aos funcionários do DI ou da SSI. Segundo o depoimento do ex-ministro, almirante Mário César Flores, a Eugênio Diniz (Diniz, 1994, p. 115), a SAE foi, na percepção do ministro, principalmente, uma herdeira da antiga Secretaria-Geral do Conselho de Segurança Nacional e não do Serviço Nacional de Informações.

4 Ver depoimentos dos militares no livro: D'ARAUJO Maria Celina, SOARES, Gláucio Ary Dillon e CASTRO, Celso (Orgs.). A volta aos quartéis: a memória Militar sobre a abertura. Rio de Janeiro: Relume-Dumará, 1995.

O desprestígio da Atividade de Inteligência na pauta política durante a primeira década sob a Constituição de 1988 pode ser atribuído a três fatores principais. Primeiro, o repúdio da maioria da opinião pública às estruturas associadas à ditadura militar. Segundo, o medo do tipo de enfrentamento que poderia ser produzido em relação aos militares. Este segundo fator ficou evidente na renúncia a implementar medidas características da Justiça de Transição (Brandão; Cepik, 2024). Terceiro, a negligência acerca do papel da Atividade de Inteligência nas relações de poder internacionais e a necessidade de desenvolver políticas próprias de um regime democrático tendo em vista o papel da inteligência nas distintas áreas de atuação do Estado nacional.

Com a eleição de Fernando Henrique Cardoso (FHC) em 1994, novos desdobramentos institucionais começaram a emergir, ainda que lentamente. A primeira proposta para a criação do que viria a ser a Agência Brasileira de Inteligência (ABIN) foi apresentada pelo governo FHC na medida provisória (MP nº 813) que reorganizava a Presidência da República, em 1º de janeiro de 1995. No entanto, o presidente foi criticado por propor a criação de órgão de inteligência por meio de uma MP, ao ponto de precisar retirar a proposta e se comprometer com um debate público. No ano seguinte, em 21 de maio de 1996, ocorreu audiência pública na Câmara dos Deputados, organizada pela Comissão de Defesa Nacional. Ao longo da década de 1990, pelo menos três deputados então filiados ao Partido dos Trabalhadores (PT) propuseram legislação visando à criação e regulamentação do setor de inteligência: José Fortunati, José Dirceu e Jacques Wagner (Antunes, 2002)⁵.

Após a realização da audiência pública na Comissão de Defesa Nacional, a tramitação de todos os projetos foi suspensa, aguardando projeto de iniciativa do Poder Executivo que proporia a criação da ABIN.

5 Para uma discussão sobre todas as propostas apresentadas por parlamentares e pelo Executivo, ver: ANTUNES, Priscila C. B. *SNI e ABIN. Uma leitura da atuação dos serviços secretos brasileiros ao longo do século XX*. Rio de Janeiro: Editora FGV, 2002.

Na prática, porém, o governo se referia e tratava a ABIN como se ela já existisse, o que era problemático por si. De fato, o governo só avançou na aprovação do novo marco legal depois da reeleição de FHC em 1998.

5. Do surgimento da ABIN e do SISBIN até a crise mais recente (1999-2022)

Quando estudamos a reforma de instituições vinculadas aos setores de defesa, segurança pública, chancelaria e inteligência, muitas vezes compreendemos suas particularidades recorrendo ao estudo neoinstitucionalista de Amy Zegart. De acordo com a autora, em sua obra *"Flawed by Design: The Evolution of the CIA, JCS and NSC"* (1999), as características marcantes do desenvolvimento das burocracias no campo da segurança e da defesa são distintas das burocracias no campo social ou de política econômica. Em resumo, as burocracias da área de segurança e defesa, mesmo em contextos democráticos, tendem a ser criadas por iniciativa do Poder Executivo, com um papel secundário e relutante do Legislativo. Ademais, as escolhas sobre o desenho organizacional e as regras iniciais estabelecidas refletiriam o ordenamento institucional prévio do Poder Executivo e as disputas entre setores da própria burocracia, que tende a dominar tecnocraticamente o debate especializado, protegida pelo segredo governamental. Por causa das características anteriores, o Congresso acabava por exercer uma forma de supervisão pouco sistemática e inefetiva. Desse modo, tanto nas democracias mais consolidadas quanto nos países legatários das ditaduras, é difícil democratizar as questões relativas às áreas de defesa e segurança. De certa forma, em um mundo marcado por altos níveis de desigualdade, temas como moradia, saúde e educação tendem a mobilizar mais os setores sociais organizados e a obter maior prioridade na agenda pública (Zegart, 1999).

O modelo de Zegart nos ajuda a compreender também o processo que levou à criação da ABIN. A baixa participação parlamentar, decorrente do pouco preparo da maioria dos Congressistas para lidarem com o

tema, em um contexto de Presidência forte e baixa densidade de interesses envolvidos com o tema na sociedade civil, explica por que, apesar da longa tramitação, houve poucos avanços na lei de criação da ABIN e do SISBIN em 1999 em relação ao projeto do Poder Executivo apresentado em 1996.

A Lei nº 9.883, aprovada pelo Congresso Nacional e sancionada pelo Presidente FHC em dezembro de 1999, estabeleceu formalmente a ABIN e criou também um Sistema Brasileiro de Inteligência (SISBIN). Tanto a ABIN quanto o SISBIN, sob a coordenação da agência, teriam a função de integrar as ações de planejamento e execução das atividades de inteligência do país, o que inclui o processo de obtenção, análise e disseminação “de informações necessárias ao processo decisório do Poder Executivo” e a salvaguarda da informação “contra o acesso de pessoas ou órgãos não autorizados” (Art. 1º). Para efeitos de sua aplicação, a Lei nº 9.883, de 1999, definiu a Atividade de Inteligência como

uma atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado.

O artigo 2º determinou que todos os órgãos e entidades da Administração Pública Federal que possam produzir conhecimentos de interesse das atividades de inteligência, especialmente os responsáveis pela defesa externa, segurança interna e relações exteriores, fariam parte do SISBIN e que, mediante os ajustes necessários, as Unidades da Federação poderiam compô-lo. A lei de 1999 veda o uso dos serviços de inteligência para a perseguição política ou para atender a interesses privados dos dirigentes e autoridades. Nos termos da lei, a ABIN passou a desempenhar o papel de órgão coordenador do sistema, cabendo-lhe:

planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País” e “I – planejar e executar ações, inclusive sigilosas, relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o Presidente da República; II – planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade; III – avaliar as ameaças, internas e externas, à ordem constitucional; IV – promover o desenvolvimento de recursos humanos e da doutrina de inteligência, e realizar estudos e pesquisas para o exercício e aprimoramento da Atividade de Inteligência”.

A legislação aprovada em 1999 foi um avanço, sendo a instituição da ABIN um marco importante entre os marcos da Constituição de 1988, juntamente com a criação do Ministério da Defesa e a transformação da Casa Militar em Gabinete de Segurança Institucional (GSI). As três novas instituições passariam por crises e controvérsias ao longo das décadas seguintes. No caso da lei de criação da ABIN e do SISBIN, vale destacar dois problemas que já eram evidentes à época.

Em primeiro lugar, a Lei nº 9.883, de 1999, regulamentava apenas a atuação da ABIN e não dos demais órgãos que viriam a compor o SISBIN. Não foram regulamentadas, de modo particular, as atividades de inteligência e contrainteligência das forças armadas, das polícias estaduais e da Polícia Federal, todas com impactos importantes sobre as capacidades estatais e o funcionamento das instituições democráticas. Em segundo lugar, o balizamento geral do escopo de atuação do sistema foi muito vago. A lei não definiu a estruturação hierárquica do sistema, não forneceu informações sobre a subordinação do SISBIN, não atribuiu a quem deveria responder e não regulamentou que tipo de coordenação poderia ser exercida sobre seus componentes. Tampouco definiu se haveria controle operacional da ABIN sobre os componentes ou apenas coordenação, que passaria a depender do tipo de relacionamento entre os dirigentes de cada órgão.

Deduz-se, com base no modelo proposto por Zegart e diante das evidências documentais disponíveis, que o desenho institucional da ABIN atendeu às preferências e interesses mais amplos do grupo alinhado com o general Alberto Cardoso (que anteriormente era responsável pela SSI e depois passou a comandar o Gabinete de Segurança Institucional [GSI] da Presidência da República)⁶. Tal conclusão sobre o papel do general Cardoso fica reforçada quando se considera a decisão, tomada em 2000, já no contexto da primeira crise do setor de inteligência vivida sob a nova legislação, de subordinar a ABIN ao GSI.

Tampouco houve interesse do Legislativo em estabelecer os marcos de controle sobre a agência. Embora a Lei nº 9.883, de 1999, também tenha determinado a criação de um órgão de controle, apenas no final de 2000, no decorrer da crise do BNDES, houve reação do Congresso Nacional no sentido de criar efetivamente a Comissão de Controle da Atividade de Inteligência (CCAI). Como se saberia mais tarde, foi somente em 2013, por meio da Resolução nº 2 do Congresso Nacional, que essa comissão passaria a ter regras de funcionamento e composição devidamente institucionalizada. A CCAI é uma comissão permanente, composta por seis representantes da Câmara e seis do Senado, e tem autoridade formal para acesso irrestrito a todas as informações e locais das agências e órgãos de inteligência do SISBIN. A CCAI tem poderes para realizar investigações, requerer documentos, aprovar o nome do diretor geral da ABIN após indicação do Presidente da República, receber reclamações e convocar os responsáveis dos órgãos a dar explicações sempre que julgar necessário. Entretanto, a análise dos anos iniciais de funcionamento da CCAI indica que a comissão tem atuação puramente reativa, lenta, pouco eficaz e exclusivamente focada na ABIN, não no SISBIN como um todo (Brandão, 2010).

6 Em entrevista com Priscila Brandão e Celso Castro, o general afirmou que a proposta inicial seria estabelecer os marcos fundamentais, para depois dar seguimento aos arranjos institucionais que comporiam o sistema (Brasília, 14 de abril de 1999).

O fraco desempenho da CCAI contrasta com o fato de que o período entre 2000 e 2014 foi de grande expansão do número de órgãos membros do SISBIN e de precária institucionalização de outros instrumentos de controle externo sobre a Atividade de Inteligência (Cepik, 2022). Além da subordinação da ABIN ao GSI e da expansão do SISBIN, conforme decreto aprovado em 2002⁷, houve também expansão ainda maior do Subsistema de Inteligência de Segurança Pública (SISP)⁸, criado em 2000, e do Sistema de Inteligência de Defesa (SINDE), criado por portaria do Ministério da Defesa em 2002⁹. No caso do SISBIN, portarias subsequentes do GSI regulamentaram o funcionamento do Conselho Consultivo e as regras de intercâmbio de informações entre os componentes do sistema¹⁰. Durante os governos de coalizão liderados pelo PT, não houve alteração legal na arquitetura de funcionamento da inteligência, à exceção da extinção do GSI no segundo governo Dilma Rousseff, transformado em Casa Militar em 2015 e recriado em 2016, quando Michel Temer assumiu a presidência após o controverso *impeachment* de Rousseff.

Este período de expansão dos sistemas foi caracterizado pelo aumento do número de órgãos e frações administrativas dedicados à Atividade de Inteligência definida amplamente, além de um investimento substancial na área. Como destaca Cepik (2022), a expansão foi causada por três fatores principais. Primeiro, o agravamento da crise de segurança pública nos anos 2010. Segundo, o novo posicionamento regional e global do Brasil nos mandatos do presidente Lula. Terceiro, a realização de um ciclo longo de grandes eventos, que teve início ainda em 2007, com os Jogos Pan-Americanos, passando pela Conferência das Nações Unidas Para o Desenvolvimento Sustentável, em 2012, a Copa do Mundo em 2014 e os Jogos Olímpicos

7 Decreto nº 4376, de 13 de setembro de 2002.

8 Decreto nº 3695, de 21 de dezembro de 2000.

9 Portaria Normativa nº 295 do Ministério da Defesa de 3 de junho 2002.

10 Portarias 24-GSI-PR de 20 de dezembro de 2002 e 239-GSI-PR de 20 de junho de 2003.

em 2016. A expansão organizacional e orçamentária do setor também foi acompanhada por maior uso de metodologias típicas da Atividade de Inteligência, inclusive no setor privado da economia. Também sobre essa expansão no setor privado são necessárias pesquisa adicional e atenção dos órgãos de controle.

Mesmo sem institucionalização igualmente robusta dos instrumentos de controle externo sobre a inteligência, a estabilidade política do período 1994-2014 e a melhoria dos indicadores de desenvolvimento se traduziram em incremento da legitimidade das atividades de inteligência, principalmente a partir da aprovação da Lei de Acesso à Informação (LAI), em 2011.

Ainda assim, houve crises, fracassos e denúncias que atingiram o setor de inteligência na fase de maior expansão sob o regime democrático da Constituição Federal de 1988. Basta lembrar das crises desencadeadas pela Operação Satiagraha e pela revelação dos documentos que comprovavam a espionagem do governo americano contra a Presidência da República e a Petrobras (caso Snowden).

O aumento da polarização política e a crise econômica a partir de 2014 iniciaram um novo período na história da inteligência, no qual o desenho institucional legado do presidencialismo de coalizão seria crescentemente pressionado por novas dinâmicas na sociedade e no regime. A conjuntura entre 2015 e 2018 seria marcada por instabilidades e novos fatos: a polarização política provocada pelos impactos da Operação Lava-Jato, pelo *impeachment* da presidente Dilma Rousseff, pela política de austeridade do governo Temer e a recessão econômica decorrente, pela prisão do ex-presidente Lula, pela baixa popularidade de Temer e pela intervenção federal no Rio, culminando na eleição de Jair Bolsonaro. Durante o governo Temer, sob forte influência do general Sérgio Etchegoyen, então ministro do GSI, foram publicados dois decretos, o primeiro em 2016, que estabelecia uma Política Nacional de Inteligência (PNI), e o segundo em 2017, que esta-

belecia uma Estratégia Nacional de Inteligência (ENINT). Mesmo contando com dois documentos de orientação geral para o sistema, com a eleição de Jair Bolsonaro para a Presidência da República em 2018, surgiram mais controvérsias e denúncias de ilegalidades na conduta de diferentes órgãos brasileiros de inteligência durante os quatro anos seguintes¹¹.

Os acontecimentos dos últimos anos ainda estão sendo investigados pelas autoridades competentes, mas ensejam uma reflexão sobre as tensões entre institucionalização e condicionantes culturais. As instituições, formais e informais, são importantes porque organizam as ações coletivas e definem as regras das interações entre os agentes. Mas a cultura, por sua vez, influencia fortemente a maneira como os agentes interpretam tais regras e atribuem significado para suas ações (Helmke e Levitsky, 2006).

Este tipo de questão aparece justamente no processo de profissionalização dos servidores que atuam na área de inteligência. Todas as profissões se definem por um alto grau de exigência em termos de requisitos cognitivos, valorativos e de sociabilidade (Durkheim, 1983). No caso da área de inteligência, Thomas Bruneau (2001) destacou a necessidade de combinar um tipo específico de conhecimentos e habilidades com um tipo específico de fraternidade interna à organização. Entretanto, o comportamento dos agentes sempre envolve a cultura e os valores externos à própria organização. Portanto, Cepik e Antunes (2002) entendem que o profissionalismo da atividade envolve a combinação

entre um *ethos* burocrático na conduta, que está ligado à impessoalidade das normas, com um *ethos* meritocrático na regulação das carreiras, que diz respeito à própria relação dos indivíduos com

11 Ver: <https://www.poder360.com.br/brasil/em-2020-bolsonaro-disse-ter-sistema-particular-de-informacoes>. Acesso em 20/07/2024.

a organização, e um *ethos* democrático, que diz respeito à socialização dos valores e à relação entre principais e agentes dentro de uma atividade profissional qualquer (Cepik; Antunes, 2002, p. 112).

Em um *survey* respondido por 47 servidores do quadro permanente de nível superior da ABIN em 2002, que considerou quatro conjuntos de critérios propostos para a análise do processo de desenvolvimento profissional dentro da ABIN (conhecimentos, carreira, formação e código de ética), os autores encontraram uma tendência positiva em termos de diversidade de gênero, parâmetros éticos e formação acadêmica. Na época, haviam ocorrido dois concursos, em 1994 e em 1998. Posteriormente, ocorreriam concursos públicos em 2004, 2008, 2010 e 2018. Mesmo persistindo problemas diversos do ponto de vista da gestão de pessoas, inclusive pendências de regulamentação da Lei 11.776, de 2008, que dispôs sobre o Plano de Carreiras e Cargos da ABIN, nos parece evidente que o padrão de profissionalização em uma agência civil, com finalidade exclusiva de prover inteligência, sujeita a pelo menos alguns controles externos democráticos e de conformidade, é distinto de outros modelos. A recente aprovação de um código de ética formal na ABIN é um indicador a mais nesta conclusão¹².

Basta notarmos as crises profundas ocorridas nos sistemas de inteligência menos profissionalizados de outros países da região, como Colômbia, Peru, Equador e Argentina. No caso do Brasil, ainda existem déficits de institucionalização e diferenças de cultura entre diferentes componentes do SISBIN e também entre os órgãos federais e os componentes de inteligência nos Estados e municípios. Contudo, seria preciso avançar nas pesquisas comparativas sobre a formação, os valores e comportamentos do pessoal empregado nesse tipo de atividade nas forças armadas, nas polícias, no setor financeiro e tributário e outros, sobretudo pensando em termos da convergência

12 O Código de Ética e Conduta dos Agentes Públicos da ABIN foi aprovado por meio da PORTARIA Nº 66/GAB-DIVAP/GAB/DG/ABIN/GSI/PR, de 17 de fevereiro de 2022.

ou não do *ethos* burocrático, meritocrático e democrático em diferentes situações.

Um exemplo da tensão entre regras institucionais e cultura política ocorreu na época da Operação Satiagraha, ainda na década de 2000, que apurava o desvio de verbas públicas e corrupção, conduzindo à prisão políticos, empresários, doleiros, diretores de bancos e outros indivíduos. Na ocasião, as provas produzidas contra o principal alvo, o banqueiro Daniel Dantas, foram anuladas, pois foi considerada ilegal a participação de 76 agentes da ABIN na investigação, os quais tinham acesso às interceptações telefônicas que teriam servido de provas (Conselho de Justiça Federal, 2011).

Na prática, aquela decisão judicial orientou um novo comportamento dentro do Sistema, quando deixou claro que a cooperação do SISBIN tinha limites impostos pelos regulamentos de persecução penal e não pela lei que criava o SISBIN. A confusão entre investigação policial e inteligência foi banida posteriormente (ao menos como prática acriticamente aceita). Mas, na época, quando se falava em "sistema", especialmente um no qual a ABIN era o coordenador central e a Polícia Federal um membro destacado, não estava claro como essas relações deveriam ser estabelecidas. Esse é um exemplo de como a clarificação de regras institucionais pode induzir mudanças comportamentais.

Na direção contrária, o caso mais recente da chamada "ABIN Paralela", durante o governo Bolsonaro, indica que, mesmo diante de significativos avanços institucionais, uma cultura permissiva para com o uso politicamente enviesado de recursos de poder pode ensejar comportamentos em desacordo com as finalidades estabelecidas legal e doutrinariamente. As investigações sobre o uso abusivo de ferramentas de vigilância e de desvios de finalidade para atender interesses privados da família Bolsonaro ainda estão em andamento, mas pesam sobre dirigentes e funcionários públicos cujo envolvimento, se com-

provado, caracterizaria as práticas do período como comportamento oficial, não “paralelo”.

Segundo D’Araujo (2021), Bolsonaro se elegeu apesar de propagar um discurso que defende a tortura e os violadores dos direitos humanos, de se comportar de forma indecorosa em relação às mulheres, criminalizando orientações sexuais não hétero e, entre outros, atacando a Constituição Federal e o Poder Judiciário, em uma evidente atitude de desrespeito às leis. Durante sua gestão ficou conhecido mundialmente “por sua face antidemocrática, racista, negacionista, misógina e messiânica” (D’Araujo, 2021, p. 87). Subordinado a Bolsonaro, no comando do GSI durante os quatro anos do mandato do presidente, estava o general Augusto Heleno R. Pereira, que, já em 1977, havia conspirado contra o projeto de “distensão” política do general Geisel e que, em 2005, fora afastado do comando da Operação de Paz da ONU no Haiti (MINUSTAH) a pedido da Comissão Interamericana de Direitos Humanos. O mesmo Heleno manejou recursos milionários durante a realização dos V Jogos Mundiais Militares, em que foram identificadas muitas irregularidades pelo Tribunal de Contas da União (Castro, 2021). Com currículo ainda menor na área de inteligência, o delegado Alexandre Ramagem foi o diretor ABIN entre 2019 e 2022, quando deixou o cargo para se candidatar a deputado federal, após ter sua indicação para Diretor Geral da Polícia Federal barrada pelo Poder Judiciário. Dentre as controvérsias associadas a sua gestão, consta que teria traído a confiança de seus aliados ao gravar e circular imagens e áudio de uma reunião, captadas sub-repticiamente pelo próprio Ramagem, nas quais se debatia o uso da máquina governamental para favorecer os filhos do presidente, investigados pela Receita Federal do Brasil (RFB), bem como falas de Bolsonaro e Heleno sobre as possibilidades de intervenção na Receita e no Serpro (Agência Senado, 2024).

Tais comportamentos e denúncias indicam tensão entre parâmetros institucionais que vinham avançando em uma determinada direção, e uma cultura política fortemente autoritária e clientelista, de profundo

enraizamento no Brasil, como já alertava o historiador Sérgio Buarque de Holanda nos anos 1930.

6. A crise do 8 de janeiro e a reforma da ABIN e do SISBIN (2023-)

Foram gravíssimos os acontecimentos que marcaram o início do terceiro mandato de Luiz Inácio Lula da Silva (2023-2026) como presidente do Brasil. Após vencer as eleições contra Bolsonaro por uma margem estreita em 2022, houve crescente tentativa de membros do governo anterior e de setores da burocracia estatal e da sociedade para subverter os resultados da eleição, culminando nos ataques violentos às sedes dos três poderes constitucionais em Brasília, no dia 8 de janeiro de 2023.

Em meio à crise que se seguiu à tentativa fracassada de golpe de Estado, Lula indicou para dirigir a ABIN, em fevereiro de 2023, o delegado Luiz Fernando Corrêa, ex-Secretário Nacional de Segurança Pública e ex-Diretor Geral da Polícia Federal, respectivamente, nos dois governos anteriores de Lula. Mesmo com resistências internas a seu nome na ABIN, sejam aquelas motivadas pelo fato de Corrêa ser oriundo da PF, sejam pela oposição à agenda de reformas propostas, a indicação foi aprovada pelo Senado Federal com ampla votação. A nova gestão na ABIN iniciou um conjunto de mudanças que ainda demanda avaliação crítica, mas que, indubitavelmente, tentou responder, em um dos principais órgãos do SISBIN, aos desafios colocados pelo 8 de janeiro de 2023¹³.

Em primeiro lugar, a ABIN deixou de ser subordinada ao GSI e passou para a esfera da Casa Civil, conforme o Decreto nº 11.426, de março

13 Texto preparado a partir das informações disponíveis pela própria Agência. <https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/abin-iniciou-em-2023-uma-nova-etapa-na-inteligencia-brasileira>.

2023. Devido àquela medida, a ABIN ficou obrigada a redefinir e repacificar seus níveis e perfis de serviço de assessoramento de inteligência para os diferentes ministérios, incluindo o GSI.

Em segundo lugar, o Decreto nº 11.693, de setembro de 2023, produziu a maior reforma institucional na governança do Sistema Brasileiro de Inteligência desde 2002, detalhada em portarias complementares publicadas desde então. Basicamente, o decreto procurou resolver problemas de heterogeneidade entre os órgãos, de falta de objetividade nos critérios para o ingresso de novos órgãos e de baixa efetividade na governança. Além de especificar melhor as funções da ABIN como órgão coordenador do sistema, foi reformulado também o CONSISBIN, que passou a ser formado pelos ministros da Casa Civil (presidindo), do GSI, da Justiça e Segurança Pública, das Relações Exteriores e da Defesa, além do Diretor Geral da ABIN (secretariando)¹⁴.

Em terceiro lugar, a reorganização da própria ABIN, por força do Decreto nº 11.816, de dezembro de 2023. Além da separação organizacional entre os eixos de produção de inteligência (interna, externa e contrainteligência), o decreto especificou melhor as competências das diversas unidades da agência nas áreas de inteligência cibernética, de operações, de formação e doutrina, de gestão e de controles e governança.

Em discursos públicos e documentos, a agência passou a buscar posicionamento mais estratégico e transparente. Foram definidas como prioridades para 2024, por exemplo, a avaliação de riscos e ameaças nas ações de desintrusões de terras indígenas, na realização do Concurso Público Nacional Unificado (CPNU), na realização das eleições municipais, nos eventos do G20 e nas ações preparatórias para a presidência brasileira do BRICS e da COP-30, eventos que serão realizados em 2025 no país. Embora não seja possível avaliar aqui os

14 Ver: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/cartilha-do-novo-sisbin-e-lancada>. Acesso em 03/10/2024.

resultados dessas e outras iniciativas e ações, como aquelas implicadas no Programa Nacional de Proteção do Conhecimento Sensível (PNPC), a maior transparência quanto às áreas de atuação e os temas permite que os governantes e os órgãos de controle avaliem de forma mais permanente e profunda a Atividade de Inteligência da ABIN e dos demais órgãos do SISBIN, o que, historicamente, apenas ocorreu em situações de crises e escândalos no Brasil.

Por fim, vale destacar a publicação, em dezembro de 2023, de uma nova Doutrina da Atividade de Inteligência¹⁵. Trata-se de uma visão de doutrina da ABIN, não do SISBIN como um todo, mas o documento foi publicado ostensivamente e tende a influenciar o debate sobre a Atividade de Inteligência em outros órgãos do SISBIN (incluindo o SINDE e o SISP) e no público interessado. Dividido em cinco partes principais, o documento explicita fundamentos políticos (inclusive internacionais), constitucionais, legais e éticos para a existência de uma atividade permanente e estatal de inteligência. Também explicita entendimentos sobre os ramos de inteligência e de contrainteligência, bem como sobre os elementos de análise e de operações que singularizam a atividade.

Trata-se de avanço em relação, por exemplo, à situação da Doutrina Nacional de Inteligência de Segurança Pública (DNISP), que ainda hoje não foi publicada ostensivamente, apesar do enorme contingente de profissionais que atuam na área no governo federal e nos Estados e municípios. A DNISP começou a ser elaborada em 2003, mas os debates pararam e foram retomados em 2005, com forte influência da doutrina do SISBIN de 2004¹⁶ e da DISPERJ de 2005¹⁷. A DISPERJ

15 Ver: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/doutrina>. Acesso em 05/10/2024.

16 Manual de Inteligência – Doutrina Nacional de Inteligência – Bases Comuns; Brasília, Gráfica – Abin. 2004.

17 Governo do Estado do Rio de Janeiro. Secretaria de Estado de Segurança Pública. Subsecretaria de Inteligência. Doutrina de Inteligência de Segurança Pública do Estado do Rio de Janeiro (DISPERJ). Abril de 2005.

havia sido elaborada por um coronel reformado que fora integrante do Centro de Informações do Exército durante a ditadura. Neste sentido, na primeira versão da DNISP, a principal diferença em relação à antiga Doutrina de Informações recaía sobre a noção de “Inteligência Policial Judiciária”¹⁸. De modo bastante problemático, por exemplo, considerava-se que enquanto a investigação é orientada pelo modelo de persecução penal, tendo como objetivo a produção de provas (com norma processual própria), a inteligência estaria orientada para a produção de conhecimentos, mas “excepcionalmente” poderia produzir provas (Brandão, 2010). A DNISP foi aprovada oficialmente em 2009, depois revisada em 2013 e 2015, mas os problemas foram mantidos¹⁹.

Neste sentido, a nova formulação empreendida pela Doutrina de Inteligência divulgada pela ABIN atualiza o debate em diálogo com a literatura internacional mais recente. Também permite uma melhor explicitação sobre as diferenças (e eventuais contradições) entre inteligência de Estado e inteligências setoriais especializadas, sejam elas militares, policiais, judiciais, fiscais ou ambientais.

Conclusão

A produção de conhecimentos especializados para subsidiar o processo decisório no Brasil nas áreas de segurança, chamados de informações até 1990 e de inteligência desde então, surgiu no Brasil de forma permanente no século passado. Na esfera civil, a primeira missão da Atividade de Inteligência foi atuar como polícia política na década de 1920. Ao longo da primeira metade do século XX, sobretudo durante a ditadura do Estado Novo, praticamente não há evidências de que a atividade tenha sido mobilizada para outras funções menos

18 Secretaria Nacional de Segurança Pública. Doutrina Nacional de Inteligência de Segurança Pública. 4ª Edição. Revista e ampliada. (classificada)

19 Secretaria Nacional de Segurança Pública. Doutrina Nacional de Inteligência de Segurança Pública. 4ª Edição. Revista e ampliada. (classificada)

repressivas, com a possível exceção da contrainteligência. Após a deposição de Vargas e fortemente influenciada pela experiência do Exército na Segunda Guerra Mundial, os militares brasileiros começam a desenhar institucionalmente o que viriam a ser os primeiros órgãos civis de inteligência com missões mais abrangentes, como o SFICI e o SNI. Mesmo assim, sobretudo no caso do SNI, as percepções de ameaça e as atuações eram fortemente marcadas pelo posicionamento do regime brasileiro durante a Guerra Fria e pelo enfrentamento contra a oposição desarmada e armada nos chamados anos de chumbo. Mesmo depois da Constituição Federal e da ruptura causada pelo governo Collor, o debate sobre o que deveria ser e fazer um sistema de inteligência federal foi adiado e marcado por crises.

Apesar da ausência de debates parlamentares e na sociedade, o que resultou em diretrizes e parâmetros legais bastante genéricos e ambíguos, o sistema de inteligência se expandiu significativamente nas últimas duas décadas. Durante o governo Bolsonaro (2019-2022) agudizou-se a crise no setor de inteligência, culminando nos eventos de 8 de janeiro de 2023.

Ao se aproximar de completar 25 anos, o SISBIN, e a ABIN como seu órgão coordenador e responsável pelo assessoramento ao Presidente da República e seus ministros, têm como desafios dar continuidade a um processo de reforma que permita superar cabalmente traços culturais indesejáveis e algumas inconsistências institucionais recorrentes na trajetória brasileira. Reconhecemos a complexidade da definição das políticas públicas relacionadas à Atividade de Inteligência. A cadeia de atores relevantes para o seu desenho institucional, aplicação e controle, bem como os fatores que pesam sobre essas possibilidades, tornam o desafio significativo, mas ainda assim necessário num mundo em profunda transformação.

Referências

Legislação

- Decreto nº 9.775-A, de 6 de setembro de 1946.
- Decreto nº 44.489-A, de 15 de setembro de 1958.
- Decreto nº 45.040, de 6 de dezembro de 1958.
- Decreto nº 68.448, de 31 de março de 1971.
- Projeto de Lei nº 1.862, de 1991.
- Projeto de Lei nº 3.031-A, de 29 de junho de 1992.
- Lei nº 8.490, de 19 de novembro de 1992.
- Decreto nº 782, de 25 de março de 1993.
- MP nº 813, de 1º de janeiro de 1995.
- Lei nº 9.883, de 7 de dezembro de 1999.
- Decreto nº 3.695, de 21 de dezembro de 2000.
- Portaria Normativa nº 295, do Ministério da Defesa, de 3 de junho de 2002.
- Portaria nº 24, do GSI, de 20 de dezembro de 2002.
- Portaria nº 239, do GSI, de 20 de junho de 2003.
- Manual de Inteligência Doutrina Nacional de Inteligência Bases Comuns; Brasília, Gráfica – Abin. 2004
- Governo do Estado do Rio de Janeiro. Secretaria de Estado de Segurança Pública. Subsecretaria de Inteligência. Doutrina de Inteligência de Segurança Pública do Estado do Rio de Janeiro (DISPERJ). Abril de 2005
- PORTARIA Nº 66/GAB-DIVAP/GAB/DG/ABIN/GSI/PR, de 17 de fevereiro de 2022.
- Decreto nº 11.426, de 1º de março de 2023.
- Decreto nº 11.693, de 6 de setembro de 2023.
- Decreto nº 11.816, de 6 de dezembro de 2023.

Bibliografia

AGÊNCIA SENADO. Humberto diz que gravações de Ramagem comprovam existência de “Abin paralela”. 16 de julho de 2024. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/07/16/humberto-diz-que-gravacoes-de-ramagem-comprovam-existencia-de-201cabin-paralela201d>. Acesso em: 16 out. 2024.

ALMEIDA, Valesca. **Transferir, transformar e desativar: neoliberalismo e desestatizações na transição da ditadura à democracia no Brasil (1974-1985)**. Niterói: PPGH-UFF, 2024.

ANTUNES, Priscila C. B. **SNI e ABIN: uma leitura da atuação dos serviços secretos brasileiros ao longo do Século XX**. Rio de Janeiro: Editora FGV, 2002.

Arquivos do regime militar são abertos. **Memorial da Democracia**, 18 de novembro de 2005. Disponível em: <http://memorialdademocracia.com.br/card/aceso-publico-a-arquivos-da-ditadura>. Acesso em: 16, out. 2024.

BRANDÃO, Priscila C., CARVALHO, Bernardo R., TEIXEIRA, Carla Drielly dos Santos e ROCHA, Igor Tadeu Camilo Rocha. **Ilegais e imorais. Autoritarismo, interferência política e corrupção dos militares na história do Brasil**. Belo Horizonte: Editora Fino Traço, 2023.

BRANDÃO, Priscila C. “A Polícia Federal no processo de transição: o desafio da Justiça de transição e da superação dos valores autoritários, analisados a partir da gestão do delegado Romeu Tuma”. **Tempo**. Niterói, vol. 28, n. 1, Jan/Abr, 2022.

BRANDÃO, Priscila C. “Homens cordiais, filhotes da ditadura: uma leitura da escalada do poder dos delegados da Polícia Federal na virada do século XX para o XXI” **SÆCULUM – Revista de História** [v. 27, n. 47]. João Pessoa, p. 284-305, jul./ dez. 2022.

BRANDÃO, Priscila C. Amerino Raposo e a Polícia Federal: quando o medo do esquecimento se traduz na obsessão pela imposição de uma narrativa. **Faces da história**, Assis-SP, v.6, nº1, p.246-270, jan.-jun., 2019.

BRANDÃO, Priscila C. e CEPIK, MARCO A. C. **Inteligência de Segurança Pública. Teoria e Prática no controle da criminalidade.** Niterói: Editora Impetus, 2013.

BRANDÃO, Priscila C. e CEPIK, MARCO A. C. Forças Armadas e Serviços de Inteligência no Brasil. In: D'ARAUJO, Maria Celina e REZENDE, Lucas Pereira. **Forças Armadas e Política no Brasil Republicano.** A Nova República (1988-2018). Rio de Janeiro: FGV Editora, 2024.

BRASIL. Comissão Nacional da Verdade. Relatório / Comissão Nacional da Verdade. – Recurso eletrônico. – Brasília: CNV, 2014. 976 p. – (Relatório da Comissão Nacional da Verdade – Volume 1 – página sem numeração).

BRITTO, Ângela. **"A polícia política na década de 1920: a gênese e atuação da 4ª Delegacia Auxiliar. "A sala de detidos": Atuação e ascensão da Polícia Política da Capital Federal do Brasil, 1920-1937.** Tese de doutorado apresentada ao Programa de pós-graduação em História, Política e Bens Culturais do CPDOC/FGV. 2011.

BRUNEAU, Thomas C. "Controlling Intelligence in new democracies," **International Journal of Intelligence and CounterIntelligence** 14, no. 3, 2001.

CAMPELO, Guiomar. Reforma acaba com SNI e EMFA : Leônidas admite que órgãos são dispensáveis e caros. *Correio Braziliense*, Brasília, nº 8954, p. 3, 18/10.

CANCELLI, Elizabeth. **A organização policial. O mundo da violência.** Brasília: Editora UNB, 1994.

CASTRO, Lúcio D. "Desvios, fraudes e licitações arranjadas: o esquema comandando por generais que desviou milhões em verba pública", *Sportlight*, 28 set. 2021. Disponível em: <https://agenciasportlight.com.br/index.php/2021/09/28/desvios-fraudes-e-licitacoes-arranjadas-o-esquemacomandado-por-generais-que-desviou-milhoes-em-verba-publica/>. Acesso em: 27 jul. 2023.

CEPIK, Marco A. C. "Brazil". In: MATTEI, Florina C.; HALLADAY, Carolyn; ESTEVEZ, Eduardo. *The Handbook of Latin American and Caribbean Intelligence Cultures*. Maryland: Rowman and Littlefield, 2022. Pages 91-109.

CEPIK, Marco e ANTUNES, Priscila. Profissionalização da Atividade de Inteligência no Brasil: Critérios, Evidências e Desafios. In: Suzana Lemozy; Russel Swenson. (Org.). **Intelligence Professionalism in the Americas**. Washington D.C: Joint Military Intelligence College, 2003.

COMISSÃO NACIONAL DA VERDADE. Relatório Comissão Nacional da Verdade. Brasília: Presidência da República, 2014, v. 1. Disponível em: http://cnv.memoriasreveladas.gov.br/images/pdf/relatorio/volume_1_digital.pdf. Acesso em: 14 jan. 2019.

CONSELHO DE JUSTIÇA FEDERAL. STJ: É ilegal a participação da ABIN na Operação Satiagraha. **Justiça Federal**. 2 de março de 2011. Disponível em: <https://www.cjf.jus.br/cjf/outras-noticias/2011/marco/stj-e-ilegal-a-participacao-da-abin-na-operacao-satiagraha>. Acesso em? 16, out. 2024.

D'ARAUJO, Maria C. "O autoritarismo eterno e o Brasil do século XXI", *Mundos Plurales*, n. 8, 2021. Disponível em: <https://repositorio.flacsoandes.edu.ec/handle/10469/17705>. Acesso em: 24 jul. 2023.

D'ARAUJO, Maria Celina, CASTRO, Celso e SOARES, Gláucio Ary Dillon (orgs). **Visões do golpe: a memória militar sobre 1964**. Rio de Janeiro, Relume Dumará, 1994a.

D'ARAUJO, Maria Celina, CASTRO, Celso e SOARES, Gláucio Ary Dillon (orgs). **Os anos de chumbo: a memória militar sobre a repressão**. Rio de Janeiro, Relume Dumará, 1994b.

D'ARAUJO, Maria Celina, CASTRO, Celso e SOARES, Gláucio Ary Dillon (orgs). **A volta aos quartéis: a memória militar sobre abertura**. Rio de Janeiro, Relume Dumará, 1995.

D'ARAUJO, Maria Celina, CASTRO, Celso e SOARES, Gláucio Ary Dillon (orgs). **Democracia e Forças Armadas no Cone Sul**. Rio de Janeiro, FGV, 2000.

D'ARAUJO, Maria Celina, CASTRO, Celso e SOARES, Gláucio Ary Dillon (orgs). **Ernesto Geisel**. Rio de Janeiro, FGV, 1997.

DINIZ, Eugênio. *Estratégia, Informação e Defesa Nacional*. Novos Estudos, CEBRAP, n.39, jul. 1994.

DURKHEIM, Emile. **A Divisão do Trabalho Social**. São Paulo: Martins Fontes, 1983.

FICO, Carlos. **Como eles agiam**. Rio de Janeiro, Record, 2001.

FICO, C. *Além do golpe: versões e controvérsias sobre 1964 e a Ditadura Militar*. Rio de Janeiro: Record, 2004.

FIGUEIREDO, Lucas. **Ministério do Silêncio**. Rio de Janeiro: Record, 2005.

HELMKE, Gretchen; LEVITSKY, Steven [editors]. **Informal Institutions and Democracy: Lessons from Latin America**. Baltimore, The Johns Hopkins University Press, 2006.

HOLLANDA, Sérgio Buarque de. "O homem cordial". In: *Raízes do Brasil*. 26a Edição. São Paulo. Companhia das Letras, 1995.

LAGÔA, Ana. **SNI: como nasceu, como funciona**. São Paulo, Brasiliense, 1983.

MOTTA, Rodrigo P. S. "A cultura política brasileira e o desafio da democracia". **ComCiência**, UNICAMP, v. 1, 2015.

MOTTA, Rodrigo P. S. **As universidades e o regime militar**. Rio de Janeiro: Zahar, 2014.

OLIVEIRA, Nilo. "**A centralização do sistema**". (1956 a 1961). Tese de doutorado apresentada ao Programa de História Social da Pontifícia Universidade Católica de São Paulo, 2013.

QUADRAT, Samantha. *Global Intelligence Academies: Information Schools during the Civil-Military Dictatorship in Brazil*. In: Rüdiger Bergien; Debora Gerstenberger; Constantin Goschler. (Org.). **Intelligence Agencies, Technology and Knowledge Production**. 1ed. Abingdon: Routledge, 2022.

QUADRAT, Samantha. A preparação dos agentes de informação e a ditadura civil-militar no Brasil. *Varia História*. v. 28, p. 19-41, 2012.

QUADRAT, Samantha. *A repressão sem fronteiras: perseguição política e colaboração entre as ditaduras do Cone Sul*. Niterói: PPGH-UFF, 2005.

QUADRAT, Samantha. *Poder e informação: o sistema de inteligência e o regime militar no Brasil*. Rio de Janeiro, IFCS/UFRJ, 2000.

RESENDE, Pamela. *Os vigilantes da ordem*. Rio de Janeiro: Arquivo Nacional, 2015.

SÁ, Laís Nóbrega Gabetto de. "SNI 2ª FASE": o Serviço Nacional de Informações no processo constituinte brasileiro (1985-1988). Rio de Janeiro: PPGH-UNIRIO, 2024.

SILVA, Golbery do Couto e. *Planejamento Estratégico*. São Paulo: Companhia Editora Nacional, 1955.

ZEGART, Amy. *Flawed by Design. The Evolution of the CIA, JCS and NSC*. Stanford-CA: Stanford University Press, 1999.



Breve histórico da Cooperação em Inteligência: Dinâmicas atuais para a Reformulação do SISBIN

Leonardo Singer Afonso

Oficial de Inteligência
Superintendente no Paraná

Cintiene Sandes Monfredo Mendes

Professora Adjunta
Escola Superior de Defesa (ESD)

Em 7 de dezembro de 1941, o Serviço Aéreo Imperial da Marinha Japonesa atacou a base naval estadunidense de Pearl Harbor, em Honolulu, no Havaí. O propósito da ação militar era destruir a Frota do Pacífico dos Estados Unidos e impedir que intervisse nos interesses expansionistas do Japão na região. O ataque se aproveitou do elemento surpresa, encontrando um inimigo desprevenido. Apesar de não ter atingido integralmente seu objetivo, foi contundente e traumático a ponto de forçar a entrada dos Estados Unidos na Segunda Guerra Mundial.

Naqueles meses finais de 1941, a tensão diplomática entre os EUA e o Império do Japão crescia velozmente, e a perspectiva de guerra entre essas potências figurava no horizonte de ambas. Era de se esperar que o aparato de inteligência estadunidense estivesse apto para interpretar com precisão a gravidade da situação e para além da retórica diplomática ambígua do Império japonês. Por isso, a perplexidade causada pela impressionante vulnerabilidade norte-americana no momento do bombardeio energizou o debate interno acerca das falhas de inteligência que teriam permitido o fator surpresa utilizado pelo adversário.

Após o fim da II Guerra, comissões de investigação governamentais e privadas se debruçaram sobre o ataque surpresa japonês a Pearl Harbor. Em suma, concluíram que a ausência de alertas representava falha grave de inteligência motivada por múltiplos fatores, sobretudo pela falta de integração de análises departamentais e coordenação do compartilhamento de informações entre as inteligências estadunidenses. O insumo crítico que reforçaria a crença de que um ataque japonês aos Estados Unidos era iminente se encontrava fragmentado em diversas agências¹.

Existiam lacunas fundamentais na compreensão dos contextos conflitivos, causadas mais especificamente pela falta de uma camada de análise de inteligência capaz de contextualizar e articular as informações a partir de uma perspectiva multidimensional. Ainda que os setores militar, diplomático e de segurança possuíssem suas agências de inteligência dedicadas, os decisores responsáveis pelo planejamento estratégico amplo do Estado estavam privados dessa capacidade de assessoramento direto e dependiam dos resultados fragmentados e restritos provenientes das agências de inteligência departamental²,

1 A falha de inteligência que privou os Estados Unidos de um alerta estratégico capaz de mitigar os efeitos de um ataque daquelas proporções apenas reforçou percepção que vinha se avolumando desde o período entre as duas guerras mundiais. Conflitos internacionais, inclusive a guerra, eram assuntos cuja complexidade havia crescido ao ponto de exigirem tratamento amplo, para além do foco de burocracias especializadas: *"The First World War had indeed shown that total war needed total intelligence; foreign military power had come to depend on factors of industrial capacity, demography and morale which fell outside the analysis of normal military and naval intelligence"* (Herman, 1996, p. 25).

2 Agências de Inteligência Departamental se referem aos organismos orgânica e legalmente dedicados ao assessoramento do processo decisório de autoridades cujas atribuições se restringem a um setor específico ou pasta governamental. Entre eles, para fins de exemplificação, temos no Brasil a Assessoria de Inteligência de Defesa (AIDef), órgão central do Sistema de Inteligência de Defesa e subordinada ao Estado Maior Conjunto das Forças Armadas e ao Ministério da Defesa, e a Secretaria Nacional de Segurança Pública do Ministério da Justiça (SENASP), órgão central do Subsistema de Inteligência de Segurança Pública e subordinada ao Ministro de Estado da Justiça.

que se dedicavam a responder necessidades de camadas decisórias muito específicas, como a do Secretário de Estado ou, à época, do Secretário de Guerra.

Como efeito do acirramento da Guerra Fria a partir de 1946, foi publicado o *National Security Act* de 1947. A necessidade de maior compartilhamento e integração das informações estratégicas em nível nacional compôs o conjunto de novas concepções que fundamentaram as propostas de estruturas que substituiriam o antigo aparato de inteligência norte-americano. Após longos debates acerca do nível de centralidade necessário para aumentar a coordenação entre as agências de inteligência, decidiu-se estabelecer uma agência central de natureza integradora, a *Central Intelligence Agency*, mas preservando as burocracias departamentais independentes e autônomas que, em conjunto, formaram o que se conhece hoje como a “comunidade de inteligência” estadunidense.

O desenrolar da Guerra Fria e as características desse conflito político-ideológico passaram a impor aos demais Estados adaptações institucionais que foram satisfeitas por intermédio da absorção de modelos experimentados e considerados bem-sucedidos. Ademais, a concepção norte-americana³ de um sistema de inteligência espalhou-se por muitos países ocidentais durante a Guerra Fria também como uma necessidade estratégica dos Estados Unidos⁴. Foi o caso da adaptação sofrida pelo aparato de inteligência brasileiro a partir da década de 1950.

3 Grosso modo, essa concepção previa um sistema formado por agências de coleta especializada de dados e de produção de inteligência setorial organizadas ao redor de uma estrutura central integradora vinculada diretamente a chefes de Estado ou a setores responsáveis pela segurança nacional.

4 De acordo com Hughes-Wilson (2016, p. 268): “*Nowadays, it is axiomatic that a single assessment and tasking staff must coordinate and integrate a nation's intelligence effort at the highest level like any other scarce resource*”.

De acordo com o general Rubens Denys, em entrevista fornecida ao Centro de Pesquisa e Documentação Histórica/FGV citada por Brandão (2002), haveria um compromisso do governo brasileiro com o governo americano de se criar um serviço nos moldes da CIA como parte de estratégia de fortalecimento das estruturas dos países da OEA, que era de “extremo interesse para o governo americano”. Nesse contexto, em 1946, foi criado o Serviço Federal de Informações e Contrainformações.

A partir daí, em função das configurações políticas que se impuseram no Brasil desde então, os sistemas de inteligência brasileiros que se seguiram sofreram adaptações mais ou menos drásticas. Atualmente, o Sistema Brasileiro de Inteligência (SISBIN) é a última forma do processo de adaptação desse aparato, não mais por meio da influência norte-americana, mas em razão do processo de redemocratização iniciado na década de 1980 e dos desafios que se impuseram ao País desde então. Não obstante apresentar diferenças com relação ao modelo estadunidense, preserva também seus elementos centrais.

O funcionamento do SISBIN vem sendo vagarosamente aperfeiçoado desde sua criação. Entretanto, inconstâncias em seu desempenho demandaram melhorias complexas e que transcendessem a intensificação das relações entre seu órgão central, a Agência Brasileira de Inteligência (ABIN), e os demais membros do sistema. Foi necessário repensar e privilegiar fundamentos, estrutura e estratégia para garantir que o SISBIN proporcionasse a integração apropriada dos conhecimentos departamentais para o cumprimento de suas atribuições estabelecidas por lei.

Problemas como o baixo engajamento dos membros às necessidades do sistema; a estagnação do fluxo das informações compartilhadas, a despeito do crescimento do número de membros; a baixa capacidade de coordenação e supervisão do órgão central; e a persistência de processos e ferramentas insuficientes para operacionalização do fluxo de informações e conhecimentos se somaram à carência de instru-

mentos legais com condão de conferir maior legitimidade ao arranjo, segurança à Atividade de Inteligência de Estado, seus servidores e à sociedade que goza de seus resultados.

A falta de atenção e discussão aprofundada sobre a inteligência de Estado⁵ no âmbito do governo e da sociedade enfraqueceu a infraestrutura e o arcabouço legal da atividade, fragilizando o SISBIN. Também reduziu o ritmo do empoderamento de sua principal agência de inteligência, a ABIN, redundando em um sistema de supervisão fraca, o que se reflete inclusive na capacidade dos órgãos de controle externos da atividade.

Mais recentemente, essas disfuncionalidades passaram a ficar claras não somente para os profissionais da área e categorias correlatas, habituadas a lidar com questões de inteligência, mas também para o público em geral. Em 2023, a readequação do SISBIN passou a ser prioridade manifesta pelo próprio Presidente da República à ABIN, que precisou se debruçar sobre os problemas e iniciar um processo de restabelecimento do sistema e da Atividade de Inteligência de Estado no Brasil.

No mesmo ano, a ABIN recriou setor responsável exclusivamente pela gestão do SISBIN nos âmbitos federal e estadual. A equipe de oficiais de inteligência reunida para esse fim passou a coletar material e perspectivas de usuários e profissionais de inteligência para analisar a situação do SISBIN, com o propósito de formalizar diagnóstico do qual partiriam soluções baseadas na priorização dos problemas mais urgentes.

5 Não há uma definição pacificada para o termo “inteligência de Estado”. Contudo, uma definição possível que utilizamos para fins de entendimento desse capítulo, é que a inteligência de Estado se refere ao assessoramento de usuários cujas responsabilidades sejam supradepartamentais. Nesse sentido, contrasta com a inteligência departamental, afeta às decisões restritas de pastas governamentais. Essa definição sugerida deriva do conceito de “inteligência nacional”.

É nesse sentido que, a partir daqui, passaremos a analisar o SISBIN e suas principais debilidades, para justificarmos o mais recente esforço de adequação do funcionamento desse sistema de inteligência nacional.

1. Da criação do SISBIN e sua estrutura interagencial

O SISBIN foi criado a partir da Lei Nº 9.883, de 7 de dezembro de 1999, e inicialmente regulado pelo Decreto Nº 4.376, de 13 de setembro de 2002, posteriormente revogado pelo Decreto Nº 11.693, de 6 de setembro de 2023. A lei atribuiu ao SISBIN o propósito de integrar "... as ações de planejamento e execução das atividades de inteligência do País, com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional" (Brasil, 1999). Tal como o modelo de sistema de inteligência estadunidense, ficou estabelecido que o SISBIN assessoraria a esfera representada e simbolizada pelo "Presidente da República", cuja magnitude das decisões demandaria integração de informações e análises que transcenderiam objetivos departamentais trabalhados pelas inteligências e setores de informação ministeriais.

Na lei ficou também explícito o esforço pela estruturação do novo sistema ao estabelecer que "os órgãos e entidades da Administração Pública Federal que, direta ou indiretamente, possam produzir conhecimentos de interesse das atividades de inteligência, em especial aqueles responsáveis pela defesa externa, segurança interna e relações exteriores, constituirão o SISBIN" (Brasil, 1999). Houve previsão, inclusive, da inserção das unidades da Federação como membros. Esse dispositivo específico foi idealizado para que se tornasse essencial para a instrumentalização do intercâmbio adequado de informações entre os níveis federal, estadual e municipal.

Na mesma lei foi criado o órgão central do SISBIN, a ABIN. A ela ficou reservada a tarefa de integrar as informações produzidas no âmbito

do Sistema a fim de assessorar sobretudo ao Presidente da República. Nesse sentido, o Parágrafo Único do art. 4º, que elenca as atribuições da ABIN, estabelece que “Os órgãos componentes do Sistema Brasileiro de inteligência fornecerão à Abin, nos termos e condições a serem aprovados mediante ato presidencial, para fins de integração, dados e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais” (Brasil, 1999).

O estabelecimento por lei de um usuário é o orientador do propósito de uma agência de inteligência específica, mas nunca uma “reserva de mercado” para essa agência. A depender do contexto, o principal cliente do SISBIN recebe assessoramento, de acordo com os limites legais, de onde desejar. Do centro do seu sistema, idealmente, ele pode esperar a inteligência que deriva da integração das informações de múltiplas fontes e conhecimentos provenientes dos demais setores do governo de forma suficientemente ampla a ponto de se adequar às necessidades de seu nível de decisão.

Igualmente relevante é chamar a atenção para o fato de que o SISBIN se conforma como um ambiente de intercâmbio de informações. Nesse sentido, acaba não sendo uma via de mão única. Idealmente, o assessoramento vertical, devido ao Presidente da República, convive com o assessoramento horizontal, que tem o condão de fortalecer, de maneira complementar, a tomada de decisão em níveis departamentais. Ademais, o estímulo ao compartilhamento⁶ amplia a disponibilidade de informações para as demais agências de inteligência, fortalecendo subsistemas e instituições singulares de inteligência em suas atribuições específicas.

6 O processo de compartilhamento de informações no contexto do SISBIN não pode ser confundido com assessoramento horizontal. O primeiro se refere ao fluxo de insumos que, integrados, derivarão em um produto de inteligência. O segundo diz respeito à produção e difusão de conhecimentos de inteligência com o propósito de responder a uma demanda informacional de uma instância decisória departamental.

Por fim, o Decreto 4.376/02 determinou a organização e o funcionamento do SISBIN. Nele foram elencados todos os órgãos e ministérios que comporiam o sistema, bem como foram definidos os setores da ABIN responsáveis pela sua operacionalização. Também foi instituído o Conselho Consultivo do Sistema Brasileiro de Inteligência (CONSISBIN), composto por grupo reduzido de instituições membros, cujas competências envolviam capacidades deliberativas, como a incorporação de novos membros.

Essa prerrogativa da Lei pressupõe um sistema já idealizado aos moldes de uma estrutura de cooperação entre diferentes órgãos que, ao fazerem parte de uma arquitetura de inteligência, estariam compartilhando informações, dados e conhecimento para garantir mecanismos de preparo aos tomadores de decisão no mais alto nível estratégico. Ainda que a inteligência mantenha como responsabilidade a compartimentação da informação, na garantia de segurança e proteção de informações sensíveis, o modelo interagências do SISBIN notadamente mantém o compartilhamento e trocas de conhecimento como essencial.

Para Kapucu (2006), o compartilhamento de informações é essencial para organizações que trabalham em rede. A conjuntura atual, de ameaças complexas e ambiente desafiador quanto ao fluxo informacional, tornou relevante a construção de uma rede interorganizacional, estabelecida a partir de uma governança, capaz de difundir conhecimento, trocar experiências e robustecer as análises frente a questões de segurança nacional. Comunicação e coordenação multiorganizacional tornaram-se foco de diversas atividades interagenciais como forma de adaptar-se à nova vulnerabilidade e preocupar-se em aperfeiçoar políticas públicas de rápida resposta.

Bardach (2001) destaca que, ao unir esforços e compartilhar informações, as agências podem enfrentar problemas complexos de maneira mais integrada, resultando em soluções mais eficazes e abrangentes.

Essa sinergia, especialmente em contextos de segurança nacional, onde a fragmentação das informações pode comprometer a resposta a ameaças emergentes torna-se essencial. Para fins dessa perspectiva, os modelos de inteligência, já reportados historicamente, bem como o SISBIN, iniciaram suas estruturas de forma a compartilhar e integrar agências em um mecanismo de rede.

A regulamentação que criou o Sistema Brasileiro de Inteligência e sua agência central se mostrou conceitualmente coerente em relação à aspiração brasileira a um arranjo amplo com funções integradoras e direcionado ao nível máximo do processo decisório do Executivo Federal, tal como preconizava o modelo de sistema de inteligência criado pelos Estados Unidos em 1947. Contudo, o processo de reconstrução da inteligência de Estado no Brasil, iniciado em 1999, progrediu lentamente e, após o estabelecimento de seus fundamentos, permaneceu sujeito ao aparente desinteresse governamental e caminhou na esteira de contextos negativos e crises, o que permitiu o acúmulo de problemas e a elaboração de soluções meramente paliativas.

Ao longo do tempo, o arcabouço legal que sustenta o SISBIN se provou insuficiente para que uma democracia como o Brasil lide com um sistema que representa o nível máximo desse setor de tamanha sensibilidade. Muito antes, ainda em 2002, Brandão (2002, p.174) criticava "Para um debate que já se arrastava há quase 10 anos, a regulamentação de um sistema brasileiro de inteligência deixou a desejar".

Problemas percebidos – mas não oficialmente diagnosticados – na condução do SISBIN ao longo dos últimos 25 anos, como o baixo engajamento dos membros às necessidades do sistema; a estagnação do fluxo das informações compartilhadas, a despeito do crescimento do número de membros; a baixa capacidade de coordenação e supervisão do órgão central; e a persistência de processos e ferramentas insuficientes para operacionalização do fluxo de informações e conhecimentos se somam à carência de instrumentos legais com con-

dão de conferir maior legitimidade ao arranjo, segurança à Atividade de Inteligência de Estado, seus servidores e à sociedade que goza de seus resultados.

Mais recentemente, essas disfuncionalidades passaram a ficar claras não somente para os profissionais da área e categorias correlatas, habituadas a lidar com questões de inteligência, mas também para o público em geral. Em 2023, a readequação do SISBIN passou a ser prioridade manifesta pelo próprio Presidente da República à ABIN, que precisou se debruçar sobre os problemas e iniciar um processo de restabelecimento do sistema e da Atividade de Inteligência de Estado no Brasil.

No mesmo ano, a ABIN recriou setor responsável exclusivamente pela gestão do SISBIN nos âmbitos federal e estadual. A equipe de oficiais de inteligência reunida para esse fim passou a coletar material e perspectivas de usuários e profissionais de inteligência para analisar a situação do SISBIN, com o propósito de formalizar diagnóstico do qual partiriam soluções baseadas na priorização dos problemas mais urgentes.

2. Diagnóstico do SISBIN

Ainda durante as exposições técnicas realizadas na Audiência Pública de 21 de maio de 1996, organizada pela Comissão de Defesa Nacional e que precederam as discussões que ensejaram a Lei 9883/1999, foram expostos dilemas que continuam atuais e fundamentais de serem analisados. Na ocasião citada, antecipando a dificuldade que o SISBIN apresentaria no que diz respeito à sua governança, o general Alberto Cardoso ressaltou que “a organização do sistema não conotaria nenhuma ideia de hierarquia. Os componentes do sistema não estariam subordinados à ABIN, que apenas produziria a integração das informações repassadas pelos órgãos com vista à segurança de Estado”⁷ (Brandão, 2002).

⁷ A concepção da ABIN pelo legislador, expressa por sua lei de criação, confere-lhe capacidades próprias de coleta de informações, inclusive sigilosas. Portanto, o trabalho dessa

A observação feita pelo general Cardoso foi uma cautela que encontra respaldo na história e na prática moderna de outros sistemas de inteligência. É comum em países democráticos que essas estruturas sejam compostas por membros independentes e autônomos que têm o dever institucional de contribuir para o esforço de consolidação da inteligência devida ao processo decisório nacional. No entanto, a ideia de integração das fontes, dos dados coletados e das análises de inteligência produzidas em nível departamental é um princípio fácil de falar, mas extremamente difícil de colocar em prática. Todas as agências de inteligência possuem seu próprio monopólio de segredos em campos específicos, e da mesma forma, todas evidentemente relutam em contá-los às agências parceiras (Hughes-Wilson, 2016, tradução nossa).

Ainda de acordo com esse autor, há dois motivos básicos para que esse fenômeno ocorra no contexto dos sistemas de inteligência: primeiramente, todas as agências deste ramo tendem a acentuar questões de segurança da informação, pois insumos compartilhados sem o devido cuidado representam riscos graves, como perda de controle dos métodos de coleta e das próprias fontes. Em complemento à ideia do autor citado, pode-se considerar que a obtenção de informação não é necessariamente uma prática barata e pode não somente ter exigido volumoso aporte financeiro, mas também ter sido executada às custas de grande esforço institucional. Mais ainda: o tratamento inadequado de algumas informações pode colocar em risco a vida de profissionais de inteligência e de fontes humanas recrutadas operacionalmente. A regra básica sempre foi: não se compartilha determinadas informações com qualquer um.

Em segundo lugar, coloca-se uma razão nada edificante, mas, ainda de acordo com Hughes-Wilson (2016), compreensível. Burocracias ten-

agência não se limita à integração do que se recebe do sistema. Para atender as necessidades do nível de decisão definido por lei, a ABIN as interpreta e planeja a reunião de dados em função da necessidade de complementação das informações que o SISBIN e bancos de dados próprios já disponham.

dem a competir entre si. Agências que detêm monopólio sobre fontes específicas de informação terão maior influência, poder e orçamento ao garantirem acesso exclusivo a setores decisórios estratégicos. A competição entre inteligências é determinante para as dificuldades de relacionamento entre membros de sistemas nacionais, é provável corresponsável pela maioria dos principais erros de inteligência e representa obstáculo formidável para qualquer agência central de natureza integradora. Sobretudo se levarmos em conta que, para seu devido funcionamento, tais agências se esforçam para canalizar para o centro do sistema informações produzidas no âmbito de múltiplas instituições que, por natureza, seguem extremamente cautelosas quanto ao compartilhamento desse insumo.

Assim como apontado nas teorias interagências, nem sempre as agências envolvidas em determinadas tarefas estão realmente vinculadas a um objetivo comum, coletivo. Algumas delas, e naturalmente isso faz parte do processo público, demonstram a partir de suas culturas organizacionais suas prioridades ainda que num ambiente que deveria ser de cooperação. Nesse momento, as relações oscilam para um espaço competitivo. Tal como abordado acima quanto ao sistema de inteligência e o compartilhamento de informações, as disputas por recursos humanos, orçamentários, materiais e também pelo brilhanismo da reputação institucional, minam a natureza cooperativa pelas quais foram criadas.

O SISBIN se conformou como um sistema horizontalizado, cujo centro se pronuncia de maneira extremamente discreta. A Agência Brasileira de Inteligência coexiste com fortes instituições e, a depender do caso, suas agências de inteligência departamentais. Parte delas atua nos campos fundamentais da defesa, da segurança e das relações exteriores do Estado. Historicamente, o intercâmbio entre essas agências específicas e a ABIN no contexto do SISBIN representa o fluxo mais estável e significativo do sistema, mas sempre se manteve bastante aquém do ideal, mediante baixa coordenação ou supervisão.

Nesse contexto, sem contar com instrumentos cogentes e sem uma estratégia sofisticada para atrair a informação para o centro do SISBIN, sua coordenação se baseava no estabelecimento e manutenção das relações interinstitucionais e por meio de encontros entre corpos funcionais e entre chefias da ABIN e dos demais membros. O processo de construção de confiança entre dois organismos de inteligência no decorrer de suas relações de cooperação, conhecido na comunidade de inteligência como “olho no olho”, é imprescindível para que duas instituições possam analisar capacidades, práticas e intenções com o propósito de baixar ou erguer a guarda, viabilizando ou inviabilizando o intercâmbio de informações. Todavia, essa prática isolada tende à instabilidade, principalmente quando se baseia nas relações pessoais. Acaba sendo também insuficiente para satisfazer as necessidades de um sistema do porte do SISBIN, já que faltam estímulos institucionais para energizar, organizar e automatizar o intercâmbio quando os laços pessoais afrouxam.

Em sentido mais amplo, o arcabouço legal que fundamentava o SISBIN tendia a tratar todos os seus membros e pretendentes de maneira homogênea. Não existia segmentação ou qualquer limitação quanto ao escopo e as competências específicas das instituições que se candidatavam a uma vaga no sistema. A incorporação massiva de organizações que apresentam capacidades de inteligência muito variadas preocupava os membros mais tradicionais que já gozavam de forte cultura de proteção das informações ou que possuíam funções originais expressas de inteligência. Essa condição desestimulava o compartilhamento de insumos no âmbito do SISBIN e ia de encontro a seus pressupostos.

Além disso, a falta de referenciais objetivos gerou efeitos negativos também na composição do CONSISBIN, que se tornou incoerente. Ainda que os componentes do Conselho refletissem minimamente o escopo prioritário do SISBIN estabelecido por lei, a composição de seus representantes era absolutamente assimétrica. Nesse sentido,

por exemplo, na mesma mesa, gerentes intermediários possuíam o mesmo poder de decisão de ministros de Estado, o que desestimulava a participação e descredibilizava o arranjo.

Ainda no que diz respeito ao campo da governabilidade e composição do SISBIN, observava-se a falta de critério e procedimentos para a devida incorporação das Unidades da Federação no sistema. Na prática, o intercâmbio de informações entre o SISBIN e órgãos estaduais e municipais sempre ocorreu, mas é consenso que as lacunas produzidas pela falta de institucionalização adequada tornavam esse compartilhamento eventualmente sujeito a instabilidades e questionamentos, principalmente diante de contextos políticos heterogêneos. Instrumentos de governança, a partir da liderança, da lógica acerca do papel dos parceiros, das ações promovidas em benefício de uma entrega coletiva (Matias-Pereira, 2010) não se tornaram prática e elemento de legitimidade do sistema de inteligência.

Devido às necessidades relativas às questões internas do Brasil e de suas fronteiras, a rede de superintendências mantida pela ABIN é uma capacidade imprescindível, sobretudo no que diz respeito à antecipação e gestão de crises que interessam aos governos em todas as esferas federativas. Tal rede de superintendências depende das capacidades de inteligência das agências estaduais e municipais.

Mais do que isso, o exame do cotidiano do fluxo documental no âmbito das superintendências estaduais da ABIN mostrou que a dinâmica das interações entre o SISBIN e as agências de inteligência estaduais e municipais é, geralmente, mais fluida e intensa do que entre os membros do próprio sistema em seu extrato exclusivamente federal. Sendo assim, absorver os Estados e municípios de forma apropriada mostrava-se uma necessidade urgente para o SISBIN.

Outro problema no âmbito do sistema dizia respeito ao que estabeleceu a lei de criação da ABIN quanto à sua função de promotora e desen-

volvedora dos recursos humanos e da doutrina de inteligência. Para que haja fluxo adequado de informações e conhecimentos no interior do sistema, as doutrinas de inteligência e as metodologias de produção de conhecimento dos membros devem tender à homogeneidade e apresentar semelhanças em pontos fundamentais. Com o crescimento do número de membros no SISBIN e de escolas setoriais de inteligência, a Escola de Inteligência da ABIN passou a apresentar dificuldades para promover o diálogo que permitiria a acomodação entre as doutrinas que proliferaram.

A profissionalização da inteligência envolve a análise de diversos aspectos, incluindo conceituais, teóricos, conjunturais, históricos, legais, éticos, tecnológicos, metodológicos e humanos, que são fundamentais para fortalecer a Atividade de Inteligência. Ao aprofundar-se nesses temas, busca-se criar uma base sólida que não apenas otimize a coleta e a análise de informações, mas também garanta a integridade e a eficácia das operações de inteligência, assegurando que estas se alinhem às necessidades estratégicas do país e aos princípios éticos que devem orientar a atuação do Estado (Mendes; Mendes, 2024).

O ferramental e o modelo oferecido pela ABIN ao SISBIN para tramitação segura de documentos mostravam-se insuficientes. Tratava-se da combinação entre mensageria institucional e criptografia que conferiam boa segurança ao processo de tramitação ponto a ponto⁸ do conhecimento no interior do sistema, mas pecavam pela falta de transparência, agilidade e praticidade, elementos imprescindíveis diante do dinamismo das ameaças e das urgências do processo decisório.

Finalmente, “Planejar, executar, supervisionar e controlar as atividades de inteligência do País”, conforme a Lei 9.883/1999 atribui à ABIN,

8 Transmissão de dados ponto a ponto se refere a um método de comunicação em que a informação é transferida diretamente de um emissor para um receptor específico, sem a necessidade de intermediários.

torna-se difícil diante do recurso exclusivo ao modelo de compartilhamento ponto a ponto de documentos. O órgão central necessita de visualização do fluxo do intercâmbio de informações no interior do SISBIN para que possa estabelecer indicadores, parâmetros e estratégias, o que não era possível a partir do antigo modelo. Era urgente construir capacidade para que a atividade do SISBIN possa ser rastreável e auditável, o que conferiria maior confiabilidade e legitimidade à Atividade de Inteligência no País, bem como contribuiria para sua maior compatibilização com os princípios democráticos.

3. O Novo SISBIN: Perspectivas

Identificados os problemas mais imediatos que dificultavam o controle e a supervisão das atividades do SISBIN e impediam a otimização do fluxo de informações e conhecimentos no âmbito do sistema, fez-se necessário elaborar soluções com o intuito de superá-los. Essas medidas deveriam obedecer a uma estratégia que envolvesse as soluções encontradas e as organizasse em prol de propósitos bem definidos, bem como garantisse a continuidade do processo de aprimoramento do SISBIN, que fatalmente exigirá adaptações ao longo do tempo.

O objetivo maior estabelecido foi que o SISBIN desse um salto em eficiência e efetividade. Isso significava não somente cumprir com suas funções de inteligência, municiando o Presidente da República com os conhecimentos de inteligência necessários para seu nível de decisão e abastecendo complementarmente subsistemas e agências de inteligência de departamentos específicos e estratégicos para o Estado. Fazia-se de grande importância também a viabilização das capacidades de coordenação e supervisão a fim de garantir que as atividades desempenhadas no contexto do SISBIN estivessem sendo executadas em função de parâmetros objetivos que conferissem maior segurança e controle.

Tal objetivo exigiria o fortalecimento da ABIN em seu papel de agência central. Porém, esse movimento não poderia ser materializado em medidas que ressaltassem assimetrias de poder entre a agência central e os demais membros do sistema, pois a credibilidade e o equilíbrio do arranjo ainda dependem das considerações feitas pelo general Cardoso em 1996. A centralidade da ABIN deveria ser construída sobre sua capacidade de atrair insumos para o centro com base em ganhos marginais oferecidos aos membros pela estrutura do próprio SISBIN.

Por essa perspectiva, o sistema precisava acrescentar ao esforço contínuo de construção de confiança entre seus membros vantagens vinculadas sobretudo ao compartilhamento de informações e conhecimentos. A agência central passaria de uma postura passiva para outra ativa, comportando-se como um facilitador cujo papel é fortalecer todas as unidades do sistema e desbloquear fluxos de insumos essenciais para a integração da inteligência capaz de contribuir fundamentalmente para a segurança da sociedade e do Estado.

Todas as medidas expostas a seguir ainda se encontram em estágio de maturação e representam um ponto de partida para a reconstrução do SISBIN. O primeiro esforço nesse sentido foi a produção de um novo instrumento legal que substituísse o Decreto Nº 4.376 de 2002 e que, a partir de suas linhas, fosse capaz de iniciar o processo que suplantaria as dificuldades iniciais identificadas e acima descritas. Nesse sentido, em 06 de setembro de 2023, foi publicado o Decreto Nº 11.639, cujo propósito é dispor sobre o funcionamento do SISBIN.

Esse instrumento dinamizou as funções do Órgão Central do SISBIN, que puderam ser, grosso- modo, agrupadas em conjuntos relacionados 1) à reunião e integração das informações e conhecimentos do sistema, 2) à coordenação e à supervisão do sistema, 3) à disponibilização de infraestrutura própria do sistema, 4) ao planejamento da capacitação dos membros em articulação com os demais componentes do sistema, 5) ao processo de adequação e homogeneização da

doutrina de inteligência e 6) à representação do SISBIN. Pelo decreto, a ABIN também absorveu a competência de aprovar o ingresso de novos membros no SISBIN, anteriormente reservada ao CONSISBIN, e a de criar novos subsistemas em seu interior.

O novo decreto atribuiu à ABIN a responsabilidade pela construção conjunta de Planos de Trabalho com cada órgão e entidade integrante do sistema. Tais Planos deverão substituir o Plano de Inteligência, documento direcionado para a organização da coleta de dados e da produção de conhecimentos no âmbito do SISBIN. A diferença entre um Plano de Trabalho e o Plano de Inteligência é que o primeiro particulariza as necessidades informacionais de cada um dos membros do sistema e define com maior precisão o papel deles em sua relação com o Órgão Central em oposição ao caráter generalista e ao aspecto de “via de mão única” dada pelo segundo. Além disso, o compartilhamento de Planos de Trabalho permitirá que os membros do sistema tenham maior consciência das necessidades de seus pares e possam planejar melhor a cooperação e o compartilhamento de informações sem o intermédio do Órgão Central.

Outra contribuição fundamental trazida pela adoção dos Planos de Trabalho diz respeito à capacidade de supervisão do sistema por seu Órgão Central. Com planejamentos individualizados, a ABIN terá melhores referenciais para exercer suas atribuições estabelecidas por lei e produzir informações sistemáticas mais robustas para os órgãos responsáveis pelo controle externo da Atividade de Inteligência.

Para maximizar o potencial de intercâmbio seguro de informações e conhecimentos no contexto do SISBIN, o decreto estabeleceu que o Órgão Central disponibilizará ferramentas para comunicação segura e plataforma de compartilhamento. Espera-se que essas ferramentas, protegidas por criptografia de Estado, neutralizem a utilização de aplicativos de mensageria privados entre os membros do sistema e que as informações devidas ao SISBIN – principalmente no formato

de bancos de dados – sejam consensualmente disponibilizadas na plataforma em troca de acesso regulado.

A plataforma é um dos elementos centrais que conferirão motricidade ao SISBIN, pois somente por meio de uma estratégia digital é possível vencer as limitações e o descontrole impostos pela exclusividade da modalidade de tramitação ponto a ponto de documentos. Observando os princípios da Doutrina da Atividade de Inteligência e as legislações vigentes, é indispensável que informações e conhecimentos úteis ao atendimento das necessidades informacionais do Presidente da República e previstos nos Planos de Trabalho pactuados possam ser armazenados com extrema segurança, localizados mediante capacidade de realizar a busca e descoberta global⁹ das informações existentes¹⁰ e instantaneamente resgatados para utilização.

Atendendo à demanda por maior transparência e controle da inteligência, é intenção da ABIN que essa plataforma possibilite o rastreamento das atividades e dos acessos às informações sensíveis e sigilosas. Dessa forma, o Órgão Central eliminará os pontos-cegos e poderá visualizar o SISBIN em funcionamento, o que permitirá que exerça apropriadamente suas atribuições de “planejar, executar, supervisionar e controlar” o sistema, além de estar adequadamente preparado para o atendimento tempestivo das demandas dos órgãos externos de controle e absolutamente alinhado com os princípios democráticos.

Outrossim, a promoção da capacitação dos recursos humanos do SISBIN ficou sob a responsabilidade do Órgão Central. Na medida em que o sistema se consolida, está prevista volumosa demanda por capacitação que só poderá ser atendida por meio da utilização integrada

9 É a procura ativa e sistemática de informações específicas em bancos de dados integrados que contenham dados e informações de diferentes naturezas provenientes de diferentes fontes.

10 Respeitando a compartimentação e a garantindo apresentação de motivação e interesse público.

dos centros de ensino de inteligência existentes no SISBIN. Complementarmente, a circulação de profissionais de inteligência pelos múltiplos centros de ensino concorrerá para o processo de aproximação das doutrinas de inteligência dos membros do sistema.

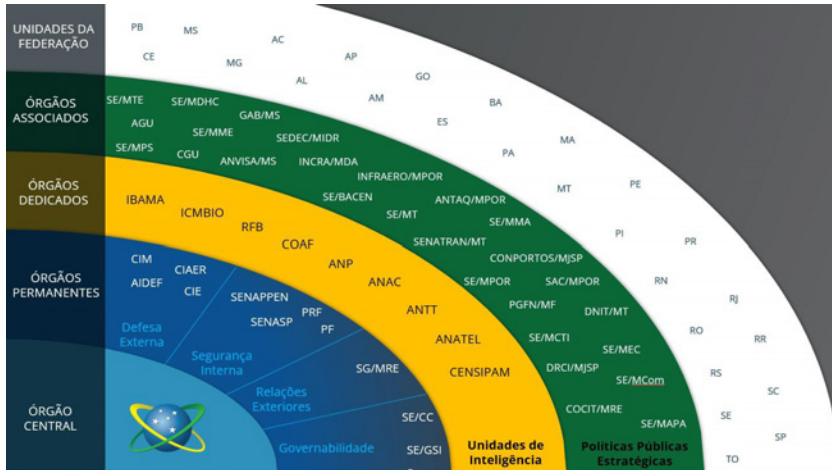
Como parte de uma tendência crescente, muitos países têm investido na profissionalização dos analistas de inteligência, enfatizando a especialização e a formação de profissionais capacitados para lidar com as complexidades desse setor. É fundamental reconhecer que as tecnologias atuais, como inteligência artificial e automação, estão se tornando indispensáveis para melhorar a coleta e a análise de dados. Além disso, a consideração de aspectos éticos e legais, como a proteção dos direitos individuais e a conformidade com a Constituição, é essencial na formação desses profissionais, garantindo que suas atividades respeitem a privacidade e os direitos fundamentais. Nesse aspecto, o processo de desenvolvimento dos estudos de inteligência e capacitação do profissional são elementos essenciais de modernização e aprimoramento da rede.

Além da reorganização das competências do Órgão Central com o propósito de fortalecê-lo, a modificação mais notória do novo decreto foi a segmentação do SISBIN. Como já mencionado, os 25 anos de coordenação do SISBIN encontraram na falta de regulação, na proliferação de membros e na assimetria entre eles um limite para os fluxos do compartilhamento de insumos e para os assessoramentos horizontais e verticais. Para solucionar esse problema, adotou-se a lógica de círculos concêntricos, com a ABIN como a esfera central e quatro camadas circulares de organizações-membros (Figura 1) que se diferenciam umas das outras em aspectos essenciais ao assessoramento e ao compartilhamento de inteligência:

- 1 - Órgão Central
- 2 - Órgãos Permanentes;
- 3 - Órgãos Dedicados;

- 4 - Órgãos Associados;
- 5 - Órgãos Federados.

Figura 1
Representação da estratificação do Sistema Brasileiro de Inteligência



Fonte: ABIN.

Órgãos Permanentes são aqueles que, de acordo com a lei de criação do SISBIN, espelham seu campo de atuação prioritário, pois se encontram nas principais dimensões de Estado: defesa externa (Assessoria de Inteligência de Defesa do Ministério da Defesa, Centro de Inteligência do Exército, Centro de Inteligência da Aeronáutica e Centro de Inteligência da Marinha), relações exteriores (Secretaria Geral do Ministério das Relações Exteriores) e segurança interna (Secretaria Nacional de Segurança Pública, Polícia Federal, Polícia Rodoviária Federal e Secretaria Nacional de Políticas Penais), acrescidas de uma dimensão denominada “governabilidade” (Casa Civil da Presidência da República e Gabinete de Segurança Institucional). São instituições que, adjacentes às suas atribuições principais, também possuem a função de informar e assessorar o processo decisório das autoridades de suas respectivas pastas e que, integradas, atendem ao propósito

maior do SISBIN. Pretende-se que esse estrato seja permanente e não esteja aberto para adesões.

Órgãos Dedicados são aqueles que não se encontram nas dimensões do Estado citadas na lei de criação do SISBIN, mas que sobretudo contam com unidades especializadas de inteligência e desempenham papel estratégico na execução das atividades de Estado, das Políticas Públicas ou dos assuntos vinculados à Política Nacional de Inteligência. Suas atribuições variam dentro de um espectro que abrange desde o monitoramento e proteção da região amazônica até a fiscalização ambiental. Além dos Órgãos Permanentes e do Órgão Central, os Órgãos Dedicados representam o que existe de mais avançado no que diz respeito à segurança da informação e cultura de inteligência no Brasil.

Órgãos Associados são aqueles de reconhecida importância para a inteligência, mas que ainda não possuem setores dedicados à atividade. Por não produzirem conhecimentos de inteligência, esses órgãos também não são capazes de realizar assessoramento através do SISBIN, contudo estão livres para receber assessoramento e compartilhar informações. Qualquer um deles está em condições de pleitear ascensão ao nível de Órgãos Dedicados, contanto que, com o auxílio das estruturas do sistema, se disponibilizem a realizar melhorias e adaptações para atenderem a critérios estabelecidos pela ABIN relativos à proteção da informação e produção de insumos de inteligência.

Órgãos Federados inserem-se em uma categoria específica e dizem respeito às unidades estaduais e municipais incorporadas ao SISBIN. Apesar de serem representados como a 4ª camada, essa posição não significa perda na qualidade do acesso a informações ou no recebimento de assessoramento eventual do sistema. As várias instituições estaduais e municipais estarão distribuídas de forma a terem inserções análogas ao segundo ou terceiro círculos, a depender das suas capacidades de inteligência e necessidade de conhecer. O esforço

pela formalização da entrada dos Estados e municípios pretende resolver definitivamente a situação anteriormente identificada de informalidade no intercâmbio entre o SISBIN e os entes federativos.

No caso do Conselho Consultivo do SISBIN, passou a apresentar funções essencialmente consultivas, além da competência de propor atualizações da Política Nacional de Inteligência e da responsabilidade de analisar os relatórios de gestão anual do sistema. A assimetria na representatividade do CONSISBIN existente no modelo anterior foi sanada ao estabelecer que o Conselho é composto pelos titulares da Casa Civil (CC), do Gabinete de Segurança Institucional (GSI), do Ministério da Justiça e Segurança Pública (MJSP), do Ministério das Relações Exteriores (MRE), do Ministério da Defesa (MD) e da ABIN. No impedimento dessas autoridades, serão representados pelos Secretários-Executivos de ministérios (CC, GSI e MJSP), pelo Secretário-Geral do MRE, pelo Chefe do Estado-Maior Conjunto das Forças Armadas (MD) e pelo Diretor-Adjunto da ABIN.

Esse modelo apresentado como um novo formato de correlação entre o órgão não diminui a capacidade de integração existente entre eles, mas aperfeiçoa os níveis de relações interagências fomentando cooperação no nível, medida e necessidade que os órgãos puderem realizar. Assim, a função desse novo sistema possa estar vinculada ao processo de dinamismo e intensidade dos fluxos informacionais, garantindo que as demandas e prioridades estejam estabelecidas sem que haja sobreposição de tarefa e com otimização de recurso e tempo.

Conclusão

O atual processo de reformulação do SISBIN teve recentemente seu primeiro impulso para mitigar os problemas crônicos identificados. É um esforço inicial que cria espaço para novas adequações e multiplica os conectores potenciais com o dinâmico desenvolvimento tecnológico nos campos da coleta e gestão da informação. Desafios modernos

e tendências nesse campo, inclusive, deverão demandar adaptações cada vez mais urgentes.

O modelo atualmente aplicado ao SISBIN deverá seguir em constante reavaliação em função dos resultados que as novas alterações forem capazes de produzir. Mesmo os EUA precisaram operar modificações significativas em seu sistema de inteligência nacional após constatação de debilidades ou falhas recentes (Best, 2014).

O atentado do 11/9 contra o *World Trade Center* e o Pentágono, por exemplo, foi considerada a maior falha de inteligência norte-americana desde Pearl Harbor. Investigações oficiais acusaram novamente problemas de compartilhamento de informações no interior da comunidade de inteligência. As soluções implementadas, contudo, transcenderam o desenho da estrutura institucional dos sistemas de segurança nacional daquele país e promoveram também a incorporação de tecnologia de ponta na gestão da informação e nos processos de compartilhamento da inteligência.

O processamento de material em quantidades avassaladoras é um desafio presente enfrentado também pelo SISBIN. A chamada infobesidade¹¹ vem requerendo capacidades de processamento somente possíveis mediante a incorporação de tecnologia de ponta aos processos de produção do conhecimento e de intercâmbio de insumos de inteligência. Estratégias anacrônicas de coordenação do sistema e métodos antigos e vagarosos de compartilhamento de informações se tornaram perigosos porque não acompanharam a sofisticação das ameaças, criando oportunidade para a ocorrência de crises e falhas de inteligência.

O desenvolvimento e disponibilização para todos os membros do SISBIN de uma plataforma de compartilhamento seguro de dados – mu-

11 O termo se refere ao excesso de informação a que estamos expostos na era digital.

nida de criptografia de Estado desenvolvida na própria ABIN – deverá possibilitar a incorporação futura de tecnologias avançadas. Não se trata apenas da utilização de inteligência artificial e de outros recursos capazes de substituir boa parte da intervenção humana de caráter mais mecânico no processo de produção de conhecimento, mas também da capacidade de permitir que as instituições brasileiras produzam inteligência em um mesmo ambiente e conjuntamente quando o contexto assim impuser.

A atual reforma do SISBIN cria expectativas positivas por lidar pragmaticamente com seus principais desafios e utilizar tecnologia para romper com antigos costumes nas relações entre as agências de inteligência brasileiras sem impor quaisquer desvantagens aos seus membros. Pelo contrário, como demonstrado, a estratégia do novo SISBIN é mitigar as resistências por meio da atuação de um Órgão Central capaz de promover o fortalecimento de todos os quadrantes do sistema de inteligência sem os submeter.

Essa reestruturação busca não apenas otimizar a troca de informações, mas também harmonizar os esforços de análise e resposta a ameaças complexas. A cooperação da inteligência em âmbito interagências torna-se fundamental para garantir que cada entidade contribua com sua expertise, criando uma abordagem mais abrangente e eficiente frente a desafios contemporâneos. Além disso, a reformulação do SISBIN reflete a necessidade de adaptação a um ambiente em constante mudança, onde a sinergia entre as agências é essencial para uma atuação coordenada e proativa na defesa dos interesses do país. Trata-se de mais uma oportunidade para dotar o País de uma inteligência mais adequada aos princípios democráticos e à altura de seu peso e de seus desafios.

Frente ao incremento na complexidade de antigas ameaças e ao aparecimento de novos desafios para um país da estatura do Brasil, os problemas de efetividade apresentados pelo SISBIN impuseram a ne-

cessidade urgente de repensá-lo. Um sistema de inteligência nacional débil incide negativamente sobre a segurança e o desenvolvimento do País, já que privaria suas instâncias mais elevadas desse insumo que constitui um poderoso referencial para a condução dos processos decisórios de alto nível.

Mais do que crises e falhas de inteligência, a perda de variadas oportunidades devido à insuficiência da integração no âmbito do SISBIN ao longo de décadas certamente limitou as capacidades brasileiras, pondo em risco resultados nos campos das principais políticas de Estado. O Brasil, com seus graves problemas internos irresolutos, seu crescente peso internacional e suas altivas aspirações como nação, necessita cada vez mais de capacidade decisória lastreada em conhecimentos confiáveis e sobretudo soberanos. No atual contexto, é praticamente impossível se alcançar o status desejado sem a contribuição de um sistema de inteligência nacional funcional e uma agência central de inteligência de Estado forte, comprometida com os princípios constitucionais que regem o Estado e orientada pelos principais decisores da nação.

A discussão acerca da atividade e do que se espera do Sistema Brasileiro de Inteligência não pode continuar restrito à comunidade de inteligência brasileira e à academia. Nesse sentido, urge-se multiplicar o debate aprofundado e intenso sobre o SISBIN na sociedade brasileira e no âmbito do Executivo, do Legislativo e do Judiciário.

Referências

BARDACH, E. Developmental dynamics: interagency collaboration as an emergent phenomenon. **Journal of Public Administration Research and Theory**, [s. l.], v. 11, n. 2, p. 149-164, abr. 2001. DOI: <https://doi.org/10.1093/oxfordjournals.jpart.a003497>. Disponível em: <https://academic.oup.com/jpart/article-abstract/11/2/149/937046>. Acesso em: 22 out. 2024.

BEST, R. A. Leadership of the U.S. Intelligence community: from DCI to DNI. **International Journal of Intelligence and Counterintelligence**, [s. l.], v. 27, n. 2, p. 253-333, 7 mar. 2014. DOI: <http://dx.doi.org/10.1080/08850607.2014.872533>. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/08850607.2014.872533>. Acesso em: 22 out. 2024.

BRANDÃO, P. C. **SNI e ABIN: uma leitura dos serviços secretos brasileiros ao longo do século XX**. Rio de Janeiro: FGV Editora, 2002.

BRASIL. **Lei nº 9.883, de 7 de dezembro de 1999**. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências. Brasília, DF: Presidência da República, [1999]. Disponível em: http://planalto.gov.br/CCIVIL_03/LEIS/L9883.htm. Acesso em: 22 out. 2024.

_____. **Decreto nº 4.376, de 13 setembro de 2002**. Dispõe sobre a organização e funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei nº 9.883, de 7 de setembro de 1999, e dá outras providências. Brasília, DF: Presidência da República, [2002]. Disponível em: http://planalto.gov.br/CCIVIL_03/decreto/D4376.htm. Acesso em: 22 out. 2024.

_____. **Decreto nº 11.693, de 6 setembro de 2023**. Dispõe sobre a organização e funcionamento do Sistema Brasileiro de Inteligência. Brasília, DF: Presidência da República, [2023]. Disponível em: http://planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11693.htm#art21. Acesso em: 22 out. 2024.

CEPIK, M. **Espionagem e democracia**. Rio de Janeiro: FGV Editora, 2003.

_____. Intelligence and security services in Brazil reappraising institutional flaws and political dynamics. **The International Journal of Intelligence, Security and Public Affairs**, [s. l.], v. 23, n. 1, p. 81-102, 2 jan. 2021. DOI: <http://dx.doi.org/10.1080/23800992.2020.1868784>. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/23800992.2020.1868784>. Acesso em: 22 out. 2024.

HANDEL, M. L. Intelligence and the Problem of Strategic Surprise. **Journal of Strategic Studies**, [s. l.], v. 7, n.3, p. 229-281, 1984. DOI: <http://dx.doi>.

[org/10.1080/01402398408437190](https://doi.org/10.1080/01402398408437190). Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/01402398408437190>. Acesso em: 22 out. 2024.

HERMAN, M. **Intelligence power in peace and war**. Cambridge: Cambridge University Press, 1996.

HUGHES-WILSON, J. **On Intelligence: the history of espionage and the secret world**. Londres: Constable & Robinson, 2016.

KAPUCU, N. Interagency communication networks during emergencies: boundary spanners in multiagency coordination. **The American Review of Public Administration**, [s. l.], v. 36, n. 2, p. 207-225, jun. 2006. DOI: <http://dx.doi.org/10.1177/0275074005280605>. Disponível em: <https://journals.sagepub.com/doi/abs/10.1177/0275074005280605?journalCode=arpb>. Acesso em: 22 out. 2024.

MATIAS-PEREIRA, J. A governança corporativa aplicada no setor público brasileiro. **Administração Pública e Gestão Social**, [s. l.], v. 2, n. 1, p. 109–134, 2010. DOI: [10.21118/apgs.v2i1.4015](https://doi.org/10.21118/apgs.v2i1.4015). Disponível em: <https://periodicos.ufv.br/apgs/article/view/4015>. Acesso em: 22 out. 2024.

MENDES, C. S. M.; MENDES, R. L da C.. A Profissionalização da Inteligência e os desafios à modernização do conhecimento. **Zenodo**, [s. l.], v. 2, n. 1, p. 1–11, 5 fev. 2024. DOI: <https://doi.org/10.5281/zenodo.10616692>. Disponível em: <https://zenodo.org/records/10616692>. Acesso em: 22 out. 2024.

WOHLSTETTER, R. **Pearl Harbor: warning and decision**. Stanford: Stanford University Press, 1962.

ZEGART, A. B. **Flawed by design: the evolution of the CIA, JCS, and NSC**. Stanford: Stanford University Press, 1999.



A Inteligência como política pública: desafios para a ABIN

Rodrigo de Aquino

Oficial de Inteligência
Secretário da Secretaria de Planejamento e Gestão (SPG)

Ao atingir o marco de 25 anos de criação da Agência Brasileira de Inteligência (ABIN), parece razoável avaliar a Atividade de Inteligência enquanto política pública, visando ampliar o debate sobre a revisão dos seus instrumentos orientadores e da sua arquitetura de implementação e governança em busca de maior eficiência, efetividade e legitimidade, pressupostos mínimos para o seu desenvolvimento em contexto democrático. Mais ainda, trata-se de discutir alternativas para ajustar meios e fins da Atividade de Inteligência desenvolvida pela ABIN, considerando a evolução social e política da sociedade, que enseja maior transparência e aprimoramento de controles, bem como a necessidade de adaptação ao ambiente estratégico no qual a atividade se insere.

O estudo de políticas públicas promove abordagem analítica, sob uma ótica racional e normativa, do processo decisório para a solução de problemas sociais. Para essa finalidade, desenvolveu-se, inicialmente, o conceito de ciclo de políticas públicas que desdobrou esse processo em fases (Laswell, 2003). Esse modelo, embora reconhecidamente limitado por seu enfoque fragmentário e simplificado, costuma ser utilizado como referência analítica. A partir desse conceito, novas propostas e elementos foram agregados (Boullosa, 2024). De todo modo, o modelo mais conhecido e utilizado por cientistas políticos considera

as fases de construção de agenda, formulação e implementação da política e avaliação (Howlett; Ramesh, 2003).

A proposta deste capítulo é destacar alguns elementos para debate relacionando-os ao ciclo de políticas públicas, sobretudo aos “momentos” de formulação, implementação e avaliação, entendido como processo complexo, interativo e contínuo (Lotta, 2019). Desse modo, busca-se demonstrar a relação da formulação da política de Inteligência com a agenda política nacional, descrever as características de sua implementação, comentar desafios para a avaliação da política e apontar possibilidades para maior controle em sua execução. A partir dessa discussão pretende-se contribuir para a necessária revisão dos referenciais da política pública e de forma de implementação visando a qualificar assessoramento prestado pela Atividade de Inteligência ao processo decisório nacional.

Reconhecendo o desafio de demonstrar o impacto do assessoramento prestado pela Atividade de Inteligência, devido à complexidade do processo decisório, pretende-se listar algumas contribuições em áreas estratégicas, em contraponto a críticas e questionamentos quanto às falhas e aos desvios, sobretudo da ABIN e de seus profissionais. Analisar falhas e desvios, como efeitos indesejados da política pública, é essencial para vislumbrar oportunidades de melhoria no funcionamento do arranjo institucional de implementação e governança visando a garantir maior eficiência, efetividade e legitimidade no desenvolvimento da atividade.

1. Ciclo de políticas públicas e a Atividade de Inteligência

As políticas públicas são o resultado de um processo complexo, interativo e contínuo, sujeito à interferência de fatores variados, voltado para solucionar problemas sociais (Lotta, 2019). Nesse sentido, a Atividade de Inteligência pode ser entendida como uma política pública executada pelo governo. Ela se caracteriza pelo exercício permanente

de ações especializadas destinadas à produção de conhecimentos e à proteção da sociedade e do Estado, com vistas ao assessoramento de autoridades de sucessivos governos, nos respectivos níveis e áreas de atribuição. Tal assessoramento abrange, dentre outros pontos, a identificação de oportunidades e ameaças à consecução das políticas de governo. Por esse motivo, não se caracteriza pela oferta de serviços e produtos diretamente à população.

Baseando-se em um enfoque racional e normativo do processo decisório, desenvolveu-se, inicialmente, o conceito de ciclo de políticas públicas que desdobrou esse processo em fases (Laswell, 2003). Esse modelo, embora reconhecidamente limitado por seu enfoque fragmentário e simplificado, costuma ser utilizado como referência analítica. O modelo mais conhecido e utilizado por cientistas políticos considera as fases de construção de agenda, formulação e implementação da política e avaliação (Howlett; Ramesh, 2003).

As políticas públicas podem ser entendidas como o resultado da convergência de fluxos de soluções, problemas e ambiente político favorável constituindo uma janela de oportunidade a ser aproveitada por empreendedores políticos (Kingdon, 1995 *apud* Barcelos; Calmon, 2010; Secchi, 2010). Por esse motivo, a formação de agenda e alternativas disponíveis para a solução dos problemas sociais influem sobremaneira no processo decisório e na forma de implementação das políticas públicas. Uma série de temas compõe a agenda governamental, por despertar o interesse dos tomadores de decisão, mas somente parte deles será efetivamente tratada para fins decisórios. A forma como os problemas são construídos social e politicamente determina como esses temas serão posicionados na agenda decisória.

A inclusão da Atividade de Inteligência na agenda decisória para fins de formulação de uma política pública decorre do grau de percepção de ameaça à segurança da população e das instituições na dinâmica

histórica da sociedade e o grau de prioridade atribuído pelos atores políticos a esse tema diante dos demais problemas sociais que demandam algum tipo de solução. Além disso, eventos críticos associados à questão da segurança da sociedade e das instituições governamentais podem motivar a discussão de propostas que não encontravam espaço político favorável e, dessa forma, promover a política de Inteligência com a finalidade de melhor preparar o Estado para detectar, prevenir e monitorar ameaças.

A importância da implementação como objeto de análise no campo de estudo das políticas públicas decorre justamente da constatação de que há riscos elevados, empiricamente comprovados, de que os objetivos colimados no processo de formulação da política pública não sejam atingidos ou surjam efeitos não previstos (Cardim, 2009).

Existem, no entanto, várias formas de compreender e abordar analiticamente a implementação de políticas públicas. Alguns autores privilegiam a visão *top down*, a qual considera que políticas públicas são decisões tomadas pelas autoridades formais para enfrentar um problema social. Esses estudos focam, portanto, em avaliar se a implementação pela estrutura burocrática está adequada aos objetivos decididos legitimamente pelos atores políticos. Outros adotam uma visão *bottom up*, na qual políticas públicas são o resultado de múltiplas decisões dos atores encarregados da implementação, sobretudo a burocracia estatal, mas também outros que se envolvem no processo, como empresas e organizações não-governamentais.

Atualmente, os estudos sobre implementação de políticas públicas incorporaram variadas abordagens e modelos de análise que buscam compreender novas formas de ação do Estado. Nesse contexto, destacam-se análises sobre processo decisório em várias esferas e múltiplos níveis e novos arranjos institucionais e de governança (Lotta, 2019). Parte-se do pressuposto de que há uma simbiose entre os processos de formulação e implementação. Mais que execução, a imple-

mentação é um momento de coordenação, integração e socialização (Cardim, 2009).

Desse modo, os estudos sobre implementação não se limitam a compreender os fatores que influenciam a eficiência e a efetividade das políticas públicas. Também englobam novas formas de atuação dos agentes públicos, destacando o papel de articulação interorganizacional e de indução de atores e recursos da sociedade e sua influência na formulação da política. Traz para o centro das discussões o dilema da discricionariedade, ou seja, aceitar a função dos agentes públicos na tradução das decisões políticas para sua aplicação nos casos reais e não previstos como forma de garantir maior efetividade da ação governamental ou aumentar regulações e controles para limitá-la e, dessa forma, privilegiar o alinhamento com os objetivos definidos pelos tomadores de decisão para garantir a legitimidade política da ação governamental (Lotta, 2019).

A análise sobre a implementação da política de Inteligência permite contemplar essas várias formas de abordagem. Cada qual traz pontos importantes a serem considerados. Além de avaliar se as ações realizadas pelos órgãos de Inteligência estão alinhadas às diretrizes estabelecidas na política, também busca compreender se os arranjos institucionais, os recursos disponíveis e as estruturas de governança e controle são suficientes para atingir os objetivos previstos.

Na sequência desse modelo sistêmico de abordagem das políticas públicas, a avaliação cinge-se de fundamental importância com um olhar retrospectivo, visando aferir se as metas foram atingidas, como os serviços e produtos foram entregues e que efeito tiveram na solução dos problemas para os quais foram desenhados ou mesmo na satisfação do público-alvo para o qual fora destinada. Também se refere a um processo prospectivo, pois, a partir da análise dos resultados e seus efeitos – sejam eles esperados, não projetados ou indesejados –, pode-se estimar impactos e promover adaptações que deter-

minem seu alinhamento com a evolução do cenário político decisório. Não se limita a mera constatação sobre o atingimento das metas, pois permite identificar oportunidades para a inovação na ação governamental (Vedung; Pedone, 2021).

A principal função da avaliação seria produzir informações sobre os resultados atingidos. Posteriormente, foi agregado a essa função a necessidade de permitir melhor alocação de recursos, sobretudo em relação a limitações orçamentárias. Mais recentemente predominam também preocupações sobre legitimidade, eficiência e efetividade das políticas públicas (Trevisan; Van Bellen, 2008).

No caso da Atividade de Inteligência, o estágio de avaliação da efetividade da política pública também precisa ser seguido de uma fase de controle onde a legitimidade dela também é avaliada. Isso se dá pelos dilemas enfrentados na dinâmica de convivência entre democracias e serviços de inteligência, tais como aquele entre segredo governamental/direito ao acesso à informação e segurança estatal/segurança individual, que exigem a criação de mecanismos eficientes de controle e de avaliação das atividades das agências de inteligência (Cepik, 2003).

A concepção do planejamento da implementação de políticas públicas utilizando a metodologia do marco lógico, no qual se busca caracterizar o problema social e a racionalidade de intervenção, favorece a compreensão do que se espera em termos de resultados a serem alcançados. Por esse motivo, políticas estruturadas dessa maneira normalmente apresentam indicadores e metas que permitem melhor avaliar a eficiência e a efetividade da ação governamental. Além disso, também permitem melhor identificar os recursos necessários para produzir os resultados e impactos esperados.

A utilidade do processo de avaliação, ainda que oneroso para o Estado, justifica-se não somente por indicar qual foi o impacto da ação gover-

namental na situação problema, mas também por permitir compreender a relação entre investimento de recursos e efeitos. Desse modo, a avaliação possibilita aos cidadãos e órgãos de controle maior transparência sobre a eficiência e efetividade na gestão dos recursos destinados à política pública (Trevisan; Van Bellen, 2008).

Além dos desafios comuns ao processo de avaliação de políticas públicas, a análise referente à Atividade de Inteligência se mostra ainda mais complexa devido à questão do sigilo e à dificuldade de identificar o impacto do assessoramento prestado, uma vez que não se caracteriza pela oferta de serviços e produtos diretamente à população, com já foi observado. Por esse motivo, é particularmente importante no caso da Atividade de Inteligência não restringir a avaliação a indicadores de eficiência e efetividade, ainda que relevantes para a prestação de contas, e considerar o aspecto da legitimidade das ações.

Embora apresentada em recortes limitados às fases de formulação, implementação e avaliação, a política pública de Inteligência deve ser compreendida como processo iterativo e contínuo. Tampouco se pretende estabelecer o insulamento entre atores políticos e a burocracia, uma vez que o funcionamento do Estado se estabelece pela negociação entre os diversos atores, mediada institucionalmente. Por esse motivo, ao apresentar as características da formulação e implementação da política de Inteligência, o engajamento dos atores nesse processo, e comentar aspectos sobre a avaliação de seus resultados e efeitos indesejados, pretende-se contribuir para os ajustes necessários no desenvolvimento da Atividade de Inteligência.

2. Formulação e Planejamento

A etapa de formulação das políticas públicas da Atividade de Inteligência, especialmente em regimes democráticos em que o Poder Executivo depende do Congresso para aprovar leis, é caracterizada pelo relativo baixo engajamento e protagonismo da comunidade polí-

tica. Em geral, os atores políticos enfrentam dificuldade em obterem informações e assessoramento técnico qualificado sobre a Atividade de Inteligência, por sua associação à questão da segurança nacional e pela confidencialidade de seus métodos e processos. Mais ainda, o distanciamento também se explica pelo baixo interesse de grupos de pressão, do baixo retorno esperado em termos de ganhos políticos e dos riscos associados a futuras acusações de interferência em uma área dominada pelo Poder Executivo e pelas forças militares e de segurança (Cepik, 2003).

No Brasil, a resistência dos atores políticos para abordar o tema é ainda maior, dado o estigma de serviços de informação por seu papel no apoio à ditadura militar. A função de polícia política, como instrumento de repressão à subversão, associada ao Serviço Nacional de Informações (SNI) e ao Sistema Nacional de Informações (SISNI) associou a Atividade de Inteligência, sobretudo entre formadores de opinião na comunidade política e acadêmica, a uma percepção de ameaça aos direitos civis e humanos e, por seu turno, incompatível com a democracia (Ambros, 2017).

Dessa forma, mesmo após o fim do regime militar, o processo de democratização não ensejou de imediato a formulação de uma nova política para a Atividade de Inteligência. Embora a necessidade de reforma estivesse presente nas discussões da Assembleia Nacional Constituinte, o SNI não foi extinto logo ao fim do regime militar em 1985, sob o argumento de que a nova Constituição bastaria para atingir essa finalidade. A extinção formal do órgão ocorreu somente em 1990, durante a presidência de Fernando Collor de Mello. Todavia, na prática, o que ocorreu foi a transferência da estrutura do antigo SNI para a Secretaria de Assuntos Estratégicos (SAE). Mesmo que, inicialmente, a medida tenha representando perda simbólica de espaço político, o segmento militar manteve sua influência sobre a atividade, sobretudo a partir de 1996, quando a atividade passa à subordinação da Casa Militar (Zaverucha, 2008).

Ainda que a democratização tenha propiciado o ambiente para a mudança na formulação da política de Inteligência e das estruturas para a sua implementação, foram crises associadas a desvios de conduta de agentes e falhas das agências que trouxeram a Atividade de Inteligência para o centro da agenda política no Brasil (Gill, 2002). O PL nº 3.651/1997 (Brasil, 1997a), que tramitava por cerca de dois anos, foi finalmente aprovado em dezembro de 1999. Recordar-se que, ao longo de 1999, ganharam repercussão nos meios de comunicação as investigações sobre o envolvimento de agentes vinculados à estrutura de Inteligência no monitoramento ilegal de telefones do BNDES em julho de 1998, por ocasião da privatização da Telebrás (Fagundes, 1999; Gondim, 1999; Temor, 1999). A preocupação com limites ao emprego de ações sigilosas estavam já, de todo modo, presentes na exposição de motivos e projeto de lei encaminhados em 1997, que as condicionava “à irrestrita observância dos direitos e garantias individuais, à fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado” (Brasil, 1997b).

A Lei nº 9.883 foi aprovada em 7 de dezembro de 1999, por meio da qual foi instituído o Sistema Brasileiro de Inteligência (SISBIN) e criada a Agência Brasileira de Inteligência (ABIN) como seu órgão central (Brasil, 1999). A mesma lei previa uma Política Nacional de Inteligência (PNI), a ser implementada pela ABIN e, por extensão, pelos órgãos componentes do SISBIN, sob supervisão da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), do Conselho de Governo. Mais ainda, estabelecia o controle externo da Atividade de Inteligência a ser exercido pelo Poder Legislativo. Interessante também observar que, após sua criação, a agência foi vinculada ao Gabinete de Segurança Institucional (GSI) (Brasil, 2000).

A referida lei trouxe definições genéricas sobre o mandato legal da agência, sobretudo no que se refere ao uso de técnicas e meios sigilosos para a obtenção e a análise de dados para a produção de conhecimentos necessários ao processo decisório do Poder Executivo. Foi

o resultado possível das propostas que tramitaram no Legislativo e as pressões sociais, no contexto das relações cívico-militares da época (Cepik, 2003).

Essa dinâmica se reproduziria nos anos subsequentes influenciando o processo de formulação dos normativos referenciais da política de Inteligência. O GSI passou a “coordenar as atividades de Inteligência Federal”, com base nas disposições sobre a organização da Presidência da República. Por esse motivo, em conformidade com suas competências legais, o GSI exerceu influência na elaboração das propostas dos normativos relativos à Atividade de Inteligência por parte do Poder Executivo.

Apesar do relativo desinteresse da comunidade política sobre a Atividade de Inteligência, denúncias e investigações sobre desvios na ação da agência ou de seus servidores serviriam de motivadores para a formulação de propostas legislativas, porém com baixo destaque do tema na agenda do Congresso Nacional (Salles; Valle, 2018). Apesar dos avanços obtidos na organização da estrutura para a implementação e a governança da política – sobretudo a criação da Comissão Mista de Controle da Atividade de Inteligência no Poder Legislativo (CCAI) e a aprovação de seu regimento (Brasil, 2013) – e a criação de uma carreira dedicada à Atividade de Inteligência (Brasil, 2004; Brasil, 2008), não houve aprimoramento dos mandatos e limites legais para o exercício do papel previsto na legislação.

Enquanto não editada a PNI, conforme estava previsto na Lei nº 9.883/1999, diretrizes para o desenvolvimento da Atividade de Inteligência seriam aprovadas mediante resoluções da Câmara de Relações Exteriores e Defesa Nacional (CREDEN). Conforme o Decreto nº 4.801, de 6 de agosto de 2003, caberia à CREDEN, sob a presidência do GSI, formular políticas públicas e diretrizes relacionadas, entre outras matérias, à Atividade de Inteligência (Brasil, 2003). Desse modo, sob a supervisão do GSI, o corpo técnico da ABIN participaria

da elaboração das proposições relativas à Atividade de Inteligência que seriam submetidas para a aprovação da CREDEN.

A elaboração da PNI inicia-se, formalmente, em 2009, quase dez anos após a edição da Lei nº 9.883/1999, mediante a criação de comitê ministerial para esta finalidade (Brasil, 2009). Sob coordenação do GSI, a ABIN conduziu reuniões de trabalho com participação de representantes da Casa Civil, Secretaria de Assuntos Estratégicos e ministérios da Justiça, Defesa, Relações Exteriores e Planejamento, Orçamento e Gestão. A proposta foi apreciada pelo Conselho de Defesa Nacional e, posteriormente, enviada, em 9 de dezembro de 2009, para a apreciação do Congresso Nacional (Brasil, 2009) e retornaria, cerca de um ano depois, com sugestões que foram incorporadas ao texto. Apesar da importância da política para estabelecer valores, escopo e prioridades no desenvolvimento da Atividade de Inteligência para todos os órgãos do SISBIN, a proposta só seria aprovada em 2016, confirmando a baixa prioridade da questão na agenda política.

A Política Nacional de Inteligência, fixada pelo Decreto nº 8.793, de 29 de junho de 2016, conforme seu próprio texto, representa o normativo de mais alto nível para orientar o desenvolvimento da Atividade de Inteligência no Brasil. Nela são expressos os principais conceitos, pressupostos, valores e instrumentos da política pública de Inteligência. Destaca a função do SISBIN como arranjo institucional para a implementação da política, marcando a importância do planejamento integrado e do compartilhamento de dados. Os controles interno e externo da atividade foram também mencionados como importante elemento da política (Brasil, 2016).

A orientação para a obtenção de dados e a produção de conhecimentos dos órgãos do SISBIN fundamentou-se em rol de ameaças, entendidas como "aquelas que apresentam potencial capacidade de pôr em perigo a integridade da sociedade e do Estado e a segurança nacional do Brasil" (Brasil, 2016). A PNI prioriza as seguintes amea-

ças: espionagem; sabotagem; interferência externa; ações contrárias à Soberania Nacional; ataques cibernéticos; terrorismo; atividades ilegais envolvendo bens de uso dual e tecnologias sensíveis; armas de destruição em massa; criminalidade organizada; corrupção; e ações contrárias ao Estado Democrático de Direito.

Para além da PNI, outros documentos de referência da política pública de Inteligência no Brasil, como a Estratégia Nacional de Inteligência (ENINT) e seus planos decorrentes, foram elaborados sob supervisão do GSI e coordenação da ABIN, em colaboração com outros órgãos do SISBIN, sem maior engajamento político ou participação de atores externos. A elaboração da PNI e os planos decorrentes trouxeram a concretude necessária para viabilizar a implementação da política pública. No entanto, a baixa orientação da comunidade política na formulação desses documentos balizadores diminuiu tanto a legitimidade quanto a efetividade da política pública de Inteligência.

Em diferentes governos, houve entendimento variado sobre a melhor forma de planejar a execução da política pública de Inteligência. Nas ocasiões em que não fora tratada como atividade de apoio às políticas públicas, buscou-se inserir a política de Inteligência no Plano Plurianual (PPA), concedendo-lhe maior visibilidade ao se apresentar o planejamento de implementação da política na forma de programa finalístico.

Apesar da variação nas metodologias adotadas para a apresentação de programas finalísticos no PPA nos diversos governos, a abordagem técnica busca replicar as características do marco lógico. A ideia é partir de um problema para delinear propostas de intervenção alinhadas ao conceito estratégico governamental que resultem em entregas objetivas, apresentadas na forma de produtos e serviços. Os resultados esperados são traduzidos em Indicadores e metas. Os recursos orçamentários associados a essas entregas conferem a dimensão do esforço para o atingimento das metas e servem de referen-

ciais para avaliar a eficiência e a efetividade dos programas na fase de avaliação.

Conforme se observa no Manual Técnico do Plano Plurianual 2024-2027 (Brasil, 2023, p. 14):

“No PPA, o modelo lógico apresenta-se como a principal ferramenta para a construção do desenho dos programas. Nesse sentido, segue a especificação de alguns elementos constitutivos dos programas: a) do problema ser enfrentado (ou mitigado); b) das alternativas existentes para combater o problema; c) dos resultados pretendidos pela intervenção, ou seja, dos benefícios a serem auferidos pelo público-alvo; e d) do volume de recursos financeiros requeridos para intervenção pública”

Em que pese a maior publicidade conferida à Atividade de Inteligência, nas ocasiões que compôs o PPA como programa finalístico, não foram observados adequadamente os elementos previstos para o desenho do programa. No PPA 2008-2011, o programa 0641 – Inteligência Federal previa como entregas “ações realizadas” para a principal atividade de assessoramento da ABIN (Brasil, 2008). As metas anuais propostas variaram entre 620 e 775 ações realizadas ao longo da vigência do programa, mas não havia maior detalhamento sobre a natureza dessas ações ou como o indicador seria apurado. Como ainda não havia sido aprovada a PNI, as diretrizes para a Atividade de Inteligência eram estabelecidas, na ocasião, por meio de resoluções da CREDEN, de modo que não havia publicidade sobre o escopo temático dessas ações e o que representariam em termos de benefícios ao público-alvo da política. Nos PPAs entre 2012 e 2019, a Atividade de Inteligência não constou como programa finalístico, sendo considerada dentro do programa de apoio a políticas públicas.

No PPA 2020-2023, a Atividade de Inteligência não foi diretamente mencionada, mas compunha o programa finalístico 4002 – Segurança Institucional (Brasil, 2019). Conforme a metodologia adotada, figurava

como resultado intermediário esperado do programa a entrega “0018 – Inteligência para o assessoramento político/estratégico fornecida”, cuja meta anual era atingir 80% das solicitações atendidas por meio de relatórios de inteligência produzidos e difundidos como assessoramento às questões relacionadas à soberania, aos interesses nacionais e à segurança do Estado e da Sociedade (Brasil, 2021). Embora melhor qualificada a entrega (relatórios de inteligência), a meta proposta não se mostrava suficiente para compreender os resultados esperados para o público-alvo.

Uma vez aprovada a PNI, constata-se que a Atividade de Inteligência deve acompanhar leque variado de temas, apresentados na forma de ameaças, além da expectativa de que possa contribuir com conhecimentos para o apoio às demais políticas públicas. Por esse motivo, a Atividade de Inteligência no Brasil, sobretudo a ABIN, no seu papel de órgão central, tem como desafio prestar assessoramento a elevado número de potenciais usuários com necessidades informacionais diversas entre si, cuja prioridade de acompanhamento oscila conjuntamente. Isso explica a dificuldade encontrada para desenhar os programas finalísticos, conforme as orientações técnicas, e reforça a noção de que se caracteriza melhor como atividade de apoio às políticas públicas ou, alternativamente, deveria ser apresentada como ação transversal aos demais programas do PPA, exigindo, para tanto, maior esforço de planejamento e articulação interministerial.

A análise do planejamento da implementação da política de Inteligência, conforme os documentos públicos, demonstra que não está clara a forma de intervenção, ou seja, da relação de causa e efeito da ação governamental na forma de assessoramento de Inteligência nas decisões dos usuários. Isso prejudica a demonstração da lógica de planejamento na destinação de recursos financeiros, humanos e tecnológicos para garantir resultados. Como consequência, cria-se um desafio para o estabelecimento de indicadores e metas capazes de mensurar a eficiência e a efetividade das entregas, prejudicando a avaliação da

política pública, bem como a prestação de contas à sociedade sobre a relevância da atividade e a importância de empregar recursos públicos para a sua execução.

Mais ainda, a ação sistêmica da arquitetura de implementação da política na forma do SISBIN não tem sido adequadamente endereçada nos instrumentos de planejamento governamental. O arranjo institucional é composto por organizações que produzem conhecimentos com finalidades decisórias diversas e bem delimitadas para atender às necessidades dos dirigentes máximos de suas unidades, com exceção da ABIN, que no papel de órgão central, deve atender a escopo mais abrangente de temas da PNI e demandas para assessoramento a políticas públicas. Sem adequado compartilhamento de responsabilidades e capacidades, há risco de ineficiência e falhas no atingimento dos objetivos colimados pela política. Há que se ter em mente que o SISBIN foi tratado nos documentos de referência da política como principal elemento do arranjo de implementação.

Após a recente transferência de subordinação da ABIN para a Casa Civil (Brasil, 2023a), iniciativas têm sido implementadas para a reorganização do SISBIN e a reestruturação da própria Agência. Resta ainda promover a revisão dos marcos referenciais da política, sobretudo a atualização da PNI e revisão dos demais documentos dela decorrentes, como a ENINT e os planos de trabalho, instituídos pelo decreto do novo SISBIN (Brasil, 2023b).

A revisão da PNI deve considerar as mudanças no ambiente estratégico no qual a Atividade de Inteligência deve atuar. A proliferação de atores e fontes de conflito, segurança cibernética, crime organizado, mudanças climáticas, desinformação, atos contra o Estado democrático, transição energética, conflitos e violência motivados por questões étnicas, religiosas e ideológicas são tendências para as quais a Atividade de Inteligência deve estar preparada. Inovações tecnológicas revolucionaram a forma de acesso, coleta e análise de

dados e informações. Cada vez mais a atuação em rede e o compartilhamento de informações e capacidades se mostram determinantes para o adequado desempenho das funções de assessoramento e contrainteligência. O aprofundamento dos mecanismos de controle e supervisão e a transparência ativa são elementos essenciais para a garantia da segurança da Sociedade e do Estado Democrático de Direito.

3. Implementação

A implementação da política pública da Atividade de Inteligência, desde 1999, se estruturou ao longo de dois eixos principais: a coordenação do SISBIN e a produção de conhecimentos para o assessoramento do processo decisório nacional. Como decorrência da Lei 9.883/1999, o Decreto nº 4.376/2002 dispôs sobre a organização e funcionamento do SISBIN. A construção da arquitetura do sistema derivou da experiência histórica na qual o órgão central buscava manter a autonomia estrutural para reforçar sua centralidade. Um Conselho Consultivo, composto pelo GSI e órgãos dedicados à Atividade de Inteligência das áreas de Defesa, Relações Exteriores, Segurança Pública e Fazenda conformaria o núcleo do sistema. Esse Conselho ficou responsável por emitir pareceres sobre a PNI, propor normas para o funcionamento do sistema, contribuir para o aperfeiçoamento doutrinário e opinar sobre a integração de novos órgãos ao sistema. A composição dos SISBIN sofreu diversas alterações ao longo dos anos devido à inclusão de novas organizações.

Devido à peculiaridade e à especialização no desenvolvimento da Atividade de Inteligência nos diversos órgãos que o compunham, o sistema conviveu com o desafio de ampliar a coesão entre seus membros. O alargamento do sistema, embora destacando a crescente importância da atividade, contribuiu para a variação na densidade no intercâmbio e para a diversificação de dados e conhecimentos.

A avaliação sobre a efetividade do arranjo para a implementação da política carece de indicadores adequados, uma vez que somente foram consideradas variáveis de esforço voltadas para monitorar o nível de intercâmbio entre seus membros. Mesmo diante dos desafios para maior integração e adensamento das comunicações e intercâmbio de dados, o SISBIN apresentou avanços na coordenação e planejamento de atividades, sobretudo por ocasião da realização de grandes eventos no Brasil e nas operações de proteção das fronteiras.

Considerando a outra forma de implementação da política pública de Inteligência, isso é, a produção de conhecimento para assessoramento estratégico às autoridades nacionais, merece destaque o assessoramento prestado pela Atividade de Inteligência em apoio ao processo decisório em temas relativos a questões socioambientais, segurança pública e políticas migratórias. Na área de Contraineligência, com o Programa Nacional de Proteção do Conhecimento Sensível (PNPC) (Brasil, 2024a), o Programa de Articulação entre Governo, Empresas e Instituições Acadêmicas para a Prevenção e Mitigação do Risco de Eventos Químicos, Biológicos, Radiológicos e Nucleares Seleccionados (Pangeia) (Brasil, 2024b) e o Programa Nacional de Integração Estado-Empresas da Área de Bens Sensíveis (Pronabens) (Brasil, 2024c). Na área de prevenção ao extremismo violento e ao terrorismo, além da detecção e monitoramento de ameaças, a Agência desenvolveu o Protocolo de Prevenção ao Extremismo Violento, que foi adaptado para a aplicação também na prevenção de atos violentos em escolas.

É importante mencionar que o assessoramento prestado pela ABIN nesses temas tem contado com a cooperação dos órgãos do SISBIN, que fornecem dados, informações e conhecimentos, que são integrados a outros, produzidos pela agência, e resultam em relatórios de inteligência para difusão aos usuários e aos próprios membros do sistema.

No campo da pesquisa e desenvolvimento para a segurança da informação e das comunicações, foram igualmente relevantes o desen-

volvimento e o contínuo aperfeiçoamento da criptografia de Estado e sua aplicação em soluções para proteger as comunicações governamentais. Desde 1996, o Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC) vem prestando assessoramento à Justiça Eleitoral para a segurança do processo eleitoral brasileiro. Atualmente, o centro busca a vanguarda tecnológica no desenvolvimento de criptografia pós-quântica, que está sendo utilizada nas soluções para segurança da urna eletrônica e demais produtos disponíveis para uso dos órgãos governamentais (Pacheco *et al*, 2022).

A Escola de Inteligência é responsável pela formação dos profissionais de Inteligência egressos de concursos públicos que passaram a desempenhar a Atividade de Inteligência e as funções de apoio logístico especializado na ABIN. Também se encarrega da capacitação de agentes públicos de órgãos que compõem o SISBIN. Com o credenciamento junto ao MEC, a ESINT passou a oferecer cursos de especialização para os órgãos do SISBIN e, mais recentemente, outros cursos orientados para o desenvolvimento de competências específicas aos membros das carreiras de Inteligência da ABIN. Finalmente, a ESINT vem implementando projeto para reformulação e adequação doutrinária (Brasil, 2023b) e dos métodos e processos da Atividade de Inteligência. Esse esforço materializa a busca de alinhamento da atividade ao contexto democrático em resposta às demandas da sociedade.

4. Avaliação e Controle

A especificidade da política pública de inteligência demanda abordagem diferenciada em termos de avaliação, que não se limite aos critérios típicos de eficiência e efetividade, mas que também atente para a legitimidade da sua implementação. Além disso, a complexidade das relações entre agências de inteligência e usuários, nem sempre permite identificar a influência e a qualidade do assessoramento prestado para a tomada de decisões, uma vez que estas são determinadas por uma série de fatores e fontes de informação.

Considerando o critério da eficiência, a avaliação da política pública de Inteligência com base nas métricas usuais no desempenho de programas do PPA se mostra limitada. Conforme referenciamos anteriormente, indicadores e metas associados aos programas finalísticos para área de Inteligência não se mostraram adequados ou suficientes para servir de parâmetro para a análise desta dimensão da ação governamental nesse segmento.

A efetividade da política pública de Inteligência, ou seja, a capacidade de atingir os resultados pretendidos, é geralmente mal dimensionada, pois, por definição, os sucessos de uma agência de inteligência frequentemente precisam ser mantidos em segredo, enquanto as falhas são alvo de escrutínio público, midiático e político. Assim, poucas referências existem sobre o assessoramento bem-sucedido resultante da Atividade de Inteligência. Normalmente, são falhas que chegam ao conhecimento público e motivam questionamentos políticos, investigações e reforma de sistemas e instituições dedicados à Atividade de Inteligência (George; Bruce, 2008). Ao longo de sua história, a Atividade de Inteligência no Brasil, sobretudo a ABIN, foi igualmente afetada por essa tendência.

As falhas na Atividade de Inteligência podem estar relacionadas à orientação e à priorização dos trabalhos, por não atenderem às necessidades informacionais dos usuários, ou mesmo deficiências na coleta ou na busca de dados, por se mostrarem insuficientes ou não relevantes para a finalidade de produção de conhecimento. Neste particular, é preciso reconhecer que as limitações de recursos humanos, orçamentários e tecnológicos influenciam a capacidade de resposta e o escopo dos assuntos sob acompanhamento da Atividade de Inteligência.

Em muitos casos, falhas ocorrem na análise dos dados, por não considerar a eventual incorreção na formulação de hipóteses ou a interferência de vieses cognitivos, sem mencionar a possibilidade de desinformação por parte dos atores adversos. Também pode haver falhas

na difusão dos conhecimentos, como o envio de relatórios com muita antecedência ao usuário cuja agenda política está tomada por outros assuntos de maior importância imediata; a disponibilização de documentos sem que haja tempo hábil para tomada de decisão; ou a falta de acesso a conhecimentos relevantes e úteis ao usuário que detinha necessidade de conhecer. Mais ainda, há falhas resultantes da relação entre os tomadores de decisão e os órgãos responsáveis pela produção de conhecimentos, seja devido à inadequada interferência política no desenvolvimento da Atividade de Inteligência ou à resistência dos usuários a se apropriarem dos conhecimentos produzidos, sobretudo quando apontam situações e tendências que contrariam a percepção ou o direcionamento dos usuários.

No caso brasileiro, não somente dúvidas sobre a qualidade dos dados coletados ou dos conhecimentos produzidos, mas também sobre a utilidade e a oportunidade do assessoramento prestado foram objeto de críticas por parte de autoridades, meios de comunicação e instâncias de controle externo da Atividade de Inteligência. Essas críticas devem, no entanto, ser ponderadas com as limitações de recursos humanos e orçamentários e a extensão dos mandatos legais para o desenvolvimento da atividade. Além disso, desvios de finalidade ou mesmo de conduta de agentes públicos instigaram crises e reformas institucionais no órgão central e no sistema de Inteligência.

Esses efeitos indesejados na implementação da política pública de Inteligência devem ser estudados para aperfeiçoar os instrumentos da política de Inteligência e estabelecer controles adequados visando não somente garantir maior efetividade, mas também legitimidade à atividade. Dada a sensibilidade da atividade e crescente demanda da sociedade por maior transparência e controles, elementos essenciais em contexto democrático, é crucial que se estabeleçam mecanismos para garantir amplo acesso às instâncias responsáveis pelo controle externo da Atividade de Inteligência. A transparência ativa e o engajamento da comunidade epistêmica e outros formadores de opinião

também são fatores determinantes para a legitimidade da Atividade de Inteligência.

De todo modo, considerando o sigilo como característica peculiar da atividade, a avaliação da política tende a trabalhar quase que exclusivamente com informações sobre falhas e desvios passados. Por esse motivo, é inevitável que as reformas na política de Inteligência ou na arquitetura de implementação ocorram em momentos de crise e estejam orientadas a dar resposta a situações passadas, ou seja, há a possibilidade de que as formulações não sejam adequadas para mitigar ou evitar riscos futuros.

Avaliando os principais desvios na Atividade de Inteligência no passado recente, pode-se concluir que estiveram relacionados com a aplicação de técnicas operacionais em ações especializadas sigilosas para a obtenção de dados. Esses casos motivaram não somente questionamentos perante a CCAI, mas também foram investigados em CPIs e inquéritos policiais.

As técnicas operacionais são procedimentos e métodos especializados para desenvolver ações sigilosas de busca de dados necessários para a produção de conhecimentos (Brasil, 1999). A utilização de técnicas operacionais é necessária para suplantar obstáculos à obtenção de dados negados (Brasil, 2023b). Isto para viabilizar o acompanhamento de fatos ou situações que podem representar ameaças aos interesses nacionais ou para possibilitar a contraposição a ações de agentes adversos, sejam eles estatais ou não, domésticos ou estrangeiros. As técnicas operacionais podem ser desenvolvidas tanto no espaço físico quanto no espaço cibernético (Brasil, 2023b).

O emprego de técnicas operacionais pode representar riscos à privacidade, à intimidade e à proteção de dados pessoais, garantias fundamentais previstas na Constituição brasileira. Não obstante, o arcabouço normativo brasileiro não disciplina com a profundidade que

os riscos exigem e com a especificidade necessária a extensão dos mandatos da atividade, particularmente no que se refere ao emprego dessas técnicas.

Como observa Cepik (2003, p. 165):

Os mandatos legais são necessários tanto para estabelecer parâmetros para os governantes controlarem o grau de eficiência e efetividade dos serviços de inteligência e de segurança (agilidade), quanto para auxiliar os cidadãos a controlarem o grau de compatibilidade entre a atuação desses mesmos serviços e as regras institucionais democráticas (transparência). Um aspecto pouco notado a respeito dos mandatos é que, do ponto de vista dos serviços de inteligência, estes funcionam também como uma forma de proteção das agências contra eventuais pressões políticas de ministros ou chefes de Estado para a realização de missões impróprias que, diante da existência de mandatos codificados legalmente, seriam também ilegais e passíveis de responsabilização.

Como forma de preservar as garantias fundamentais previstas na Constituição e mitigar riscos de desvios na conduta operacional na Atividade de Inteligência, entende-se necessária, oportuna e conveniente a regulamentação, pelo Congresso Nacional, do emprego de técnicas operacionais e tecnologias associadas para fins da Atividade de Inteligência.

Mais ainda, além das diretrizes e controles do próprio Poder Executivo e ampliação do controle externo do Poder Legislativo, outra forma de mitigar riscos de desvios na Atividade de Inteligência seria envolver o Poder Judiciário. Mesmo que reconheça sua incapacidade para julgar práticas do Poder Executivo em matéria de segurança nacional, o Poder Judiciário poderia exercer controle de legalidade e razoabilidade por meio de aprovação *ex ante* na aplicação de técnicas operacionais (Cepik, 2003, p. 169). Esse controle se fundamentaria em exame e autorização para o emprego de determinadas técnicas ponderando

o potencial de ameaça à segurança da sociedade e do Estado imposta pela situação sob exame da Atividade de Inteligência, enquanto ainda não configurado ilícito penal, cível ou mesmo infração de ordem administrativa. Essa experiência de controle jurisdicional da Atividade de Inteligência é realidade em alguns países como Argentina, Canadá, Espanha e EUA¹.

A regulamentação de capacidade postulatória específica para provocar o Poder Judiciário para prévia autorização ao emprego de técnicas operacionais, com a criação de juízo especializado para conhecer de temas relativos à Atividade de Inteligência de Estado, induziria a prestação jurisdicional mais robusta e o controle mais efetivo dos riscos relativos à proteção de direitos e garantias fundamentais. Desse modo, a limitação da discricionariedade dos profissionais de inteligência no emprego de ações sigilosas seria tratada nos casos concretos, ponderando quais e em que nível essas técnicas operacionais e soluções tecnológicas podem ser empregadas, diante do risco à privacidade e à proteção de dados pessoais e da necessidade de obter dados relevantes e confiáveis para prevenir ameaças e resguardar a segurança da sociedade e do Estado brasileiros.

Há inegável conflito entre o segredo, essencial para o desenvolvimento da Atividade de Inteligência, e a demanda por maior controle e transparência em regimes democráticos. A busca de maior legitimidade na implementação da política de Inteligência depende de atitude proativa das instituições dedicadas ao exercício da atividade em ampliar os canais de diálogo com a sociedade e atores políticos. No estágio atual da democracia brasileira, a resistência das instituições em alinhar suas práticas ao que lhes é exigido e demandado pela sociedade e pelas instâncias de controle, representa prejuízos na busca de

1 Argentina: Título VI – Interceptación y captación de comunicaciones, Ley de Inteligencia Nacional (Ley 25.520/2001); Canadá: Part II – Judicial Control, Canadian Security Intelligence Act (1985); Espanha: Ley Orgánica 2/2002, reguladora de control judicial previo del Centro Nacional de Inteligencia; EUA: Foreign Intelligence Surveillance Act of 1978.

maiores recursos, da segurança jurídica para o exercício da atividade e, finalmente, para garantir a legitimidade do assessoramento prestado aos tomadores de decisão.

Conclusão

A dinâmica de participação da Atividade de Inteligência na agenda política e o modo como os atores políticos interagiram com a questão, variando entre distanciamento e elevado interesse em momentos de crise, determinaram os rumos do processo decisório para a formulação dos referenciais da política de Inteligência. A realidade brasileira não se distancia do que tem sido observado por especialistas no tema em relação à situação em outros países. De certo modo, a ação reativa dos agentes políticos a falhas ou desvios na ação das instituições orientam-se para solucionar problemas pretéritos, o que não garante que as propostas de reforma sejam adequadas para prevenir ou evitar situações similares no futuro. Normalmente, do embate de interesses e assimetrias de capacidades entre os atores políticos resultam decisões negociadas de forma incremental e experimental, promovendo ajustes graduais, satisfatórios para o momento, mas não necessariamente suficientes para promover a transformação necessária.

Devido à especificidade técnica e à confidencialidade de métodos e processos da atividade, a sociedade e os formadores de opinião demonstram pouco interesse em debater e se apropriar das questões relativas à Inteligência. Além disso, os referenciais da política, como foi observado, pouco contribuíram para detalhar e limitar os mandatos legais das instituições encarregadas de sua implementação, sobretudo no que se refere ao uso de técnicas sigilosas. Desse modo, abriu-se espaço para maior influência dos profissionais de Inteligência na formulação da política, como também para o recurso à discricionariedade na sua implementação. Observou-se também certo descompasso entre a demanda da sociedade e das instituições democráticas por controles, transparência e demonstração de resultados e a capa-

cidade de resposta das instituições responsáveis pela implementação e governança da política pública.

É inegável a necessidade de revisão dos referenciais da política e de seu arranjo de implementação. O maior engajamento de atores políticos, da comunidade epistêmica e demais formadores de opinião contribuiria para maior legitimidade da política. Essa revisão deve, de todo modo, estar em linha com o ambiente estratégico no qual a Atividade de Inteligência se insere. Diante da complexidade desse ambiente estratégico, o SISBIN consolida-se como fator-chave na implementação da política. Por esse motivo, com vistas a garantir maior eficiência e efetividade, é necessário não apenas aprofundar a coordenação entre agências, mas promover o maior compartilhamento de capacidades. A inovação tecnológica que vem transformando o acesso, a coleta e a análise de dados e, por esse motivo, métodos e processos de produção de conhecimentos, também potencializa o compartilhamento e a integração segura de conhecimentos, observados o princípio da segurança jurídica, a necessidade de conhecer, o interesse público e a devida motivação.

Há ainda que se enfrentar o desafio de aperfeiçoar o planejamento, englobando sobretudo visão sistêmica, e a avaliação da política pública. A despeito do necessário sigilo no desenvolvimento da Atividade de Inteligência, a adequada comunicação dos resultados esperados das ações de Inteligência e de seu monitoramento contribui para ampliar a transparência e favorece a defesa de ampliação dos recursos destinados a sua execução, criando melhores condições de adequar meios disponíveis e fins almejados pela ação governamental.

Ademais, inobstante a premente atualização da PNI, associada à edição de outros normativos específicos relativos a mandatos legais da ABIN e do SISBIN, subsiste a necessidade de se promover fortalecimento, engajamento e mesmo inovações em relação aos mecanismos de controle sobre a atividade no Brasil, notadamente no que se refere à

atuação dos Poderes Legislativo, por meio da CCAI, e, eventualmente, do Judiciário, por meio da criação de juízo especializado. Além disso, entende-se necessário revisar os processos de trabalho na Atividade de Inteligência para que, a partir de criteriosa avaliação de riscos, estabeleçam-se controles preventivos, possibilitem a rastreabilidade e a devida transparência aos órgãos de controle e, sobretudo, garantam o respeito aos direitos fundamentais e a proteção da privacidade.

O aprimoramento da Atividade de Inteligência, enquanto política pública relevante ao Estado e a sociedade brasileiros, mostra-se oportuno e sobremaneira necessário quando se considera a progressiva complexidade do ambiente sócio-político em que profissionais de inteligência precisam atuar em defesa da democracia brasileira. Nesse sentido, Bruce e George (2008) destacam a importância de lideranças responsáveis na gestão dessa rede de conexões entre política pública, agências de Inteligência, decisores, atores políticos e comunidade epistêmica. Uma vez que falhas e desvios da Atividade de Inteligência se tornaram evidentes publicamente, é natural que a análise esteja condicionada a buscar oportunidades de aperfeiçoamento da política pública e da sua estrutura de implementação e governança. De todo modo, é importante igualmente reconhecer a relevância do assessoramento prestado pela ABIN e demais órgãos do SISBIN nesses 25 anos e da experiência histórica de adaptação da atividade ao contexto democrático, a partir da qual líderes do presente e do futuro projetarão as mudanças necessárias para ampliar a eficiência, a efetividade e a legitimidade da política de inteligência para segurança da sociedade e do Estado brasileiros.

Referências

AMBROS, C. C. **Inteligência governamental como política pública:** fatores cognitivos e institucionais na explicação de falhas e dilemas de efetividade. 2011. Artigo Final (Mestrado em Ciência Política) – Programa de Pós-Graduação em Ciência Política, Universidade Federal do Rio Grande do Sul, Porto Alegre.

BARCELOS, C. L. K.; CALMON, P. C. Du P. **Decisões Alcativas no Setor Público: organizando o mosaico de proposições teóricas com o auxílio de lentes conceituais – um ensaio exploratório. Encontro de Administração Pública e Governança.** Vitória/ES: Anpad, 2010.

BRASIL. **PL 3.651/1997.** Projeto de Lei que institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências. Brasília, DF: Câmara dos Deputados, [1997a]. Disponível em: <https://imagem.camara.gov.br/imagem/d/pdf/DCD23SET1997.pdf#page=10>. Acesso em: 17 out. 2024.

_____. Câmara dos Deputados. Proposta de criação da Agência Brasileira de Inteligência – ABIN e do Sistema Brasileiro de Inteligência – SISBIN, de 23 de setembro de 1997. Brasília, DF: Câmara dos Deputados, [1997b]. Disponível em: <https://imagem.camara.gov.br/imagem/d/pdf/DCD23SET1997.pdf#page=1.00&gsr=0>. Acesso em: 17 out 2014.

_____. **Lei nº 9.883, de 7 de dezembro de 1999.** Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências. Brasília, DF: Presidência da República, [1999]. Disponível em: http://planalto.gov.br/CCIVIL_03/LEIS/L9883.htm. Acesso em: 17 out. 2024.

_____. **Medida Provisória nº 1999-14, de 13 de janeiro de 2000.** Altera dispositivos da Lei nº 9.649, de 27 de maio de 1998, que dispõe sobre a organização da Presidência da República e dos Ministérios e dá outras providências. Brasília, DF: Presidência da República, [2000]. Disponível em: <https://legis.senado.leg.br/norma/558217/publicacao/15717616.htm>. Acesso em: 15 out. 2024.

_____. **Decreto nº 4.376, de 13 setembro de 2002.** Dispõe sobre a organização e funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei nº 9.883, de 7 de setembro de 1999, e dá outras providências. Brasília, DF: Presidência da República, [2002]. Disponível em: http://planalto.gov.br/CCIVIL_03/decreto/D4376.htm. Acesso em: 15 out. 2024.

_____. **Decreto nº 4.801, de 6 de agosto de 2003.** Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo. Brasília, DF: Presidência da República, [2003]. Disponível em: www.planalto.gov.br/CCivil_03/decreto/D4801.htm. Acesso em: 15 out. 2024.

_____. **Lei nº 10.862, de 20 de abril de 2004.** Dispõe sobre a criação do Plano Especial de Cargos da Agência Brasileira de Inteligência – ABIN e dá outras providências. Brasília, DF: Presidência da República, [2004]. Disponível em: www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l10.652.htm. Acesso em: 15 out. 2024.

_____. **Lei nº 11.653, de 7 de abril de 2008.** Dispõe sobre o Plano Plurianual da União para o período de 2008/2011. Brasília, DF: Presidência da República, [2008a]. Disponível em: https://bibliotecadigital.economia.gov.br/bitstream/123456789/704/2/AnexoII_At2011.pdf. Acesso em: 11 out. 2024.

_____. **Lei nº 11.776, de 17 de setembro de 2008.** Dispõe sobre a estruturação do plano de carreiras e cargos da Agência Brasileira de Inteligência – ABIN, cria as carreiras de Oficial de Inteligência, Oficial Técnico de Inteligência, Agente de Inteligência, Agente Técnico de Inteligência e dá outras providências. Revoga dispositivos das Leis nºs 9.651, de 27 de maio de 1998, 11.333, de 22 de dezembro de 2005, e 11.292, de 26 de abril de 2006, e as Leis nºs 10.862, de 20 de abril de 2004, e 11.362, de 19 de outubro de 2006. Brasília, DF: Presidência da República, [2008b]; Disponível em: <https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=11776&ano=2008&ato=337cXWE5UNRpWT12f.htm>. Acesso em: 15 out. 2024.

_____. **Decreto 44855 de 18 de fevereiro de 2009.** Institui o Comitê Ministerial para Elaboração da Política Nacional de Inteligência e Reavaliação do Sistema Brasileiro de Inteligência. Brasília, DF: Câmara dos Deputados, [2009]. Disponível em: <https://www2.camara.leg.br/>

legin/fed/decret_sn/2009/decreto-44855-18-fevereiro-2009-586440-publicacaooriginal-109934-pe.html. Acesso em: 17 out. 2024.

_____. Mensagem Presidencial nº 997, de 9 de dezembro de 2009, que encaminha o texto da proposta da Política Nacional de Inteligência, de conformidade com a inclusa Exposição de Motivos do Senhor Ministro de Estado Chefe de Segurança Institucional da Presidência da República. *In Anais do Senado Federal. Ata da 246ª Sessão da 3ª Sessão Legislativa Ordinária da 53ª Legislatura. Vol. 33, nº 92-B. Brasília: Subsecretaria de Anais, 2009.* Disponível em: https://www.senado.leg.br/publicacoes/anais/pdf/Anais_Republiva/2009/2009_Livro_92-b.pdf. Acessado em: 17 out. 2024.

_____. **Resolução nº 2, de 2013.** Dispõe sobre a Comissão Mista de Controle das Atividades de Inteligência (CCAI), comissão permanente do Congresso Nacional, órgão de controle e fiscalização externos da Atividade de Inteligência, previsto no art. 6º da Lei nº 9.883, de 7 de dezembro de 1999. Brasília, DF: Congresso Nacional, [2013]. Disponível em: <https://www2.camara.leg.br/legin/fed/rescon/2013/resolucao-2-22-novembro-2013-777449-publicacaooriginal-141944-pl.html>. Acesso em: 14 out. 2024.

_____. **Decreto nº 8.793, de 29 de junho de 2016.** Fixa a Política Nacional de Inteligência. Brasília, DF: Presidência da República, [2016]. Disponível em: www.planalto.gov.br/CCvill/03/_Ato2016-2018/2016/Decreto/D8793.htm. Acesso em: 15 out. 2024.

_____. **Lei nº 13.971, de 27 de dezembro de 2019.** Institui o Plano Plurianual da União para o período de 2020 a 2023. Brasília, DF: Presidência da República, [2019]. Disponível em: <https://bibliotecadigital.economia.gov.br/bitstream/123456789/1098/3/anexo-i.pdf>. Acesso em: 11 out. 2024.

_____. **Manual Técnico do Plano Plurianual 2024-2027.** Ministério do Planejamento e Orçamento, [2023a]. Disponível em: <https://www.gov.br/planejamento/pt-br/centrais-de-conteudo/publicacoes/manual-do-ppa-2024-2027.pdf>. Acessado em: 15 out. 2024.

_____. Agência Brasileira de Inteligência. **Doutrina da Atividade de Inteligência.** Brasília, DF: ABIN [2023b]. Disponível em: <https://www.gov.br>.

br/abin/pt-br/centrais-de-conteudo/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023.htm. Acessado em: 15 out. 2024.

_____. Ministério da Economia. **Programa Plurianual 2020-2023**. Resultados Intermediários, maio de 2021. Disponível em: <https://bibliotecadigital.economia.gov.br/bitstream/123456789/1107/relatorio-resultados-intermediarios-ppa-2020-2023.pdf>. Acessado em: 11 out. 2024.

_____. **Decreto nº 11.426, de 1º de março de 2023**. Altera o Decreto nº 11.327, de 1º de janeiro de 2023, o Decreto nº 9.435, de 2 de julho de 2018, e o Decreto nº 4.376, de 13 de setembro de 2002, para integrar a Agência Brasileira de Inteligência à Casa Civil da Presidência da República. Brasília, DF: Presidência da República [2023]. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-11.426-de-1-marco-de-2023-467443153.htm>. Acesso em: 15 out. 2024.

_____. **Decreto nº 11.693, de 6 de setembro de 2023**. Dispõe sobre a organização e funcionamento do Sistema Brasileiro de Inteligência. Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm. Acesso em: 15 out. 2024.

_____. Agência Brasileira de Inteligência. **Política Nacional de Proteção de Conhecimentos Sensíveis (PNPC)**. [2024a]. Disponível em: <https://www.gov.br/abin/pt-br/institucional/acoes-e-programas/PNPC>. Acesso em: 15 out 2024.

_____. Agência Brasileira de Inteligência. **Pangeia**. [2024b] Disponível em: <https://www.gov.br/abin/pt-br/institucional/acoes-e-programas/pangeia-1>. Acesso em: 15 out 2024.

_____. Agência Brasileira de Inteligência. **Pronabens**. [2024c] Disponível em: <https://www.gov.br/abin/pt-br/institucional/acoes-e-programas/pronabens>. Acesso em: 15 out 2024.

BOULLOSA, R.F. Por uma nova agenda de revisão crítica do duplo construto lasswelliano policy science e policy orientation: democracia, pragmatismo e criticidade. Revista Brasileira de Ciência Política, v. 43, p. e274255, 2024.

CARDIM, M. E. **Fatores chave no processo de implementação de políticas públicas em Portugal.** Artigo apresentado no XIV Congresso de Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública. Salvador/BA, 2009. Disponível em: <http://siare.clad.org/fulltext/0062606.pdf>. Acessado em: 25 abr. 2012.

CEPIK, M. A. C. **Espionagem e Democracia:** agilidade e transparência como dilemas na institucionalização de serviços de inteligência. Rio de Janeiro: Fundação Getúlio Vargas. 2003

FAGUNDES, R. Arapongas serão fiscalizados. Editorial: Brasil, p. 06. Jornal do Brasil, 1999.

GEORGE, R. Z.; BRUCE, J. B. (ed.). **Analyzing Intelligence: origins, obstacles, and innovations.** Georgetown University Press: 2008.

GILL, P. **Seminar:** Intelligence Activities in Brazil:: contributions to sovereignty and democracy.. In: CCAI Comissão Mista De Controle Das Atividades De Inteligência, 2002, Brazil. Panel: Intelligence, Public Control and Democracy. Brasília: Congresso Nacional, 2002.

GONDIM, A. **PF fez escuta de agentes da Casa Militar.** *Folha de São Paulo*, 1999. Disponível em: <https://www1.folha.uol.com.br/fsp/brasil/fc28059905.htm>. Acesso em: 10 out. 2024.

HOWLETT, M.; RAMESH, M. **Studying public policy:** Policy cycles and policy subsystems. Don Mills, Ont.: Oxford University Press, 2003.

LASSWELL, Harold. The Policy Orientation. In: BRAMAN, S. (Ed). **Communication Researchers And Policy-Making**, [S.l.], p. 85-104, 11 ago. 2003. The MIT Press. DOI: <http://dx.doi.org/10.7551/mitpress/1949.003.0007>. Disponível em: <https://direct.mit.edu/books/edited-volume/3823/chapter-abstract/125396/The-Policy-Orientation?redirectedFrom=PDF>. Acesso em: 01 nov. 2024.

LINDBLOM, C. E. The Science of. *Public Administration Review*, [S.L.], v. 19, n. 2, p. 79, 1959. **JSTOR.** <http://dx.doi.org/10.2307/973677>. Disponível em: <https://www.jstor.org/stable/973677>. Acesso em: 6 mai. 2012.

LOTTA, G. A política pública como ela é: contribuições dos estudos sobre implementação para a análise de políticas públicas. In: LOTTA, G. (org.).

Teorias e Análises sobre Implementação de Políticas Públicas no Brasil. Brasília: Enap, 2019. p. 11-38.

PACHECO, Rodrigo et al. Libharpia: a new cryptographic library for brazilian elections. **Anais do XXII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais** (Sbseg 2022), [S.l.], p. 250-263, 12 set. 2022. Sociedade Brasileira de Computação – SBC. <http://dx.doi.org/10.5753/sbseg.2022.224098>.

PEDONE, L.; VEDUNG, E.. **Avaliação de políticas públicas e programas governamentais: fundamentos e modelos.** Rio de Janeiro: Ed. Luzes, 2021.

SALLES, L.; VALLE, L. A. P. A agenda legislativa da Abin: análise das proposições sobre Atividade de Inteligência de estado no congresso nacional de 1997 a 2017. **Revista Brasileira de Inteligência**, [S.l.], n. 13, p. 149-163, 1 dez. 2018. Agência Brasileira de Inteligência. <http://dx.doi.org/10.58960/rbi.2018.13.156>. Acesso em: 17 out. 2024.

SECCHI, L. **Políticas Públicas: conceitos, esquemas de análise, casos práticos.** São Paulo: Cengage Learning, 2010.

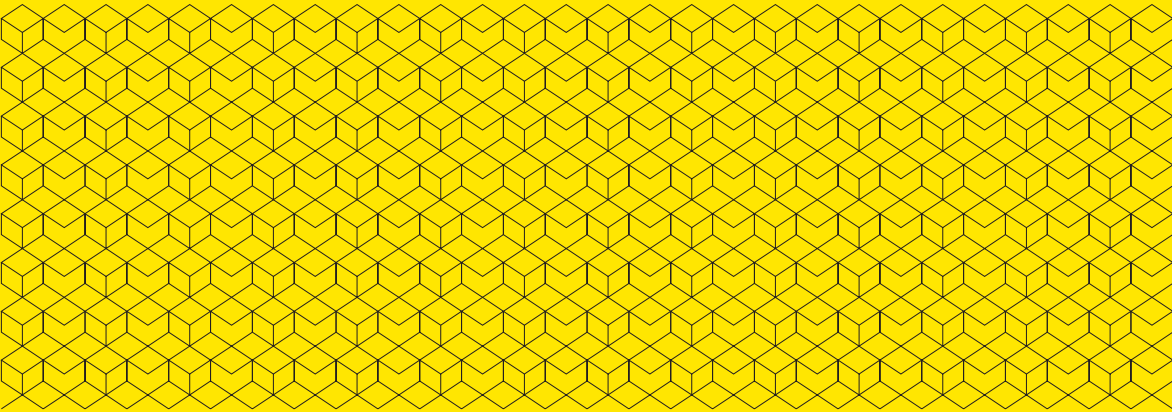
TEMOR de escândalo teria levado governo ao grampo. **Folha de São Paulo**, São Paulo, 28 de maio de 1999. Disponível em: <https://www1.folha.uol.com.br/fsp/brasil/fc28059904.htm>. Acesso em: 10 out. 2024.

TREVISAN, A. P.; VAN BELLEN, H. M. Avaliação de políticas públicas: uma revisão teórica de um campo em construção. **Revista de Administração Pública**, [S.l.], v. 42, n. 3, p. 529-550, jun. 2008. DOI: <http://dx.doi.org/10.1590/s0034-76122008000300005>. Disponível em: <https://www.scielo.br/j/rap/a/bCWckwnwwrvF8Pb9kDtjDgy/abstract/?lang=pt>. Acesso em: 17 out. 2024.

ZAUERUCHA, J. De FHC a Lula: a militarização da agência brasileira de inteligência. **Revista de Sociologia e Política**, [S.l.], v. 16, n. 31, p. 177-195, nov. 2008. DOI: <http://dx.doi.org/10.1590/s0104-44782008000200013>. Disponível em: <https://www.scielo.br/j/rsocp/a/7gtzGZwmZqDDmmF66rQDdgK/>. Acesso em: 17 out. 2024.

PARTE III

Futuro da Atividade de Inteligência no Brasil: Perspectivas





O Papel da Escola de Inteligência da ABIN: uma reflexão

Anna Cruz

Oficial de Inteligência
Diretora da Escola de Inteligência (ESINT)

Marco Cepik

Professor titular da Universidade Federal do Rio Grande do Sul (UFRGS)
Diretor-Adjunto da ABIN

A Atividade de Inteligência é comumente associada a um imaginário de opostos que, na realidade, formam balanços sempre precários que variam muito no tempo e no espaço: é possível conceituá-la e definir seus atributos específicos e, ao mesmo tempo, ela é também essencialmente variável; a atividade equilibra-se entre adotar sigilo para ser efetiva e abraçar a transparência para ser democrática; é um ofício de passado e tradição, transmitido pela experiência profissional, e uma profissão que aspira ter futuro, regrada, orientada pelo acúmulo teórico, apreensível por todos quantos se dediquem a ela.

A Escola de Inteligência (ESINT) reconhece tais tensões e procura contribuir para um equilíbrio dinâmico, cooperativo e produtivo. No ensino, a instituição ocorre para a formação de quadros e a qualificação profissional da Agência Brasileira de Inteligência (ABIN) e do Sistema Brasileiro de Inteligência (SISBIN). Na formulação doutrinária, reflete criticamente sobre a cultura e a natureza da atividade, construindo pontes entre prática e teoria. Na pesquisa, estrutura um legado intelectual neste campo epistêmico interdisciplinar e avança o conhecimento sobre inteligência. Na extensão, abre espaços de diá-

logo e engaja a sociedade na construção da segurança e no reconhecimento do próprio valor da atividade e suas especificidades. Na área de memória, constrói os meios (biblioteca e museu), mas também busca ativamente preservar as experiências e delas extrair aprendizados. São metas aspiracionais, compromissos coletivos, traduzidos em planos e iniciativas cujos resultados são sempre contingentes e necessitam de revisão periódica.

Esse é, portanto, o tema geral deste capítulo. O texto foi organizado em três seções (além desta Introdução e de uma breve Conclusão), as quais têm como subtítulos os pares conceituais “natureza/cultura”, “sigilo/transparência” e “passado/futuro”. Em cada uma delas, além de considerações gerais sobre a Atividade de Inteligência, procuramos recorrer à experiência coletiva concreta de reforma e estabelecimento de diretrizes estratégicas desde 2023 na ESINT para refletirmos criticamente sobre o que está sendo implementado e o que deve ser aperfeiçoado.

Neste sentido, não se trata aqui de fazer uma história institucional da ESINT desde a sua criação. Essa é uma tarefa necessária para superar uma lacuna historiográfica importante no campo dos Estudos de Inteligência no Brasil, mas, infelizmente, está além de nossas possibilidades neste momento. Vale mencionar, entretanto, que a ESINT foi instituída pelo Decreto 3.493/2000, o qual aprovou a estrutura da então recém-criada Agência Brasileira de Inteligência. Desde o seu surgimento, a competência da Escola já era de “formar, aperfeiçoar e desenvolver pessoal para a Atividade de Inteligência, bem como realizar estudos e pesquisas, com vistas a aprimorar sua doutrina” (Brasil, 2000).

Ao longo de mais de duas décadas de existência, a trajetória da ESINT não foi linear, pela configuração das equipes de trabalho, pelas expectativas institucionais, ou mesmo pelas condições orçamentárias e tecnológicas que afetaram seus resultados e perfil de atuação. De

modo geral, entretanto, pode-se dizer que a ESINT se manteve como uma importante referência de capacitação especializada, tanto para os servidores da própria Agência como para os demais órgãos do SISBIN. Desde 2015, a ESINT é reconhecida pelo Ministério da Educação como uma Escola de Governo e faz parte do Sistema de Escolas de Governo da União (SEGU) coordenado pela Escola Nacional de Administração Pública (ENAP).

Em 2023 a competência regimental da ESINT foi atualizada pelo Decreto 11.816/2023 (Brasil, 2023b), o qual manteve algumas atribuições anteriores e acrescentou novas. Manteve-se, por exemplo, a função de formar os candidatos selecionados em concurso público destinado ao provimento de cargos das carreiras de inteligência, bem como capacitar em inteligência e competências transversais complementares os agentes públicos em exercício na ABIN e indicados pelo SISBIN ou órgãos parceiros. A realização de pesquisas e as atividades de extensão, por outro lado, foram acrescentadas ao conjunto de atribuições da ESINT, de acordo com o compromisso assumido em 2023 de transformar a ESINT em Escola Superior de Inteligência de referência no governo brasileiro e no âmbito internacional.

Antes de passarmos ao restante do texto, gostaríamos de agradecer aos diretores que nos antecederam na função, ao Diretor-Geral da ABIN que confiou e apoiou nosso trabalho, bem como a todas e todos os servidores públicos da equipe da ESINT e demais parceiros na empreitada. A responsabilidade pelo conteúdo deste capítulo recai exclusivamente sobre os autores enquanto indivíduos. Este texto não reflete uma posição "oficial" da ABIN, ainda que ambos os autores, na sua experiência como diretores da ESINT, obviamente expressem um viés positivo ao relatarem as evidências e resultados até aqui. Os eventuais leitores poderão formar seu próprio juízo crítico sobre a validade dos argumentos desenvolvidos neste trabalho.

1. Natureza e Cultura

Nesta seção, discutimos a existência de uma natureza da atividade (p.ex.: seu caráter sigiloso e de apoio à decisão) e o fato de ela ser resultado da história política, social, legal e cultural do país e de seus órgãos de inteligência. Argumentamos que a Escola é um local de compreensão crítica desse binômio natureza-cultura e criação de consensos a seu respeito.

A Atividade de Inteligência é caleidoscópica. Há diversas concepções, ideias que mudam ao girar o globo e que tanto respondem geográfica e historicamente a fatores legais, conceituais e institucionais quanto os moldam (Davies, 2019). O exercício da Atividade de Inteligência pode ter ênfase maior ou menor na função informacional, de apoio a decisões, ou na função executora, que promove mudanças na realidade em favor dos interesses do país. Pode submeter-se a diferentes níveis de regulação, controle e transparência. Pode recair preferencialmente no campo interno, externo, cibernético ou, quem sabe, atuar em todos eles. Pode ser ferramenta de assessoramento e apoio à gestão do usuário político ou instrumento de garantia de execução de suas decisões de governo. Pode ter mandato amplo ou restrito, atuação centralizada ou descentralizada. Pode ser militarizada ou de natureza civil.

Na verdade, o próprio nome – “Atividade”- implica algo dinâmico, um processo em curso, um verbo de ação mais do que um objeto estável. Seu caráter “usuário-dependente” adiciona outra complexidade: ainda que se reconheça que o beneficiário final do seu serviço é a sociedade e que o dignitário por ela escolhido (qualquer que seja o mecanismo de escolha) é um intermediário, em alguma medida é inevitável ajustar prioridades conforme a agenda governamental da ocasião.

Warner (2002), embora acedendo que o tópico não é tão complexo nem tão inábeis os que tentam defini-lo, registra que não há uma defi-

nição consensual sobre “inteligência”. À guisa de buscá-la, Warner lista uma série de elementos intrínsecos: dependência de métodos e fontes sigilosas, existência de uma organização oficial com propósitos de Estado, foco em estrangeiros (inclusive com ação de influência por meios não atribuíveis ao Estado), relação com produção e disseminação de informação – sumariza dizendo que “inteligência é segredo, atividade de Estado para entender e influenciar entidades estrangeiras”. Posteriormente, Warner, junto a Stout (2018), afirma que entre profissionais e estudantes do campo há acordo sobre a Atividade de Inteligência ser um auxílio a líderes na obtenção e no uso de informação contra competidores.

No Brasil, o esforço de conceituação se ampara em parâmetros legais: são, assim, balizas a Lei 9883/1999 e os decretos regulamentadores subsequentes, como a Política Nacional de Inteligência e o Decreto 11693/2023. Servem como “soluções oficiais”, portanto, e, nos termos da lei que instituiu o Sistema Brasileiro de Inteligência e criou a ABIN, contra-inteligência é “a atividade que objetiva neutralizar a inteligência adversa” e inteligência é a “atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado”.

Em nosso país, portanto, a atividade tem uma dupla missão: produzir conhecimento para assessorar o processo decisório e proteger conhecimentos sensíveis, uma feição ativa e outra reativa, inteligência e contrainteligência. Não são, contudo, como poderia a conjunção aditiva sugerir, duas coisas separadas; são, antes, uma só: convergem para assessorar a tomada de decisão informada e livre. “Informada” porque os profissionais cuidam de produzir e difundir conhecimentos de inteligência relevantes e oportunos; “livre” porque também tratam de impedir ou mitigar constrangimentos ilegítimos à decisão, sejam eles ameaças como espionagem, sabotagem, extremismos, desinfor-

mação ou mesmo óbices em que não se identifica uma vontade antagônica, como impactos causados por desastres naturais.

Do lado da “cultura” (ou “culturas”, porque múltiplas), pode haver variação nas “funções periféricas” da Atividade de Inteligência (Stout & Warner, 2018), decorrentes da política local e de circunstâncias burocráticas. A “natureza”, de outro lado, sua nota de identidade própria, é de serviço e envolve sempre assessoramento relevante para decisão política – porque deseja representar uma vantagem e conta com permissões específicas para a garantia dessa vantagem.

Começando pelo fim: permissões específicas. O segredo, enquanto regulamentação pública de certos fluxos informacionais, prevista em lei, é uma dessas permissões. A regra de transparência e publicidade do serviço público é mitigada nestes casos para que se ponham a salvo os produtos da atividade, em nome da segurança do Estado e da sociedade, e também métodos, técnicas e profissionais envolvidos na Atividade de Inteligência, por sua própria segurança. O alcance e o escopo das técnicas podem ser muito variados nos diferentes serviços de inteligência, mas a concessão do sigilo é uma constante. No Brasil, a permissão também decorre da Lei 9883, que diz que à Agência Brasileira de Inteligência compete “planejar e executar ações, inclusive sigilosas, relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o Presidente da República” e, mais adiante, afirma que “os atos da ABIN, cuja publicidade possa comprometer o êxito de suas atividades sigilosas, deverão ser publicados em extrato”, incluídos os referentes às atribuições, à atuação e às especificações dos respectivos cargos, e à movimentação dos seus titulares (Brasil, 1999). A Lei 12527, de 2011, que regulamenta o acesso a informações públicas, trata também das razões para a eventual e excepcional classificação de informações cuja divulgação ampla possa colocar em risco a segurança de autoridades, instituições ou atividades de inteligência. Note-se que a legislação é clara em afirmar que é dever do Estado proteger as informações e, ao fazê-lo,

seus agentes (autoridades e burocracias) devem conduzir-se com comedimento, espírito público e sujeição aos controles externos democraticamente definidos na forma da lei.

Uma outra permissão, com contornos bastante variados a depender da latitude e da longitude, é a de intervir no mundo, mudar realidades, a função executora da atividade. Ainda que, ao agir, a atividade faça a implementação de uma decisão, não perdeu seu caráter de assessoramento para a tomada de decisão livre de constrangimentos: não age por capricho, age em busca da melhor condição para consecução e salvaguarda dos objetivos fundamentais do país.

No perímetro democrático em que a Atividade de Inteligência brasileira deve atuar, as "permissões específicas" não são ilimitadas e não podem ser abusadas sob o risco de perda de legitimidade e de eficácia do serviço. No Brasil, este "agir no mundo" é possível apenas para obter informações ou para contrapor-se a ações de inteligência contrária – e não para disfunções como interferências, detenções, perseguições ou usos políticos. O sigilo deve ser justificado e submetido a procedimentos administrativos claros. Também por ditame legal, a atividade é exercida sob a supervisão e o controle interno da Câmara de Relações Exteriores e Defesa Nacional (Creden) do Conselho de Governo, podendo ser auditada pela Controladoria Geral da União (CGU); o controle externo é realizado pelo Poder Legislativo, por meio da Comissão Mista de Controle das Atividades de Inteligência (CCAI), comissão permanente do Congresso Nacional, e pelo Tribunal de Contas da União (TCU); sua supervisão é feita, com diferentes mandatos, escopos e capacidade real de intervenção, pelo Poder Judiciário, pelo Conselho Nacional de Justiça, pelo Ministério Público e pela imprensa (Cepik, 2021).

Um outro elemento distintivo é o assessoramento de inteligência precisar ser relevante para uma decisão. Esse atributo deve-se tanto ao fato de ter de ser acionável, aplicável, não frívolo, não meramente "teó-

rico”, não simplesmente explicativo de fatos passados sobre os quais não há mais nada a fazer, e ainda porque a inteligência precisa trazer um elemento não conhecido (protegido por seu detentor ou em princípio indisponível) ou uma análise baseada em um método próprio que revela raciocínios inéditos. Há muitas fontes de informação no mundo, mas a inteligência se ocupa de questões complexas, em contextos de disputa, e lida com adversários cujas motivações frequentemente não são declaradas e que usam, também eles, a Atividade de Inteligência para informar e proteger o decisor concorrente.

De volta à asserção de que é antes um serviço e não um produto. Kent (1967) classicamente considerou-a como conhecimento (produto), atividade (processo de construção e difusão de conhecimento) e organização. Trata-la como processo é mais que compreender que deriva de um conjunto de procedimentos de pesquisa e que busca continuada e sistematicamente a verdade; é também consentir que, além de um produto final a ser entregue (relatório de inteligência ou, posto em abstrato, conhecimento de inteligência), padronizado, há um serviço adaptado à demanda, flexível, contínuo e intangível. No Brasil, a Atividade de Inteligência nacional ganha outros adjetivos: é serviço público, especializado, profissional.

Além das escolhas legais que conformam a Atividade de Inteligência no Brasil e a atuação da ABIN, há orientações doutrinárias que ressignificam a cultura e estabilizam entendimentos conceituais. Em dezembro de 2023, pela primeira vez em sua história, a ABIN divulgou ao público sua Doutrina da Atividade de Inteligência, apresentando os fundamentos da atividade, os ramos (contrainteligência e inteligência) e os elementos (análise e operações) que a compõem (ABIN, 2023). A ESINT, por meio de uma matriz disciplinar estruturada, do desenvolvimento de modelos, do acompanhamento sistemático do referencial teórico da área, da estruturação de valores e conceitos doutrinários, une e dá sentido à natureza e cultura da Atividade de Inteligência brasileira.

Considerando, aliás, o substrato histórico da cultura política brasileira e a trajetória dos serviços de inteligência em regimes políticos anteriores ao da Constituição de 1988, Cepik (2021) defende que novas tentações autoritárias só serão evitadas se a sociedade tiver segurança sobre alguns consensos acerca do exercício da atividade sob regras democráticas e orientado a objetivos sustentáveis e equitativos. Daí que essas linhas gerais sobre a “natureza construída” do produto cultural “Atividade de Inteligência” e a investida de traçá-las são úteis para estabelecer pressupostos comuns na análise do seu papel no Brasil atual e seus potenciais futuros – e saber o que somos, o que fazemos, por que fazemos e como fazemos é conjugar o entendimento de natureza e cultura, compreender o que há de subjacente e profundo e o que foi cultivado e legado – e nisto há uma tarefa fundamental da Escola de Inteligência.

2. Sigilo e Transparência

A convivência de um caráter particular, local, atado à cultura e à prática, e um outro geral, estável, que permite a teorização acerca de uma natureza da atividade, como debatido anteriormente, é apenas uma das dualidades (não necessariamente antagônicas) desse ofício. Chiru (2019) sustenta que tão importante quanto a tradicional cultura de sigilo é o gerenciamento da mais recentemente percebida necessidade de uma cultura de abertura, transparência e responsabilidade públicas.

Nesta seção, debatemos o par sigilo x transparência e defendemos que Escolas e centros de treinamento auxiliam na ambidestria requerida dos serviços de inteligência para esse equilíbrio em favor da sociedade e das instituições. Na seção anterior já se disse que o segredo é uma das “permissões específicas” e bem delimitadas da Atividade de Inteligência, componente de “sua natureza”, e que no Brasil o sigilo é previsto em norma (Lei 9883/1999 e Lei 12527/2011, notadamente artigos 22 e 23). Cepik (2001) já defendia, dez anos antes da adoção

da Lei de Acesso a Informação (LAI), que regimes democráticos devem ter desenhos institucionais baseados na transparência, de forma que eventuais segredos governamentais (retenções públicas de fluxos informacionais por meio de procedimentos de classificação, controle de acesso e punição em hipótese de revelação) precisam ser sempre justificados – seja por evitar danos à segurança nacional, seja para evitar a frustração de objetivos governamentais. O sigilo nunca deveria ser adotado como norma ou considerado aprioristicamente, sem referência a necessidades concretas e delimitadas.

Com referência a países com histórico autoritário e hoje considerados democracias liberais, como Espanha, Itália e Romênia, Chiru (2019) ilustra a adoção de relevantes medidas de abertura ao diálogo com a sociedade: o contato com outras instituições da administração pública, o intercâmbio com universidades e centros de pesquisa, a publicação de periódicos e livros, a promoção de eventos de ensino como palestras, da pesquisa como estímulo a linhas de estudo universitário e prêmios, ou da atividade mais sistemática de extensão, como desafios e campanhas direcionadas inclusive para o público jovem. Os centros de formação dos serviços teriam, ou deveriam tentar ter, condições especiais para unir, incentivar e organizar uma nova forma de relacionamento com a sociedade.

Cepik (2023, p. 323) considera que um desafio para a institucionalização dos serviços de inteligência é, além da estabilidade organizacional, a percepção social de que são valiosos, algo que depende da “capacidade do público ver e julgar, por si mesmo, os atos dos governantes na área de inteligência”. Lowenthal (2008) assume o fracasso da inteligência norte-americana não pelos eventos de 11 de setembro ou da alegada existência de armas de destruição em massa no Iraque ou no Irã:

We have failed because we have not explained ourselves adequately and comprehensibly to the public – describing our role, the

limits within which we work and our view of what can be reasonably expected from us. We have failed because we have allowed ourselves to be caricatured, vilified and misrepresented by people who do not know us, do not like us and do not understand us – or simply see us as convenient fall guys.

Também no Brasil, mesmo sob o regime da Constituição Federal de 1988, a Atividade de Inteligência tem sido um serviço público pouco debatido, pouco conhecido e, por vezes, visto por importantes atores políticos no Estado e na sociedade como um órgão vestigial e dispensável. É recente e ainda em andamento o trabalho de desmistificação e de superação dos estigmas do passado por meio da informação e do diálogos sistemáticos com outras burocracias, com os governantes, com os parlamentares e com a sociedade. Ainda que a ABIN tenha, desde sua criação, a missão imprescindível de contribuir para a segurança da democracia, da sociedade e do Estado, a baixa disponibilidade de documentos ostensivos e de comunicação dialógica sobre propósitos e realizações faz com que apenas em momentos de crises ou falhas institucionais haja alguma atenção sobre o trabalho da Agência e do SISBIN. E depois de cada crise a ausência prévia de conhecimento especializado sobre a atividade limitou historicamente o alcance de reformas e iniciativas para melhorar o desempenho e a valoração pública dos órgãos de inteligência. É importante reconhecer que a gravidade dos eventos de 8 de janeiro de 2023 criou a necessidade e a possibilidade para que muitos dos temas e preocupações relativas a efetividade, eficácia, eficiência e legitimidade da Atividade de Inteligência fossem debatidos de forma inédita e com consequências que reputamos como positivas.

Neste sentido, a ESINT tem sido uma plataforma para esse diálogo, além de ser um centro de treinamento profissional. Em 2024 foi apresentada sua primeira “carta de serviços”. Embora a ESINT tenha como público-alvo prioritário os próprios servidores da Agência Brasileira de Inteligência, os agentes públicos representantes de órgãos membros

do SISBIN e, por cooperação internacional, indivíduos indicados como alunos por serviços congêneres estrangeiros, há serviços diretamente acessíveis ao cidadão brasileiro. Na ESINT, o museu e a biblioteca, frações que lhe compõem, são, por exemplo, abertos ao público mediante agendamento e contribuem para a compreensão da sociedade sobre a Atividade de Inteligência por meio da observação direta dos acervos e expõem ao seu estudo e ao seu escrutínio nuances de uma atividade tradicionalmente considerada inacessível e perigosa.

Também em 2024, a ESINT liderou um esforço para a realização de um amplo tratamento técnico de documentos arquivísticos remanescentes de serviços e escolas de inteligência antecessores à ABIN, anteriores a dezembro de 1999, portanto. Com compromisso de transparência e plena adequação da Administração Pública aos princípios da Lei de Acesso à Informação, o projeto teve como meta encaminhar para o Arquivo Nacional manuais, relatórios técnicos e materiais didáticos cuja guarda eventualmente ainda estivesse com a ABIN, franqueando, assim, seu acesso ao público e garantindo um destino social a esses arquivos.

Em relação a trocas com as universidades e centros de pesquisa, um dos interlocutores mais frequentes dos serviços de inteligência em diferentes contextos, Chiru (2019) exemplifica resultados práticos da aproximação entre as agências de inteligência e acadêmicos, como coprodução de análises, colaboração em grupos de trabalho, estabelecimento de métodos e produtos conjuntos, comunicação além da comunidade de inteligência/segurança. Esses intercâmbios são promovidos, no caso da ESINT, por meio de um Núcleo de Pesquisa em Inteligência (NUPI) e de um programa de extensão, iniciativas que reúnem profissionais de inteligência e uma comunidade epistêmica interessada mais ampla. A pesquisa e a extensão são reforçadas pela publicação, ininterrupta desde 2005, da Revista Brasileira de Inteligência (RBI).

Tais iniciativas têm buscado cultivar relacionamentos qualificados com especialistas, participar do debate científico interdisciplinar, subsidiar o aprimoramento contínuo da doutrina e do ensino, contribuir com pesquisa aplicada para o aprimoramento da produção de inteligência e embasar o aprofundamento da reflexão sobre a Atividade de Inteligência. Essa atuação, por diretriz institucional, é pautada pela interação consciente, responsável e respeitosa, pela construção de relações sustentáveis e de confiança com pesquisadores e instituições de pesquisa, pela promoção da pluralidade de pensamento e da diversidade e pela transformação gradual das concepções e práticas concernentes às áreas de inteligência e segurança.

Desde 2023, a ESINT promove regularmente ciclos de debates com especialistas e autoridades sobre temas de relevância estratégica para o Brasil. Alguns desses eventos são de participação restrita a servidores da Agência, outros contam com a audiência de agentes de órgãos pertencentes ao SISBIN e há ainda os que admitem público amplo, com perfil acadêmico e governamental. Os assuntos tratados incluem desde desafios globais para os Estados e as sociedades contemporâneas, tais como soberania digital, mudança climática e ameaças às democracias, até questões atuais de interesse mais imediato para o Brasil, como integração regional e impacto da desinformação no período eleitoral.

A Escola é, portanto, um lugar de pesquisa e desenvolvimento doutrinário, o que também propicia ligação com a sociedade, já que a Doutrina, ostensiva, guia entendimentos, valores, motivações e procedimentos – a partir de sua divulgação, também eles públicos. E parte desta pesquisa resulta em publicações, seja na forma de artigos para a RBI, seja por meio de documentos ostensivos de caráter institucional, distintos dos Relatórios de Inteligência (RELINTs), normalmente classificados.

Os relatórios de inteligência são, em regra, classificados por causa do risco de dano à segurança e perda de vantagem decisória que sua

divulgação traria. Mas, vale reiterar, a restrição de publicidade deve se dar sob critérios legais e institucionais estáveis, afinal “os segredos governamentais são compatíveis com o princípio da transparência dos atos governamentais somente quando a justificativa de sua necessidade pode ser feita, ela própria, em público” (Cepik, 2023, p. 248). Para além de ser necessária a justificativa fundamentada do ponto de vista técnico e legal, das proteções por vezes necessárias, é importante que a Escola impulse também iniciativas de produção de relatórios ostensivos mais amplos, que permitam à sociedade conhecer os temas de acompanhamento e julgar por si mesma os métodos de análise, criando entendimentos públicos compartilhados. Como a sociedade não é “passiva” na construção dos serviços de inteligência, à medida em tais serviços são também produtos culturais de suas próprias realidades sociais e nacionais, documentos que sintetizam entendimentos das organizações sobre as principais ameaças, riscos e vulnerabilidades que recaem sobre a sociedade, relativos a horizontes temporais variados, ajudam a melhorar a deliberação coletiva sobre as medidas de proteção cabíveis. Relatórios anuais como o “Annual Threat Assessment” do Office of The Director of National Intelligence dos Estados Unidos da América, o “New Zealand’s Security Threat Environment”, ou o “International Security and Estonia”, são exemplos de uma interação mais transparente entre os serviços de inteligência e as suas respectivas sociedades que contribuem para a legitimidade dos serviços e para a segurança das pessoas e instituições.

É com este propósito que, a partir de 2024, a Escola tem investido na diversificação de produtos: além da RBI e de um relatório ostensivo sobre os desafios de segurança para o Brasil no sistema internacional, passaram a ser editadas publicações institucionais para divulgação externa de trabalhos de destaque da Agência e comunicação de seus projetos. Futuramente, a eventual consolidação de um ou mais selos editoriais, com linhas planejadas a congregarem regularmente esses conteúdos, tende a auxiliar a construção da imagem pública da Agência e sua reputação.

A comunicação interna também é um fator de transparência. Em 2023 a Escola intensificou o empenho em disciplinar seu próprio funcionamento de modo mais claro para os próprios servidores: somando-se aos já existentes regimento escolar e divulgação anual do planejamento de ações de capacitação, a ESINT investiu na construção e na divulgação de uma matriz curricular estável, com mais de uma centena de ações de ensino, na divulgação de diretrizes e prioridades para o ano subsequente e o calendário do ano corrente de ações de ensino, pesquisa e extensão, na edição de uma série de políticas, com força normativa, que informa, por exemplo, critérios para distribuição de vagas (incluindo, aqui, uma política de cotas), para acionamento de colaboradores ou para processos de avaliação.

"Plataforma" é um termo que designa um "espaço" e também um "programa". A ESINT pretende ser plataforma de abertura, espaço de debates que tem o ensino, a pesquisa e a extensão como programa, meio de preparar a Atividade de Inteligência para o assessoramento estratégico no contexto de transições globais, aperfeiçoar capacidades técnicas dos agentes públicos que exercem esse ofício, desenvolver arcabouço doutrinário que ampare sua atuação democrática e expandir o relacionamento com a sociedade. Ainda assim, o sigilo próprio da Atividade de Inteligência também alcança a ESINT. Sua matriz curricular, seus planos de ensino, seus cursos, oficinas e manuais são, em regra, sigilosos, porque revelam capacidades, técnicas e possivelmente deficiências a serem enfrentadas com formação. Equilibrar sigilo e transparência é um desafio permanente e uma especificidade importante de uma instituição de educação governamental nesta área de segurança.

3. Passado e Futuro

A Atividade de Inteligência está em evolução, de forma que olhar para o passado é um exercício de compreensão (e, frequentemente, descoberta) histórica e de obtenção de algumas percepções de futuro, mesmo que nas últimas décadas tenham mudado profundamente as

ameaças, paradigmas e métodos (Agrell, 2012). Como destacamos anteriormente, a natureza da Atividade de Inteligência e sua institucionalização no Brasil e no mundo têm história. Como indica a Doutrina publicada pela ABIN em 2023, vivemos em mundo de Estados e ao longo dos últimos dois séculos os serviços de inteligência se tornaram, inclusive por causa da evolução tecnológica e da recorrência de conflitos, um requisito importante para que os Estados possam prover políticas públicas de segurança e o desenvolvimento para as populações governadas. As organizações de inteligência, surgidas antes da Era Digital, vêm se adaptando e possuem diferentes missões e capacidades em diferentes países, mas em todos eles formam parte, juntamente com as burocracias especializadas em relações exteriores, defesa nacional e policiamento, do aparelho institucional mínimo para que um Estado possa existir soberanamente no sistema internacional. Compreender o passado e ajudar a construir o futuro é uma atribuição essencial da ESINT.

É difícil prever como será a Atividade de Inteligência do futuro, embora haja alguns indicativos: necessidade de aperfeiçoamento em análises sobre riscos e ameaças cinéticas e virtuais, métodos crescentemente verificáveis e críveis; produções cooperativas (não apenas dentro dos órgãos de inteligência, mas entre sistemas e países); diversificação de demandas, superando as capacidades organizacionais e exigindo consultorias externas; revisão de fontes e métodos clássicos ou exclusivos e substituição ou complementação por outros (Agrell, 2012). Tudo isso em cenário de rápida mudança tecnológica, disponibilidade pública de grande quantidade de informação, ameaças transnacionais, diferente tolerância social acerca de quais tipos de coleta e operações de inteligência podem ser executados em seu nome (Lowenthal, 2018). Improvável a superação desses desafios sem o envolvimento da Escola.

É na ESINT ou sob seu patrocínio e curadoria que se dá o levantamento das necessidades de desenvolvimento do corpo profissional

e, em seguida, seu treinamento e sua formação, seja para o melhor uso da tecnologia, para o tratamento correto do volume crescente de dados e o manejo das máquinas, seja para o aprimoramento analítico inerentemente humano, no exercício da lógica, na identificação de vieses, na aplicação de técnicas analíticas colaborativas e mesmo na elaboração de perguntas relevantes.

Já que a Atividade de Inteligência apoia decisões, assessora planejamento, elaboração, execução e monitoramento de políticas públicas, é atribuição inescapável da atividade tentar antecipar o futuro. A contrainteligência, buscando prevenir ação adversa e avaliar riscos, e mesmo alertas ou comunicados sucintos, que tratam tão somente de fatos passados ou presentes e não trazem projeções, se buscam subsidiar uma decisão e já que toda decisão racional avalia consequências futuras, são todos antecipatórios (Cruz, 2022). As ações da Escola também são orientadas para a frente, porque não se capacita para a obsolescência; são valores da ESINT, além do foco na aprendizagem, governança participativa, inclusão de pluralidades, valorização docente e honestidade intelectual, a inovação e a curiosidade, exprimindo a busca de novos conhecimentos e novas formas de atender aos usuários da Escola.

Assim, além de capacitar, a ESINT é ambiente que favorece a inovação, à medida que permite e encoraja conjecturas, assunção de risco, prototipagem, associações e permeabilidade ao meio externo à organização de inteligência:

To become more innovative, intelligence organizations need to pay more attention to the logics that foster innovation. In this line of reasoning, they should have a more horizontal organizational structure, focus on their outputs and outcomes at the expense of following the procedures, have the freedom to experiment and emphasize relationships with external actors (RIETJENS et. al, 2024, p. 8)

Em 2024, a ESINT vem participando de iniciativas institucionais para que os servidores da Agência tenham espaços de debate e formulação sobre o futuro da atividade, da organização e dos seus perfis profissionais, a partir de encontros e questões motivadoras de especulações a respeito de mudanças de médio prazo sobre missão, produtos, usuários e competências requeridas para os novos cenários.

Também em 2024, foi concebido na ESINT o primeiro relatório ostensivo de caráter prospectivo da Agência. Discutindo as tendências para o ano de 2025, o documento sintetiza pontos de atenção para Atividade de Inteligência e consolida entendimentos acerca de transições globais em curso, da competição internacional e da posição estratégica do Brasil na América do Sul que contextualizam desafios do futuro próximo. Esse tipo de documento sinaliza também para os demais órgãos do SISBIN como a Agência atualiza as diretrizes mais amplas da Política Nacional de Inteligência (PNI). Anualmente, a Agência define uma agenda de produção de conhecimentos (API), derivando a partir de quatro eixos (inteligência externa, interna, contrainteligência e inteligência cibernética) um conjunto bastante específico de linhas de análise e problemas de inteligência para organizar o trabalho da Agência em prol dos processos decisórios das autoridades assessoradas. Por medida de segurança, tal agenda de produção é reservada e, por isso, um documento mais amplo, complementar, de acesso público, é importante para apontar o entendimento da ABIN sobre o futuro dos problemas a serem enfrentados.

Ainda na dimensão de construção do futuro, desde 2020 existe na ABIN um laboratório interdisciplinar e interdepartamental para novas ideias, tecnologias e práticas profissionais, o LABINova. A partir de 2023 ele foi incorporado como um projeto da ESINT, documentado nas Diretrizes daquele ano como tal, também na perspectiva de que o espaço escolar tem vocação para esse tipo de experimentação e que a equipe da Escola poderia inclusive se valer do laboratório para testar metodologias e abordagens em ações mais simples antes de trans-

formá-las em ações de ensino formais, registradas na Matriz Curricular na ESINT, sobre a qual falaremos um pouco mais na Conclusão deste texto.

A Escola permite ainda acúmulo e reflexão sobre lições aprendidas por meio de duas instituições típicas e muito relevantes, o Museu e a Biblioteca, partes complementares com vocação para conservação de memória e coesão internas; a pesquisa levanta e gera a informação e o fundamento desses acervos, materiais e imateriais; o ensino difunde os conhecimentos oriundos da pesquisa aplicada e da prática profissional.

A história não é mera coleção de objetos e registro de fatos e sim um sistema de significados em constante recriação, cujos sentidos são condicionados pelo olhar presente e pelos anseios em relação ao futuro. Os sentidos do passado e as formas de compreendê-lo e contá-lo são objeto de projeto específico no âmbito da memória institucional, que visa a recriar a narrativa museológica do Museu da Inteligência à luz dos desafios atuais da ABIN e do Brasil. A coleta de relatos de veteranos e pioneiros em suas áreas ou de profissionais ainda na ativa que viveram momentos críticos da Atividade de Inteligência brasileira (como, por exemplo, a atuação da ABIN durante a pandemia ou no ciclo de grandes eventos) é também mais que registro de “casos”, pois configura oportunidade para autoanálise e aperfeiçoamento.

Assim, o ensino, a pesquisa e o relacionamento com a sociedade fomentados na Escola são o tempo de oportunidade e preparação em que se encontram as lições do passado e o planejamento para o futuro. Se a maior habilidade do profissional de inteligência é produzir conhecimento, a sua identidade é de aprendiz; a natureza do profissional de inteligência é a cultura do aprendizado. Nesses encontros (natureza, cultura, profissional, aprendiz, habilidade, conhecimento, sigilo, transparência, passado e futuro) em que duplos aparentemente

opostos se reforçam mutuamente, a ESINT tem sido um ativo importante para a construção da Atividade de Inteligência brasileira.

Conclusão

Neste trabalho, destacamos o papel da Escola de Inteligência da ABIN na reconfiguração da Atividade de Inteligência no âmbito do governo brasileiro, especialmente no período mais recente, marcado por severos questionamentos e debates sobre eventuais desvios de finalidade e acusações de falhas por parte do SISBIN na antecipação e compreensão dos eventos que resultaram nos ataques às instituições democráticas em 8 de janeiro de 2023 em Brasília.

Como ficou evidente nos trabalhos e relatórios das Comissões Parlamentares de Inquérito (CPIs) da Covid-19 e do 8 de janeiro, a ABIN como instituição manteve uma atuação relevante e correta em contextos de grande polarização política e social, fiel aos compromissos constitucionais e legais que definiram sua missão desde a criação em 1999. As investigações sobre desvios de finalidade por parte de autoridades e servidores públicos prosseguem e precisam ser concluídas para que cada indivíduo responda na forma da lei. De todo modo, o questionamento, as investigações e as demandas por maior transparência e novas prioridades de atuação ensejaram a decisão da Presidência da República de revisar os processos e a governança da área de inteligência federal, decisão materializada na publicação de três decretos que marcaram uma importante inflexão na trajetória institucional do sistema e da agência. Em março de 2023, a ABIN foi transferida para o âmbito da Casa Civil da Presidência da República. Em setembro do mesmo ano, um novo decreto reorganizou a governança e o funcionamento do SISBIN. Finalmente, em dezembro de 2023 foi publicado um decreto reorganizando a própria ABIN e seu funcionamento. Juntamente com a discussão sobre a necessária modernização da Política Nacional de Inteligência (PNI), cujo decreto é de 2016, essas três iniciativas do Poder Executivo, em diálogo com

o Congresso Nacional e o Poder Judiciário, atualizam os parâmetros para a Atividade de Inteligência na fase atual de desenvolvimento da Era Digital no Brasil.

Como parte integrante desse processo, em 2023 a Escola de Inteligência da ABIN iniciou uma reforma significativa visando a ser capaz de desempenhar uma dupla missão: ser um centro de treinamento profissional e uma Escola superior, o que permitirá que ela capacite e forme, portanto, no quê e como fazer, mas que seja também produtora e difusora de cultura, que reflita criticamente sobre por que fazer.

Na área de ensino, uma matriz curricular foi então estruturada em três eixos: "inteligência" – relacionado ao ensino de ramos, elementos e funções da atividade; "temático" – acerca de temas cuja compreensão é necessária para o acompanhamento de fatos, eventos, situações e fenômenos em que a atividade atua, nas áreas de política, economia, segurança, tecnologia, sociedade e cultura; "transversal" – sobre competências complementares às próprias da Atividade de Inteligência, úteis ao trabalho dos profissionais, como métodos, técnicas e ferramentas de gestão, docência e competências linguísticas. Sustentada em um modelo andragógico de aprendizagem, a matriz disciplinar da ESINT organiza diferentes complexidades e modalidades de ações de ensino, cursos livres, oficinas e cursos de pós-graduação *Lato Sensu* para formar de maneira contínua profissionais em competências e habilidades diversas, por exemplo: planejamento e gerenciamento da Atividade de Inteligência na democracia, cooperação interagências, ciência de dados, metodologia da produção do conhecimento de inteligência, técnicas operacionais, ética e muitas outras. Do ponto de vista material, tem sido decisiva também a implantação da ESINT Virtual e um conjunto de políticas e normas atualizadas para uma atuação ainda mais profissional e abrangente.

Na área de pesquisa, a ESINT estruturou um Núcleo de Pesquisa e, juntamente com o Centro de Pesquisa em Segurança de Comunica-

ções (CEPESC) da Agência, vem avançando no reconhecimento da ABIN como um Instituto de Ciência e Tecnologia (ICT) por parte do Ministério e das agências de fomento à pesquisa, desenvolvimento e inovação. O foco da ESINT é no desenvolvimento de pesquisas aplicadas e que tenham sinergia com o desenvolvimento doutrinário, o apoio às áreas de produção e a construção de soluções para desafios da atividade. Ligada à área de pesquisa, estruturou-se a atividade de extensão, buscando contribuir para a promoção de transparência, o reconhecimento social da missão da Agência e abrindo canais para o enriquecimento da atividade por meio do diálogo público. Da mesma forma, como já mencionamos anteriormente, o desenvolvimento de um programa de memória institucional é parte do compromisso da Escola com a construção do futuro da atividade e da agência.

As ações de ensino, pesquisa, extensão, doutrina e memória desenvolvidas na ESINT têm o foco na formação de recursos humanos e na ampliação de conhecimentos estratégicos em inteligência. As pesquisas, estudos e reflexões teórico-doutrinárias sobre inteligência e temas afins retroalimentam as atividades de ensino, levando à incorporação de novas práticas, tecnologias, abordagens metodológicas e alterações doutrinárias (Martins, 2015, p.16).

Persistem muitos desafios, de adaptação às necessidades contemporâneas, de aperfeiçoamento institucional, de construção dos meios materiais e simbólicos (orçamentos e pessoas, mas também visões de futuro e compromissos). Enfim, os desafios que são próprios de um país como o Brasil, nas suas comunalidades com o Sul Global e nos seus dilemas estratégicos singulares. Mas tais desafios não devem nos desanimar. Em um estudo recente analisando o grau de maturidade dos programas de formação superior em inteligência nas universidades e escolas profissionais dos Estados Unidos, Ramsey e Macpherson (2024) concluíram que, mesmo em um contexto com grandes contingentes de profissionais (demanda) e muitos programas bastante robustos de formação (oferta), as rápidas mudanças

no ambiente internacional (novas ameaças) e o desenvolvimento tecnológico acelerado (Inteligência Artificial) demandam combinar uma formação profissional baseada em ciências, tecnologia e filosofia com níveis de rigor, coerência e criatividade muito superiores ao que anos atrás parecia ser uma espécie de remédio universal para a inteligência de Estado: dados e estatística. Uma abordagem ampla, profunda e realista sobre a educação em inteligência é o que a ESINT está buscando construir nos anos vindouros.

Referências

ABIN. **Portaria n. 1205, de 27 de novembro de 2023**. Aprova a Doutrina da Atividade de Inteligência. Disponível em <https://www.gov.br/abin/pt-br/centrais-de-conteudo/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023>. Acesso em: 3 set. 2024.

AGRELL, W. The Next 100 Years? Reflections on the Future of Intelligence. **Intelligence and National Security**, v. 27, n. 1, p. 118–132, 2012.

BRASIL. **Lei n. 9.883, de 7 de dezembro de 1999**. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9883.htm. Acesso em: 16 jun. 2024.

_____. **Decreto n. 11.693, de 6 de setembro de 2023**. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência. Brasília, DF: Presidência da República, [2023a]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11693.htm. Acesso em: 30 ago. 2024.

_____. **Decreto n. 11.816, de 6 de dezembro de 2023**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão, das Funções de Confiança e das Gratificações da Agência Brasileira de Inteligência, e remaneja e transforma cargos em comissão, funções de confiança e gratificações. Brasília, DF: Presidência da República, [2023b].

Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11816.htm. Acesso em: 30 ago. 2024.

_____. **Decreto n. 3.493, de 29 de maio de 2000.** Aprova a Estrutura do Gabinete de Segurança Institucional da Presidência da República, na parte referente à organização da Agência Brasileira de Inteligência – ABIN, o seu Quadro Resumo de Custos dos Cargos em Comissão e das Funções Gratificadas, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto/D3493.htm. Acesso em: 30 ago. 2024.

_____. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 6 out. 2024.

CEPIK, M. Segredos Públicos: um dilema para a democracia. **Revista Insight Inteligência**. n. 14, pp. 148-155, 2001.

_____. Intelligence and Security Services in Brazil Reappraising Institutional Flaws and Political Dynamics. **The International Journal of Intelligence, Security, and Public Affairs**, v. 23, n. 1, p. 81-102, 2021.

_____. Brazil. In: MATEI, Florina; HALLADAY, Carolyn; ESTÉVEZ, Eduardo (orgs.). **The handbook of Latin American and Caribbean intelligence cultures**. Maryland: Rowman & Littlefield Publishers, 2022. p. 91-109.

_____. **Espionagem e democracia: agilidade e transparência como dilemas na institucionalização de serviços de inteligência**. 2ª ed. Belo Horizonte: Parabellum, 2023.

CHIRU, I. National intelligence cultures. In: MATEI, Florina Cristiana; HALLADAY, Carolyn (orgs.). **The conduct of intelligence in democracies: processes, practices, cultures**. Maryland: Rowman & Littlefield Publishers, 2019. p. 213-226.

CRUZ, A. O que será: notas sobre a função informacional prospectiva da

Atividade de Inteligência. **Revista Brasileira de Inteligência**, n. 17, março de 2023. Disponível em: <https://doi.org/10.58960/rbi.2022.17.211>. Acesso em: 16 jun. 2024.

DAVIES, P. Ideas of intelligence: divergent national concepts and institutions. In: ANDREW, C; ALDRICH, R J.; WARK, W K. (orgs.). **Secret intelligence**. 2. ed. Nova Iorque: Routledge, 2019. p. 13-20.

KENT, S. **Informações Estratégicas**. Rio de Janeiro: Editora Biblioteca do Exército, 1967.

KING, A. From Sage on the Stage to Guide on the Side. **College Teaching**, v. 41, n. 1, pp. 30-35, 1993.

LOWENTHAL, M. **The Future of Intelligence**. Cambridge: Polity Press, 2017.

_____. The real intelligence failure? Spineless spies. **Washington Post**, 25 maio 2008. Disponível em: <http://www.washingtonpost.com/wp-dyn/content/article/2008/05/22/AR2008052202961.html>. Acesso em: 15 jun. 2024.

MARTINS, É F de S. O papel da escola de inteligência para o avanço dos estudos em inteligência no Brasil. **Revista Brasileira de Inteligência**, n. 10, dez. 2015. p. 9-19. Disponível em: <https://doi.org/10.58960/rbi.2015.10.122>. Acesso em: 16 jun. 2024.

NZSIS. New Zealand Security Intelligence Service. New Zealand's Security Threat Environment: An assessment by the New Zealand Security Intelligence Service. Wellington: NZSIS, 2024. 47 p. Disponível em: <https://www.nzsis.govt.nz/assets/NZSIS-Documents/New-Zealands-Security-Threat-Environment-2024.pdf>. Acesso em 10 out. 2024.

ODNI. Office of the Director of National Intelligence. **Annual Threat Assessment of the U.S. Intelligence Community**. Washington: ODNI, 2024. 40 p. Disponível em: <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>. Acesso em: 10 out. 2024.

RAMSAY, J; MACPHERSON, A. The integration of statistical learning in intelligence education: is the academy equipping tomorrow's intelligence professionals to analyze data-centric threats? **Journal of Policing, Intelligence and Counter Terrorism**, v. 19, n. 1, p. 3-21, 2024.

RIETJENS, S.; SINTERNIKLAAS, R.; COULTHART, S. How intelligence organizations innovate. **Intelligence and National Security**, p. 1-20, 2024. Disponível em: <https://doi.org/10.1080/02684527.2024.2401638>. Acesso em: 10 de out 2024.

STOUT, M; WARNER, M. Intelligence is as intelligence does. **Intelligence and National Security**, v. 33, n. 4, p. 517-526, 2018.

VLA – Estonian Foreign Intelligence Service[Välisluureamet]. International Security and Estonia 2024. Talinn: VLA, 2024. 85 p. Disponível em: <https://raport.valisluureamet.ee/2024/en/>. Acesso em: 10 out 2024.

WARNER, M. Wanted: a definition of intelligence. **Studies in Intelligence**, v. 46, n. 3, pp. 15-22, 2002.



A renovação da agenda de inteligência no contexto contemporâneo

Ana Ribeiro

Oficial de Inteligência
Diretora do Departamento de Inteligência Externa

Esaú Feitosa

Oficial de Inteligência
Diretor do Departamento de Inteligência Interna

A busca pela redução de incertezas em relação a eventos, processos, pessoas ou objetos está na essência das relações entre grupos e estruturas sociais humanas. De certa forma, a origem da Inteligência reside na tentativa de resposta a esse anseio por parte de um tipo de estrutura política e social complexa, os Estados.

Embora o objetivo de redução de risco e de obtenção de vantagens comparativas em interações políticas ou militares tenha seus antecedentes na própria formação das primeiras estruturas de governo, a Inteligência, como atividade e instituição autônoma e permanente, surgiu somente a partir do século XIX, no contexto e em resposta às demandas decorrentes dos conflitos entre Estados-Nação (Jackson, 2005, p. 18). Até então, as atividades denominadas de “espionagem”, como a coleta de informações indisponíveis e as ações de quebra de códigos de comunicações, eram conduzidas, sem metodologia própria, pelas estruturas burocráticas então existentes, especialmente pela diplomacia.

Conforme afirma Jackson (2005, pp. 15 e 35), o processo de desenvolvimento de estruturas burocráticas permanentes de Inteligência se

estendeu até o fim da I Guerra Mundial, a partir de quando a Inteligência se incorporou de forma definitiva ao processo decisório político e militar dos Estados. Portanto, a Inteligência, como parte integrante da burocracia permanente de Estado, surgiu como atividade direcionada à análise de objetos externos, ou seja, com o propósito central de levantar informações estratégicas sobre outros Estados, atores estrangeiros ou eventos e processos no exterior, a fim de antecipar ameaças e oportunidades.

A despeito da orientação inicial da atividade, resultante do contexto histórico no qual ela se originou, o escopo de trabalho da Inteligência passou por processo de diversificação e complexificação. Atualmente, existem serviços de Inteligência que incorporam, na mesma estrutura, competências tão diversas quanto apoio à inserção econômica externa, avaliação de riscos decorrentes de eventos climáticos extremos, contraposição a ações de Inteligência adversa e prevenção e enfrentamento ao crime organizado e ao extremismo violento. O Brasil é exemplo de país cujo serviço de Inteligência civil de Estado, a Agência Brasileira de Inteligência (ABIN), é multitemático.

Além da variedade de competências entre as agências dos diferentes países, os sistemas de Inteligência nacionais apresentam diferentes composições e níveis de complexidade, podendo ser constituídos por grande número de agências especializadas em determinados escopos temáticos ou em métodos específicos de coleta de dados.

Em paralelo à transformação das estruturas de Inteligência, a complexificação de seus objetos de trabalho também resulta em necessidade de revisão dos recortes e enquadramentos utilizados para organizar as atividades das agências de Inteligência. A tradicional divisão entre Inteligência interna e externa exemplifica essa discussão. Em contexto de transnacionalização de processos e eventos, torna-se incontornável a avaliação acerca da pertinência em se classificar como internos ou externos os fenômenos e as questões analisados pela Inteligência,

os quais, mesmo que originados dentro das fronteiras de um país, não podem ser contidos ou não se limitam a estas.

Por fim, a própria finalidade da Inteligência é objeto de debate em instâncias de governo e acadêmicas. Jackson (2005, p. 4), ao tratar as diferentes perspectivas acerca do uso da Inteligência, afirma que se pode sintetizar as discussões sobre o tema em duas abordagens conceituais. A primeira concebe a Inteligência primordialmente como uma ferramenta para orientação das estratégias e políticas públicas, por meio do fornecimento de informações que reduzam o risco decisório. A segunda considera a Inteligência não somente um ativo de autonomia informacional, mas também um instrumento de exercício de poder e de implementação de políticas e estratégias por parte do Estado. Nesse sentido, além de ferramenta de conhecimento da realidade, teria também o papel de intervenção na realidade.

Considerando a falta de consenso e padrão sobre as finalidades, as estruturas e os sistemas organizacionais da Inteligência, a conformação dessa atividade e de seu escopo de trabalho decorre, em grande medida, de uma decisão política, que é condicionada pela trajetória histórica e burocrática de cada país. No Brasil, as competências estabelecidas normativamente para a ABIN evidenciam sua natureza predominantemente informacional. Portanto, no contexto brasileiro, considera-se que a finalidade da Atividade de Inteligência é sobretudo prover informações ou assessoramento para a redução de incertezas na tomada de decisão. No entanto, conforme indicado pela Lei nº 9.883 de 1999, que instituiu o Sistema Brasileiro de Inteligência e a ABIN, também competem à Inteligência de Estado brasileira outras funções, como a promoção da coordenação interinstitucional em Inteligência, o desenvolvimento de capacitação e doutrina em Inteligência e a proteção de conhecimentos sensíveis.

Este capítulo pretende trazer a discussão sobre o processo de renovação da agenda de Inteligência na atualidade, com base nos elementos

caracterizadores dessa atividade e na trajetória da ABIN. Com esse objetivo, a primeira seção tratará do papel da relação entre produtor e usuário para a composição da agenda de Inteligência. Na segunda e terceira seções, serão abordados os processos de complexificação da agenda de Inteligência, tanto no sentido de incorporação de novos escopos de trabalho quanto de revisão de temáticas tradicionais para a atividade, e de renovação da forma como se produz e se difunde Inteligência no contexto contemporâneo. Na parte final, foram feitas considerações sobre os desafios subjacentes a esse processo de renovação de agenda.

1. Adaptabilidade como essência da Atividade de Inteligência e o impacto da relação produtor-usuário sobre a agenda de Inteligência

Ao tratar dos obstáculos ao uso eficiente da Inteligência, Jackson (pp. 13-14) afirma que uma das limitações encontradas é o denominado problema da organização, o qual se refere à dificuldade de adaptação oportuna das estruturas e processos de Inteligência ao ritmo de transformação e à fluidez do ambiente securitário, de onde deriva a agenda de trabalho das instituições de Inteligência de Estado. Embora o autor trate especificamente da rigidez institucional e procedimental como desafio ao cumprimento da missão de assessoramento da Inteligência, a discussão acerca da adaptabilidade como essência ou baliza dessa atividade também se refere à capacidade de renovação e de revisão das questões de interesse para a Inteligência.

Como atividade que visa ao assessoramento ao processo decisório nacional, a Inteligência deve estar conectada à agenda nacional e às necessidades informacionais dos usuários, especialmente das autoridades decisórias, o que exige comunicação constante e adaptação às mudanças de prioridades. Nesse sentido, a utilidade e a eficácia dessa atividade no cumprimento de sua finalidade dependem de sua abertura à transformação de seus objetos e métodos de trabalho.

Lowenthal (2010) argumenta que o consumidor de Inteligência faz mais do que apenas consumir. Ele contribui para definir a agenda, desde as prioridades de Inteligência até a coleta e o formato de entrega. Partindo dessa premissa, o funcionamento eficaz da Inteligência depende do estabelecimento e da manutenção de um ciclo de *feedback* com os formuladores de políticas, especialmente quando novas agendas e cursos de ação estão sendo considerados (Hulnick, 1986).

A interação entre a Inteligência e os formuladores de políticas ocorre em diferentes níveis da burocracia. Diretores, coordenadores e analistas precisam captar percepções dessas interações para aprimorar suas entregas. Nesse sentido, Lowenthal (2010) afirma que não há um único vínculo entre Inteligência e Política, mas várias intersecções entre os dois sistemas.

No Brasil, a Atividade de Inteligência segue um ciclo, que inclui, em suas primeiras fases, a Objetivação, “na qual são determinados os temas, os recortes e as abordagens das áreas que serão trabalhadas”, e o Acompanhamento, que se refere ao “processo constante de planejamento, reunião e processamento de dados, informações e conhecimentos referentes às áreas acompanhadas” (Doutrina de Inteligência, 2023, pp. 56-57). Enquanto a fase de objetivação é conduzida pela alta gestão da agência de Inteligência, com base em suas interações com os usuários, o acompanhamento é realizado pelos profissionais de Inteligência e objetiva a construção de conhecimento de base.

Nesse contexto, o estabelecimento de novos escopos de atuação e a formação de Inteligência de base sobre esses temas demandam tempo e recursos para produção de resultados efetivos. Setores estruturados, por exemplo, para acompanhar o narcotráfico transnacional não poderão, em curto prazo, gerar conhecimento relevante sobre ameaças a setores econômicos estratégicos.

Ao realizar seu trabalho, a Inteligência segue os mesmos parâmetros que regem as relações clássicas de assessoramento: comunicação eficiente, mútua e transparente (Treverton, 2001). Nessa relação produtor-usuário, o primeiro é o agente público responsável pela produção do conhecimento de Inteligência, e o segundo, o tomador de decisão. Essa relação é tão crucial que Couto (2013) afirma que a própria natureza da Inteligência se remete à interdependência entre o produtor de Inteligência e o usuário.

De fato, a proximidade entre a Inteligência e os tomadores de decisão permite que os analistas conheçam suas necessidades e tensões, evitando a produção de estimativas e avaliações irrelevantes (KWA, 2012). McCarthy (1998) acrescenta que o sucesso das ações depende da consistência na proximidade entre o produtor e o consumidor em todos os níveis da burocracia.

Inteligência desconectada e intempestiva, além de representar desperdício de recursos públicos, compromete futuros assessoramentos do órgão de Inteligência. Gil, Marrin e Phythian (2009) afirmam que o protagonismo do assessoramento de Inteligência só será confirmado se as informações se provarem úteis, relevantes e oportunas.

Entretanto, a proximidade excessiva também pode ser prejudicial à construção do conhecimento e da agenda de Inteligência, uma vez que o produtor pode sentir-se pressionado ou ser influenciado a produzir análises que confirmem preconceitos e prioridades políticas (Betts, 2007). Nesse sentido, a Inteligência deve manter distância que permita isenção e autonomia, mesmo que suas conclusões contrariem as expectativas do usuário. Isso é especialmente importante em contextos críticos de polarização político-ideológica.

Além da distância adequada, confiança e compreensão mútua são essenciais nessa relação. Por parte do produtor, é necessária a confiança de que o usuário respeitará a integridade da informação e não

fará uso inadequado da Inteligência. Por parte dos tomadores de decisão, é necessário confiar que os analistas estão transmitindo suas análises de forma honesta e transparente em relação a suas premissas e ao grau de incerteza envolvido na análise.

2. Complexificação da agenda de Inteligência no contexto contemporâneo

Desde o estabelecimento das primeiras instituições autônomas de Inteligência, o rol de competências da Inteligência se modificou em dois sentidos principais. Por um lado, novas questões foram incorporadas à agenda de Inteligência, o que está associado a fatores como a ampliação dos usuários da Inteligência, o amadurecimento institucional das agências de Inteligência e a emergência de novas prioridades dos Estados, tanto em nível doméstico quanto em sua inserção internacional. Por outro lado, questões e temas já consolidados na Atividade de Inteligência tornaram-se mais complexos, impondo novos desafios em termos de capacidade e metodologia de análise e produção.

Embora a renovação da agenda de Inteligência esteja conectada às mudanças das prioridades políticas e estratégias definidas domesticamente, há sinergia nas tendências observadas nos diferentes sistemas e agências de Inteligência, o que decorre da inter-relação entre os interesses dos Estados na arena internacional. Em certa medida, a renovação do escopo de temas trabalhados pela Inteligência associa-se à transformação histórica do próprio conceito de segurança na agenda de Estado, que passou de uma acepção mais restrita, relacionada à ameaça representada por outros Estados, para a incorporação de dimensões não relacionadas diretamente à defesa e à segurança nacional e outras fontes de ameaça não vinculadas a atores estatais. Atualmente, o conceito passou a abarcar fenômenos de natureza não conflitiva, como epidemias ou eventos climáticos extremos, que ampliam as vulnerabilidades de segurança das pessoas e instituições.

No âmbito dessa discussão, o conceito de segurança humana, consolidado no Relatório do Desenvolvimento Humano do Programa de Desenvolvimento das Nações Unidas de 1994 (UNDP), sinaliza essa tendência de alargamento do enfoque securitário para abranger questões não relacionadas a conflitos militares entre Estados, que gerem vulnerabilidades aos indivíduos e às comunidades e afetem a sua integridade. Nesse escopo, estariam contempladas dimensões como segurança ambiental, segurança alimentar, segurança econômica e segurança sanitária.

Ainda que se parta da premissa que nem todas as dimensões contempladas nesta acepção ampla de segurança produzem reflexos diretos sobre a agenda de Inteligência, esta é certamente impactada pela transformação das preocupações securitárias dos Estados, na medida em que é forjada a partir da interação das agências de Inteligência com as autoridades decisórias nacionais.

A emergência de uma agenda de Inteligência econômica estratégica é exemplificativa dessa ampliação de escopos de trabalho da Atividade de Inteligência de Estado em decorrência da ampliação do rol de preocupações securitárias. Dentro dessa área da Inteligência de Estado, os recortes específicos de interesse vinculam-se às prioridades das políticas econômicas, financeiras e comerciais de cada país e podem abarcar questões muito diversas, tais como segurança de setores e insumos econômicos estratégicos, economia digital, transformação industrial e inserção econômica externa.

Desde a criação da ABIN em 1999, temáticas e questões afeitas à Inteligência Econômica foram trazidas aos trabalhos desta agência em diversos períodos, mas sem o estabelecimento de arranjos institucionais permanentes e da especialização necessária para assegurar a continuidade de assessoramento e a conexão com usuários especializados. Esse quadro se alterou nos últimos anos por meio da

estruturação de uma agenda de Inteligência Econômica e de esforço de formação de estrutura organizacional qualificada.

A incorporação das mudanças climáticas como preocupação para os sistemas de Inteligência domésticos também reflete mudança na perspectiva dos Estados sobre a segurança nacional. Considerando que o fenômeno acarreta o que, possivelmente, representa o maior processo de transição global em curso, com múltiplos efeitos sobre as instituições, a vida individual e coletiva, a geopolítica global, o meio ambiente e as estratégias e trajetórias econômicas nacionais, trata-se de campo onde a promoção de autonomia informacional se revela essencial.

Especialmente ao longo da última década, diversos serviços de Inteligência têm buscado construir capacidades para assessorar seus governos no mapeamento e na redução de riscos relacionados à mudança climática, bem como no seu reposicionamento mais eficiente frente às transformações econômicas e sociais por ela geradas. Em geral, a Inteligência aborda a questão sob quatro perspectivas principais: prevenção e gerenciamento de crises decorrentes de eventos climáticos extremos, o que também inclui a promoção da articulação institucional; intersecções entre ilícitos ambientais e agenda climática; impactos sobre setores econômicos estratégicos e economia das mudanças climáticas; e arranjos multilaterais e políticas climáticas. Enquanto agência de Inteligência multitemática, a ABIN tem incorporado recortes dessas quatro vertentes temáticas à sua agenda de trabalho.

Além dos impactos para a Inteligência decorrentes da ampliação das dimensões da segurança incorporadas à agenda estatal, a própria vertente tradicional da segurança, associada à Defesa Nacional e à segurança pública, passou por transformação, incorporando novas fontes de ameaça, como os atores armados não estatais. Como afirmam Hofmann e Schneckener (2011), existe dificuldade em estabe-

lecer definição consensual para atores armados não estatais, o que decorre de suas múltiplas características e dos diferentes tipos de organizações aos quais a expressão se relaciona. De maneira geral, o termo se refere a organizações que têm disposição e capacidade para usar a violência para atingir seus objetivos; não estão integradas na estrutura burocrática estatal, como as forças armadas regulares; e possuem algum nível de autonomia em relação aos Estados, mesmo que atuem em apoio a forças de Estado ou sejam instrumentalizadas por estas (Hofmann e Schneckener, 2011, p. 604).

As organizações criminosas e grupos terroristas são exemplos de ameaças armadas não estatais que se consolidaram nas agendas securitárias domésticas e internacional e, conseqüentemente, se estabeleceram também como fatores de atenção para os sistemas de Inteligência. Em relação às organizações criminosas, a transnacionalização, entendida aqui como processo por meio do qual a globalização produz seus efeitos sobre a criminalidade, além de tornar mais complexa a análise dessa fonte de ameaça, aumentou a centralidade da cooperação internacional em Inteligência sobre crime organizado. A complexificação dos fluxos financeiros e a ampliação das possibilidades logísticas exigem permanente cooperação entre os órgãos de segurança, que precisam se articular de forma rápida e efetiva para enfrentar redes criminais cada vez mais integradas globalmente.

As grandes organizações criminosas demonstram ainda capacidade de diversificar sua atuação, adentrando novos mercados ilícitos que envolvem desde fraudes cibernéticas inovadoras até a exploração ilegal de recursos naturais, como a extração de madeira e minérios, prática especialmente impactante para países como o Brasil e seus vizinhos do entorno amazônico. Tais desafios ampliam a necessidade de articulação entre os órgãos de segurança e de Inteligência da região, os quais passam a compartilhar a necessidade de enfrentar grupos criminosos armados em localidades remotas e de baixa densidade institucional. Com esse propósito, a ABIN tem ampliado a cooperação

com os serviços de Inteligência de países fronteiriços, tanto na realização de diagnósticos estratégicos sobre redes criminosas e ilícitos transnacionais quanto na avaliação de ameaças concretas.

No caso do terrorismo, os ataques de 11 de setembro de 2001 contribuíram para consolidar esse fenômeno como uma das principais ameaças à segurança doméstica e internacional. O alcance do discurso radical promovido por organizações terroristas, por meio de mídias sociais, a dimensão dos atentados executados e a proliferação de grupos afiliados em diversas partes do mundo posicionaram o enfrentamento ao extremismo violento baseado em discurso religioso como prioridade para agências de Inteligência e de segurança.

Nos últimos anos, outras dimensões da ameaça extremista violenta, associadas a ideologias radicais e a subculturas virtuais, violentas, transnacionais e não vinculadas a religiões, passaram a integrar a agenda de Inteligência, em razão de seus impactos para a segurança da sociedade e das instituições. A ampliação dos ataques violentos em escolas no Brasil representa apenas uma das consequências desse fenômeno, exigindo a atuação preventiva e repressiva do Estado.

O uso do espaço virtual como ambiente de promoção da radicalização e de mobilização para o cometimento de atos violentos demanda reformulação das estratégias de prevenção e enfrentamento ao extremismo violento, considerando seu caráter predominantemente descentralizado. A construção de bases metodológicas e analíticas para o enquadramento conceitual do extremismo violento, em oposição a outros fenômenos criminais, para avaliação do nível da ameaça e para estabelecimento de indicadores de radicalização e mobilização para a violência, integra a estratégia da ABIN nessa agenda.

Além de seus efeitos específicos sobre os processos de radicalização, em termos gerais, a transposição de ameaças e processos sociais do espaço real para o meio virtual resultou em novo campo de análise

para a Inteligência. Jackson (p. 44) relembra que a internet, ao mesmo tempo que representa nova ferramenta para a obtenção de informações e o monitoramento de ameaças, também amplia os espaços de geração de riscos securitários e, conseqüentemente, o volume de informações que precisa ser processado. A cibersegurança, vertente de atuação da Inteligência brasileira, se associa ao conjunto de ações e conhecimentos para compreensão, mitigação e gestão de riscos digitais relacionados a ataques ou acessos indevidos, visando assegurar a confidencialidade, a integridade e a disponibilidade das informações no ambiente cibernético (NIST, 2020).

Em paralelo à atuação relacionada a ataques e incidentes cibernéticos, a Inteligência também é parte dos esforços de promoção da soberania digital no Brasil, a qual resulta em diretriz de ampliação da autonomia tecnológica do país, em infraestruturas e ativos digitais. Nessa seara, destaca-se o papel e a atuação da ABIN em duas áreas. A primeira é o desenvolvimento, a atualização contínua e a entrega da criptografia de Estado, a qual é integrada em processos e ativos estratégicos nacionais, como o processo eleitoral e sistemas de comunicação segura. A Inteligência de Estado também participa das iniciativas voltadas à normatização e à definição dos requisitos de segurança para o estabelecimento de uma nuvem soberana de Estado, discussão presente também em sistemas de Inteligência de outros países.

3. Oportunidade e qualidade no assessoramento estratégico de Inteligência

A complexificação da agenda de Inteligência, tanto por meio da incorporação de novas dimensões de análise quanto da emergência de novas fontes de ameaça, ocorre em paralelo à necessidade de revisão da forma como se produz e se difunde Inteligência, em contexto de abundância de informação e de urgência decisória. Quando se trata de assessoramento estratégico, a pressa é um dos fatores de maior impacto no nível de qualidade da entrega. No entanto, a urgência tem

sido condição cada vez mais frequente no trabalho de Inteligência, demandando o estabelecimento de estratégias para mitigar julgamentos enviesados e análises simplificadas (Betts, 2007).

O papel da Inteligência corrente em relação à construção de conhecimento de Inteligência em nível estratégico está no centro das discussões sobre oportunidade e qualidade no assessoramento de Inteligência. Conforme a Doutrina de Inteligência (2023, p. 46), a Inteligência Corrente tem como propósito o assessoramento contínuo e atualizado sobre eventos e situações em progresso e sua evolução, tendo caráter objetivo e descritivo. Em geral, se associa a temáticas e eventos de grande impacto para autoridades decisórias no presente ou no futuro imediato, o que a diferencia de outros tipos de Inteligência, como a Prospectiva, orientados à produção de cenários estratégicos e complexos futuros.

Por parte dos tomadores de decisão, tende a haver preferência pelo consumo de conhecimentos que respondam à crise ou ao problema de curto prazo e a seus desdobramentos imediatos (Betts, 2007). Isso reflete a natureza do processo político, orientado para o presente. Como Lowenthal (2010) observa, o impulso dos eventos atuais tende a distorcer a importância da análise de longo prazo, concentrando o foco da agenda de governo na próxima reunião ministerial, na próxima cúpula ou no orçamento do próximo ano. Cogan (1994) destacou a dificuldade de incorporar o pensamento de longo prazo na agenda de governo, observando que o decisor muitas vezes está focado apenas em informações imediatas. Essa constatação, feita há três décadas, antecede a era das redes sociais, vídeos curtos e comunicações em poucos caracteres.

A gestão de crises é, assim, fator que captura a atenção dos tomadores de decisão e, conseqüentemente, da Inteligência. Quando o tomador de decisão declara uma crise, é esperado que a Inteligência ofereça respostas rapidamente para reduzir as incertezas dela decorrentes

(Coombs, 2015; Pearson, 1998) e que informe sobre uma possível quebra de normalidade e a iminência de uma nova crise.

Nesse contexto, a Inteligência enfrenta o dilema entre a necessidade premente de produção de Inteligência Corrente que reduza as incertezas na tomada de decisão de hoje e a percepção de que a construção de estratégias eficientes por parte do Estado demanda a elaboração de conhecimentos estratégicos de longo prazo. Desde sua criação, a ABIN estruturou-se de diferentes formas para fazer frente a esse desafio, estabelecendo frações especializadas na produção de conhecimento do tipo Inteligência corrente e, em paralelo, buscando incorporar a perspectiva do gerenciamento de crise nas frações com competências temáticas específicas e perenes.

Considerações finais: desafios subjacentes à agenda de Inteligência

Historicamente, a renovação da agenda de Inteligência acompanhou a transformação das prioridades estabelecidas pelas autoridades decisórias nacionais e pelas estruturas burocráticas que conferem exequibilidade às diretrizes de Estado e às estratégias de governo. Essa conexão resulta da própria finalidade informacional e de assessoramento da Inteligência, que exige atenção às necessidades e aos interesses de quem se assessora. Nesse sentido, a relação entre produtor e usuário posiciona-se como condicionante existencial para essa atividade. Em outras palavras, sem consumidor, a Inteligência não perfaz seu propósito e perde, portanto, sua utilidade.

A agenda de Inteligência tem se tornado mais complexa, em parte, porque as agendas dos Estados ganharam novas dimensões, tornando-se também mais complexas; em parte porque as agências de Inteligência passaram por processo de consolidação institucional que lhes permitiu absorver novas competências e se especializar. O desafio de manejar recursos humanos e financeiros limitados frente

a um ambiente securitário mais plural e mais complexo está subjacente à evolução da Atividade de Inteligência em geral, considerando sua essência sobretudo informacional e, portanto, sua necessidade de conexão com os desafios do mundo real.

A ampliação do que se considera questão de Inteligência é acompanhada da diversificação dos usuários de Inteligência. Como destacam Treverton e Agrell (2009, p. 4), a Inteligência, concebida originalmente como ativo informacional para um conjunto limitado de líderes políticos e militares, passou a ser consumida por grande número de usuários, inclusive externos à estrutura de administração direta dos Estados.

A execução de um conjunto de competências tão variado e o atendimento eficiente de usuários com demandas tão diferentes gera necessidade de adaptação das estruturas de Inteligência, o que não ocorre na mesma velocidade de transformação de seus objetos. Esta é uma das principais limitações da Inteligência: seus instrumentos institucionais são estabelecidos e direcionados para avaliar os problemas atuais, frequentemente falhando em identificar as ameaças emergentes.

Nesse contexto, uma das estratégias possíveis para tornar a Atividade de Inteligência mais resiliente e com maior capacidade de antecipar questões que possam emergir na agenda de Estado é criar estruturas específicas para mapear e avaliar os grandes desafios e transições globais e estabelecer exercícios de cenarização periódicos. Esse caminho, embora não elimine a necessidade de renovação dos escopos de trabalho da Inteligência, certamente torna o processo de transformação contínua dessa atividade mais planejado, antecipado e eficiente.

Referências

AGRELL, W. & TREVERTON, G. **National Intelligence Systems – Current Research and future prospects**. Cambridge University Press, 2009.

BETTS, Richard K. **Enemies of intelligence: Knowledge and power in American national security**. Nova Iorque: Columbia University Press, 2007.

COGAN, C. G. **Intelligence and crisis management: The importance of the pre-crisis**. *Intelligence and National Security*, vol. 9, nº 4, p. 633–650, 1994.

COOMBS, W. T. **Ongoing crisis communication: Planning, managing and response**. 4. ed. University of Central Florida: SAGE Publications, 2015.

COUTO, G. R. **A crise e a gestão de crises**. Rio de Janeiro: FGV, 2013.

DOCTRINA DA ATIVIDADE DE INTELIGÊNCIA. Brasília: ABIN, 2023.

GILL, Peter; MARRIN, Stephen; PHYTHIAN, Mark. **Intelligence theory: Key questions and debates**. Routledge, 2009.

HERMAN, M. **Intelligence Services in the informational age**. Routledge, 2001.

HOFMANN, C. & SCHNECKENER, U. **Engaging non-state armed actors in state and peace-building: options and strategies**. *International Review of the Red Cross*, vol. 93, nº 883, set. 2011.

HULNICK, Arthur S. **The intelligence producer–policy consumer linkage: A theoretical approach**. *Intelligence and National Security*, v. 1, n. 2, p. 212-233, 1986. DOI: 10.1080/02684528608431858.

JACKSON, P. **Historical Reflections on the Uses and Limits of Intelligence**. In: *Intelligence and Statecraft – The Use and Limits of Intelligence in International Society*. Ed: Jackson, P & Siegel, J. Praeger Publishers, 2005.

KWA, C. G. **Role of intelligence in international crisis management.**

Singapura: RSIS Working Paper (n. 243), 2012.

LOWENTHAL, Mark M. **Tribal tongues: Intelligence consumers,**

intelligence producers. The Washington Quarterly, v. 33, n. 1, p. 125-137, jan. 2010.

MCCARTHY, S. P. **The function of intelligence in crisis management:**

Towards an understanding of the intelligence producer-consumer dichotomy.

Nova Iorque: Taylor & Francis Group, 1998.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Framework for**

improving critical infrastructure cybersecurity, 2018. In: <https://csrc.nist.gov/pubs/cswp/6/cybersecurity-framework-v11/final>. Acessado em 16/09/2024.

OMAND, David. **Reflections on intelligence analysts and policymakers.**

International Journal of Intelligence and CounterIntelligence, 2020.

DOI: [10.1080/08850607.2020.1754679](https://doi.org/10.1080/08850607.2020.1754679).

PEARSON, C. M.; CLAIR, J. A. **Crisis management reframing.** Management,

vol. 23, n. 1, p. 59–76, 1998.

PNUD. (1994). **Novas Dimensões da Segurança Humana.** Relatório do

Desenvolvimento Humano 1994. Novas Dimensões da Segurança Humana Programa das Nações Unidas para o Desenvolvimento. University Press.

RIBEIRO, A. **Inteligência Externa e Diplomacia: Interfaces e Relações no**

Contexto Brasileiro. Revista Brasileira de Inteligência nº 16, p. 103-123.

Brasília: ABIN, 2021.

TREVERTON, Gregory F. **Reshaping national intelligence for an age of**

information. Cambridge University Press, 2001.

UNDP (United Nations Development Programme). **Human Development**

Report 1994: New Dimensions of Human Security. New York, 1994.

WARNER, M. **Wanted: A Definition of Intelligence.** Studies in Intelligence, vol. 46, nº3, 2002.

WERNER, G. C. **Transnacional e as redes criminosas: Presença e Influência nas relações Internacionais Contemporâneas.** São Paulo. Universidade de São Paulo, 2009.



Desafios tecnológicos emergentes: impactos para a Contraineligência e a resposta a Ameaças Cibernéticas e Interesses adversos

Cristina Célia Fonseca Rodrigues

Oficial de Inteligência
Diretora do Departamento de Contraineligência

Juliano Rodrigues Ferreira

Oficial de Inteligência
Diretor do Centro de Pesquisa e Desenvolvimento para
a Segurança das Comunicações (CEPESC)

O ambiente cibernético transformou radicalmente o panorama das ameaças tradicionais, ampliando significativamente os riscos para a soberania dos Estados e a segurança de informações críticas. Três fatores definem essa mudança, especialmente para a Contraineligência: anonimato, redução de riscos aos atacantes e amplificação do potencial de danos.

A crescente possibilidade de anonimato no ciberespaço, combinada com a redução dos riscos para os atacantes, impulsiona ações maliciosas cada vez mais ousadas. No mundo digital, os ofensores operam com maior segurança, ocultando suas identidades e localizações, o que dificulta drasticamente o rastreamento e a retaliação imediata.

O ambiente digital permite que os danos causados sejam mais amplos e devastadores. Ataques cibernéticos podem impactar múltiplos alvos simultaneamente, comprometendo infraestruturas críticas

— como redes de energia e sistemas financeiros — bem como processos políticos e sociais. As consequências desses ataques são imediatas e abrangentes, tornando a segurança cibernética uma prioridade essencial para proteger a soberania nacional.

Esses fatores constituem a base dos desafios da Contraineligência Cibernética (Goldman; Maret, 2019), que necessita prover a proteção digital em um cenário de constante avanço computacional em diversas áreas. Assim, avanços na computação quântica, em tecnologias como a Inteligência Artificial (IA) e na computação em nuvem, que ampliam a superfície de ataque e aumentam a complexidade da proteção digital, aumentam também a demanda por essa área da Contraineligência (Panda Security Labs, 2018).

A escalabilidade dos ataques cibernéticos, que agora podem ser conduzidos de maneira coordenada e em larga escala, coloca infraestruturas críticas, como redes de energia e sistemas financeiros, sob constante risco. A interconexão dessas infraestruturas também amplifica as vulnerabilidades, exigindo uma abordagem de segurança cibernética adaptada à nova realidade tecnológica (Galinec *et al.*, 2017).

Desse modo, Estados e instituições agora enfrentam o desafio de se proteger contra influências externas que podem minar a estabilidade política e econômica. A defesa eficaz contra essas ameaças requer uma abordagem integrada de segurança cibernética para redução dos riscos e a adoção de novas tecnologias que ofereçam soluções mais robustas para mitigá-los.

Nesse contexto, a segurança cibernética e a Contraineligência precisam evoluir continuamente para acompanhar o ritmo das ameaças. Soluções que combinam criptografia avançada, algoritmos de detecção baseados em IA e desenvolvimento de padrões de segurança robustos tornam-se indispensáveis para proteger as informações sensíveis e resguardar a soberania dos Estados contra interesses adversos.

Busca-se, portanto, aprofundar a análise desses três pilares – anonimato, redução dos riscos aos atacantes e amplificação do potencial de danos – explorando como, juntos, eles transformam o cenário da segurança cibernética, exigindo novas estratégias de mitigação e defesa. Em seguida, é apresentada a discussão sobre a evolução de tecnologias como a computação quântica, a computação em nuvem e a criptografia pós-quântica, que mudam por completo o ambiente cibernético, e os desafios relacionados ao emprego de cada uma dessas tecnologias emergentes para a Contrainteligência.

1. Desafios cibernéticos para a Contrainteligência

Dado o avanço tecnológico e a crescente digitalização das interações humanas, as ameaças no ambiente cibernético evoluíram, trazendo novos desafios à segurança nacional e à Contrainteligência. Esses fatores não apenas redefiniram a forma como os Estados e instituições lidam com ameaças, mas também criaram uma nova dinâmica, na qual os atacantes exploram a vulnerabilidade digital para causar danos em grande escala (Clarke, 2010).

1.1 Anonimato

Um dos fatores que tornam o ambiente cibernético menos arriscado para ofensores, em comparação com o ambiente físico, é a ausência de exposição direta. Em ações cibernéticas, o agressor não precisa estar fisicamente presente no local do ataque, eliminando o risco de ser identificado ou capturado durante a operação (Treverton, 2007). Em ataques tradicionais, como espionagem ou sabotagem física, o agente corre maior risco de ser exposto ou neutralizado, enquanto no ciberespaço as operações podem ser conduzidas remotamente, o que mantém o autor em segurança e fora do alcance das autoridades.

No ambiente digital, identificar a origem de um ataque é extremamente complexo, uma vez que agentes mal-intencionados podem utilizar diversas técnicas para esconder sua identidade e localização. Redes de anonimato, como o TOR, o uso de *Virtual Private Networks* (VPNs) e a falsificação de endereços *Internet Protocol* (IP) são exemplos de estratégias utilizadas para dificultar a identificação do agressor (Haughey *et al.*, 2016).

Tanto o uso de VPNs quanto de tecnologias de mascaramento ou de técnicas de falsificação de IP (*spoofing*) permitem ao atacante ocultar a origem de suas ações, atribuindo a conexão a outra localidade geográfica, o que dificulta a identificação e a localização do verdadeiro autor do ataque. Além disso, muitas ações cibernéticas podem camuflar a identificação pessoal do atacante, uma vez que a identificação digital, em muitos casos, é feita com base em atributos manipuláveis, como *e-mails* ou perfis de redes sociais, o que torna o rastreamento e a identificação do real motivo do ataque mais complexo (Lewis, 2011). A escalabilidade dos ataques cibernéticos, tema que será desenvolvido mais adiante no texto, também aumenta a relevância do anonimato nesse contexto.

Isso contrasta com o ambiente não cibernético, onde a atribuição de responsabilidade é conduzida pelo emprego de técnicas de rastreabilidade de menor complexidade. Assim, operar por trás dessas camadas de anonimato reduz o custo e os riscos dos agressores, potencializa a escalabilidade e dificulta a resposta e a investigação por parte das autoridades.

1.2 Redução dos riscos no ambiente cibernético

Como segundo fator, destacam-se o custo e o risco baixos envolvidos, já que no ambiente digital os ataques podem ser conduzidos remotamente, sem que o autor precise expor-se fisicamente. Isso reduz significativamente os riscos de retaliação ou captura, tornando as ações

cibernéticas mais atraentes para os ofensores. Além disso, a disponibilidade de ferramentas de ataque de baixo custo em mercados ilegais na *dark web* facilita a condução desses ataques por indivíduos ou grupos com recursos limitados.

Outro fator importante é a facilidade de execução e automação no ambiente cibernético. Ferramentas automatizadas permitem que ataques de grande proporção sejam realizados com poucos recursos humanos e financeiros. Um único indivíduo consegue gerar danos significativos utilizando *scripts* ou *softwares* maliciosos, como *botnets*, redes de computadores zumbis, que coordenam ataques contra múltiplos alvos ao mesmo tempo (Haughey *et al.*, 2016). No mundo físico, operações dessa magnitude demandariam uma logística complexa, mais recursos e coordenação muito maior.

Além disso, no ciberespaço, Estados ou organizações mal-intencionadas podem patrocinar esses ataques indiretamente, negando qualquer envolvimento direto e dificultando a atribuição de responsabilidade. O caráter transfronteiriço igualmente reduz os riscos, por agregar complexidade ao anonimato no ambiente cibernético. Isso limita a capacidade de resposta das autoridades, pois os ofensores podem estar operando em jurisdições onde a lei local não coopera com investigações internacionais.

A ausência de fronteiras também reduz os riscos para o atacante devido à dificuldade das autoridades em alcançá-lo em tempo hábil. Ataques realizados de maneira remota dificultam que ações punitivas imediatas sejam tomadas, tais como restrições de liberdade ou a abertura de processos judiciais diretamente contra a pessoa física identificada. Essa limitação nas respostas imediatas aumenta a sensação de segurança para os ofensores e, em muitos casos, torna as consequências menos severas e mais demoradas.

As barreiras legal e territorial, assim, contribuem para a redução de riscos no ciberespaço. Desse modo, enquanto ações físicas são limitadas por fronteiras geográficas e pela aplicação imediata das leis locais, ataques cibernéticos podem ser realizados de qualquer lugar do mundo, muitas vezes escapando das jurisdições tradicionais. Essa característica dificulta a aplicação de punições e retaliações, já que a cooperação internacional e a variação de legislações entre países frequentemente retardam investigações e responsabilizações, beneficiando o agressor.

1.3 Amplificação dos danos

Os danos e impactos de ações no ambiente cibernético são amplificados, principalmente, pela escalabilidade, pela facilidade de exfiltrar dados e pelo alcance global que essas operações são capazes de atingir (Clemente, 2014). Com um investimento mínimo, ofensores podem explorar vulnerabilidades em sistemas críticos, causando um efeito desproporcionalmente alto com relativamente pouco esforço.

Para melhor compreensão do potencial de danos, ressaltam-se três vertentes de atuação no ciberespaço que amplificam os danos causados por agressores: o acesso pelo ambiente cibernético a grandes volumes de dados, o ataque a infraestruturas críticas e a manipulação de informações (Lemos, 2002). Diferente de ataques físicos, que estão limitados a uma área geográfica específica, uma única ofensiva cibernética de qualquer dessas três vertentes pode se espalhar rapidamente e atingir múltiplos alvos simultâneos, em diversas partes do mundo.

A primeira vertente trata do acesso cibernético a grandes volumes de dados, que pode ocorrer, por exemplo, pela disseminação de um *software* malicioso (*malware*) que comprometa sistemas em vários países (cert.br, 2017). O impacto dessas ações é vasto e pode envolver governos, empresas privadas e indivíduos, resultando em uma escala

de danos de difícil contenção imediata (CISA, 2023). O potencial de dano causado por ataques cibernéticos dessa vertente está diretamente relacionado ao tipo de acesso que o atacante consegue obter durante a ofensiva.

Se o acesso concedido pelo ataque for suficientemente profundo, permitindo a invasão do ambiente cibernético de uma instituição ou indivíduo, o invasor pode obter acesso a um grande volume de dados. Se superar as camadas de proteção existentes, isso pode resultar em uma retirada massiva de informações sensíveis ou, ainda pior, na realização de ações destrutivas, como a cifração de dados (ataques de *ransomware*), modificação ou até mesmo destruição completa das informações (Cawthra *et al.*, 2020). Se o ataque comprometer também medidas adicionais de proteção, como os *backups*, os impactos podem ser devastadores e, em muitos casos, irreversíveis (Kaspersky, 2022).

Uma vez que o ataque é lançado, ele pode se propagar por sistemas interconectados de forma extremamente rápida, tornando difícil contê-lo. Mesmo quando os sistemas de defesa detectam o ataque, a recuperação total dos dados pode levar semanas ou meses. Esse acesso massivo de dados pode ter por finalidade não só a subtração, mas também a manipulação de dados em grande escala, o que compromete a segurança de dados sensíveis e confidenciais, assim como segredos comerciais e de governo que impactam na segurança do Estado e da sociedade. A manipulação de dados, por exemplo, como a adulteração de registros ou informações críticas, pode levar a decisões erradas, com consequências catastróficas para organizações e Estados. O impacto desse tipo de ataque pode ser devastador não só para reputação de empresas e governos, mas também para a economia e a segurança nacional.

A segunda vertente relaciona-se com a complexidade da interdependência digital, o que torna as ações de contenção mais complicadas

e menos eficazes do que as respostas tradicionais a ataques físicos (Geer, 2008). Ataques às redes de energia ou aos sistemas financeiros, de comunicações e de transporte são amplificados devido à interconexão e à dependência digital dessas infraestruturas críticas. Quando uma ofensiva cibernética compromete esses sistemas, as consequências são imediatas e de grande alcance. Um ataque a essas infraestruturas e serviços essenciais afeta diretamente a vida de milhões de pessoas e gera crise econômica e social. A incapacidade de operar essas infraestruturas de maneira segura gera danos consideráveis em setores vitais para o funcionamento da sociedade moderna.

Essa vertente de ataque gera impactos econômicos prolongados, característica marcante dos ataques cibernéticos. Além dos custos imediatos relacionados à recuperação de sistemas e à mitigação dos danos, as perdas associadas à interrupção de negócios e à queda na confiança dos consumidores provocam consequências de curto e longo prazo. Empresas perdem clientes e mercados inteiros devido à falta de confiança, enquanto mercados financeiros sofrem quedas significativas, afetando economias. Assim, o impacto econômico dessas ações cibernéticas não se limita aos danos diretos, já que exige a reconstrução da credibilidade e a implementação de novas medidas de segurança.

Finalmente, a terceira vertente é a da manipulação de opinião pública e de processos políticos, que aumenta exponencialmente o impacto de ações cibernéticas. A capacidade de influenciar narrativas e interferir em processos democráticos, por meio de campanhas coordenadas de desinformação em plataformas digitais, é uma ameaça crescente (Woolley; Howard, 2018). Perfis falsos, contas-robôs (*bots*) e campanhas de *fake news* são utilizadas para desestabilizar sociedades ao polarizar opiniões e comprometer a confiança pública nas instituições (Burbach; Watts, 2020). Assim, essas campanhas cibernéticas têm efeitos duradouros na coesão social e na estabilidade política, colocando em risco a integridade dos processos políticos.

Os fatores de anonimato, de redução dos riscos e de amplificação dos danos trazem complexidade e impacto suficientes para gerar um novo paradigma para a Contrainteligência. Nesse cenário, a área deve se adaptar a uma nova realidade, na qual as medidas de segurança precisam ser repensadas a partir da aplicação de novos padrões de segurança cibernética.

2. Ameaças da Inteligência Artificial e do avanço computacional: espionagem, interferência externa e o papel da criptografia de Estado

Ao tratar do emprego das novas tecnologias para a Contrainteligência, Cunliffe (2021) analisa que, para atender a demanda dos Estados em proteger dados, conhecimentos e infraestruturas sensíveis, os serviços de Inteligência vêm adotando novas estratégias. A necessidade de se estruturar frente a particularidades apresentadas pelas novas tecnologias passa, necessariamente, pela avaliação das novas ameaças que esse contexto de evolução tecnológica apresenta.

Trata-se da era das redes sociais, da presença *online* e da troca instantânea de informações, o que impulsiona o desenvolvimento de tecnologias emergentes que trazem consigo uma capacidade inédita de ampliação da comunicação, compartilhamento de informações e interação constante entre pessoas, organizações e Estados.

No entanto, essa facilidade de comunicação e os novos mecanismos proporcionados por essas tecnologias emergentes trazem riscos inerentes ao processo. A possibilidade de comunicações serem comprometidas e informações serem indevidamente acessadas torna-se maior em um ambiente onde a flexibilidade no uso dessas alternativas é amplamente incentivada. Quanto mais acessíveis as ferramentas, maiores as vulnerabilidades, e os riscos de inteligência adversa também crescem significativamente. A espionagem cibernética, o roubo de dados sensíveis e a manipulação de informações se tornam mais

viáveis à medida que as tecnologias avançam, exigindo maior vigilância e respostas rápidas por parte do Estado.

Busca-se, assim, tratar, ao menos, de três marcos da mudança de paradigma, que obrigam a Contrainteligência a repensar sua atuação: o uso de IA, a computação em nuvem e a computação quântica.

2.1 Espionagem e Contraespionagem com uso de IA

Nesse novo cenário tecnológico, registra-se a rápida e significativa evolução da IA, que se tornou mais acessível à sociedade nos últimos anos. A IA se destaca como uma ferramenta poderosa, promovendo avanços em áreas como a automação de processos, o reconhecimento facial e de voz. Contudo, o aspecto mais notável da IA está na sua capacidade de criação e inovação, características tradicionalmente associadas à inteligência humana, especialmente no que se refere à criatividade.

A IA ainda possui grande potencial por aumentar a capacidade de coleta automatizada de grandes volumes de dados, assim como ampliar a produção de conhecimento com maior qualidade, aspecto que está relacionado à capacidade de automatizar tarefas repetitivas, processar grandes volumes de dados, apoiar a pesquisa científica e criar novos conteúdos de maneira autônoma (Ventre, 2020).

A capacidade criativa, ademais, é o ponto central de uma área específica da IA, conhecida como Inteligência Artificial Generativa (IAG). A IAG é capaz de gerar novos conteúdos de maneira autônoma, simulando textos, vídeos e áudios com alta complexidade. No entanto, essa evolução traz novas preocupações no campo da Contrainteligência. A IAG tem o potencial de ser usada para a criação de conteúdos maliciosos, com o objetivo de enganar e manipular a sociedade e o Estado, promovendo desinformação por meio da geração de materiais falsos e convincentes. Esse aspecto apresenta riscos adicionais à soberania dos Estados e à proteção de suas informações mais sensíveis.

No contexto da espionagem tradicional, um dos recursos mais utilizados é o disfarce de identidade. Agentes de interesse adverso frequentemente assumem identidades falsas para transmitir informações com maior credibilidade ou obter acesso a dados confidenciais. Ao se passarem por outra pessoa — frequentemente alguém com as credenciais necessárias para acessar uma determinada informação —, esses agentes conseguem manipular sistemas e pessoas, infiltrando-se em áreas sensíveis. Essa técnica permite que o agente crie uma falsa sensação de segurança, facilitando tanto a coleta de informações quanto a disseminação de desinformação de maneira eficaz.

Com o avanço da IA e, mais especificamente, da IAG, o conceito de disfarce de identidade evoluiu para um nível mais sofisticado através do uso de *deepfakes*, o que permite que agentes adversos tenham a capacidade de simular a identidade de uma figura pública ou de um indivíduo com credenciais específicas de forma altamente convincente.

A partir do emprego da IAG, portanto, é possível potencializar os danos de um disfarce de identidade, pela criação de *deepfakes* — vídeos, áudios e textos falsificados que podem ser atribuídos a pessoas reais, gerando confusão e impactando negativamente processos sociais e políticos. O uso de *deepfakes* amplifica os riscos pois a tecnologia permite que essa simulação seja realizada com uma precisão quase imperceptível ao olho humano. Técnicas de IA que criam *deepfakes* ainda podem ser associadas a *bots* em mídias sociais, com o objetivo de massificar e intensificar a manipulação das informações e influenciar processos de acordo com interesses que muitas vezes estão desalinhados com os do Estado e da sociedade.

A capacidade da IA de produzir essas falsificações profundas representa um risco real para a lisura das comunicações e da confiança pública. Isso torna o disfarce de identidade digital uma ferramenta poderosa e perigosa, com potencial de impacto em escala global. Esse tipo de interferência pode comprometer a integridade de debates

públicos, eleições e outras dinâmicas sociais, gerando uma ameaça significativa à estabilidade e à segurança das nações. Assim, a Contrainteligência deve estar preparada para lidar com esses ataques mais sofisticados, onde agentes maliciosos utilizam a IA para comprometer a segurança nacional, atacar infraestruturas críticas e manipular a integridade das comunicações e da confiança pública.

Uma importante contramedida a ser desenvolvida para evitar o uso malicioso da IA são os sistemas de detecção de ameaças baseados em IA. Um detector de IA funciona ao analisar grandes volumes de dados e interações em tempo real, buscando comportamentos atípicos (Branitskiy; Kotenko, 2019). Ele pode identificar padrões de atividade que indicam a presença de *bots*, *deepfakes* ou outras formas de manipulação geradas por IA. Esses sistemas utilizam técnicas de aprendizado de máquina para monitorar e analisar interações digitais, detectando anomalias como postagens repetitivas, respostas automatizadas ou imagens manipuladas, que são características comuns de ataques realizados com IA maliciosa (Li *et al.*, 2019).

Ademais, algoritmos avançados podem comparar mídias suspeitas com arquivos legítimos, revelando discrepâncias que expõem tentativas de manipulação. Essas técnicas são essenciais para neutralizar o uso malicioso da IA por interesses estrangeiros ou adversos, garantindo a proteção dos processos políticos e sociais. A IA também contribui significativamente na verificação automatizada de fatos, cruzando informações disseminadas com fontes confiáveis para combater a desinformação em tempo real. Ao identificar rapidamente conteúdos falsos ou distorcidos, a IA permite que o material enganoso seja rotulado e sua disseminação contida antes que cause danos maiores.

Por fim, técnicas de detecção de IA pelo emprego dessa mesma tecnologia emergente ainda podem ser integradas a soluções de cibersegurança já existentes, permitindo uma resposta automática e coordenada para prevenir danos maiores. Essas tecnologias são essenciais

para a proteção de informações sensíveis e para a preservação da integridade de processos políticos e sociais, assegurando a soberania do Estado e a confiança pública.

Em conclusão, à medida que a IA é cada vez mais utilizada, é crucial que seus benefícios sejam ampliados de maneira a preservar a soberania e a integridade da sociedade. O uso de IA para mitigar desinformação, *deepfakes* e perfis falsos fortalece a confiança no ambiente digital e nos processos políticos, protegendo os interesses nacionais contra influências adversas. Com a aplicação dessas tecnologias, é possível antecipar e mitigar riscos, garantindo uma resposta rápida a possíveis ataques e protegendo tanto os interesses do Estado quanto da sociedade.

2.2 A nova fronteira da segurança: o fim da proteção baseada no ambiente físico e o desafio da computação em nuvem

Anteriormente, a segurança estava centrada apenas no controle de acesso e na proteção do ambiente físico. Contudo, esse modelo foi alterado com a ascensão da computação em nuvem, que introduziu novos desafios e oportunidades no campo da segurança digital. Com a evolução tecnológica e o crescente volume de dados digitais, a necessidade de mecanismos robustos de armazenamento e segurança cibernética tornou-se ainda mais crucial.

Embora a computação em nuvem já seja uma tecnologia amplamente adotada por muitas instituições públicas e privadas, sua expansão acelerada nos últimos anos trouxe um aumento proporcional nos riscos associados. A flexibilidade e a escalabilidade oferecidas pela nuvem são inegáveis, mas a utilização mais ampla dessa tecnologia também amplifica os riscos de segurança. A crescente dependência da nuvem e o advento de novas tecnologias como a Internet das Coisas (IoT) exige que as organizações estejam preparadas para lidar com ameaças cibernéticas mais complexas.

A capacidade de interconectividade entre infraestruturas, assim como o potencial de compartilhamento de dados e tecnologias, muitas vezes envolvendo a utilização conjunta de capacidade computacional, reduz os investimentos necessários e gera ganhos de eficiência, escala e flexibilidade nos trabalhos realizados. No entanto, é crucial reconhecer que essa interconectividade também amplia as vulnerabilidades, o que deve ser cuidadosamente considerado nas avaliações de riscos associados (Broucek; Turner, 2012).

A migração completa da infraestrutura de uma organização, incluindo capacidade de processamento, infraestrutura física e armazenamento de informações, para a nuvem eleva os potenciais prejuízos em caso de acessos indevidos. Quando dados sensíveis são armazenados em ambientes fora do controle direto das instituições, a exposição a ataques cibernéticos aumenta significativamente.

Assim, é fundamental que as instituições implementem medidas robustas de segurança na nuvem, tais como a criptografia de dados, políticas de acesso controlado e monitorização constante para mitigar os riscos envolvidos. Nesse contexto, é importante o planejamento da interconectividade entre as infraestruturas, acompanhado do planejamento de gestão de riscos. Quando infraestruturas compartilham informações e capacidades, é fundamental que o nível de segurança seja homogêneo entre as instituições envolvidas. Isso evita que o acesso indevido ocorra no elo mais fraco desse processo de interconexão.

Muitas vezes, os atacantes identificam níveis desiguais de segurança entre as partes envolvidas e escolhem explorar as vulnerabilidades nos pontos mais fracos. Ao comprometer um sistema vulnerável, eles podem lateralizar o ataque, expandindo seu acesso para outras áreas interconectadas e, assim, maximizar os danos e aumentar estrategicamente a coleta de dados. Por essa razão, é fundamental que todas as partes adotem controles de segurança equivalentes, a fim de prevenir esse tipo de comprometimento em cadeia.

Essas medidas preventivas são essenciais para fortalecer a soberania digital e dependem de uma combinação de inovações tecnológicas, regulação rigorosa, cooperação internacional e investimentos contínuos em criptografia e segurança cibernética. A Contrainteligência, portanto, carece de atuação conjunta com a segurança cibernética, em um paradigma que deixa de ser centrada apenas no controle de acesso e na proteção do ambiente físico e passa a atuar no campo da segurança digital.

Desse modo, a Contrainteligência deve atuar na proteção das informações armazenadas com uma criptografia resistente, que se tornará a última e mais importante camada de defesa contra acessos indevidos ou vazamentos de dados sensíveis. A criptografia funciona ao converter dados legíveis em um formato codificado, que só pode ser acessado por aqueles que possuem as chaves necessárias para sua decodificação. Esse processo oferece uma camada adicional de segurança, especialmente quando outras formas de proteção, como *firewalls* ou sistemas de detecção de intrusos, são superadas por ataques maliciosos. Assim, mesmo que invasores consigam acessar um sistema ou furtar dados, as informações permanecem protegidas e inutilizáveis.

A cifração desses dados é que garante, portanto, a proteção dos interesses do Estado e da sociedade. Se os perímetros de segurança forem comprometidos e o ataque adverso for bem-sucedido, a criptografia permanece como o último recurso de defesa, protegendo diretamente os dados e dificultando sua utilização por agentes maliciosos. A criptografia de Estado, ao adotar algoritmos robustos e resistentes até mesmo às ameaças emergentes, como a computação quântica, assegura que, mesmo que os invasores obtenham acesso a sistemas, as informações continuarão inacessíveis sem as chaves adequadas. Dessa forma, a criptografia atua como uma barreira crítica, preservando a confidencialidade e a soberania das informações estratégicas.

Em resumo, a criptografia de dados não é apenas uma camada de proteção: é uma estratégia vital para assegurar a confidencialidade e a integridade de informações sensíveis em um cenário digital cada vez mais complexo e ameaçado. Nesse contexto, em que se percebe claramente a importância da utilização da computação em nuvem, a criptografia é vital na proteção dos interesses do Estado uma vez que é fundamental considerar e tratar adequadamente os riscos associados à evolução da computação em nuvem.

2.3 Contrainteligência e Tecnologias emergentes

O avanço da computação quântica representa outro fator de risco significativo devido a sua capacidade exponencial de processamento, muito superior à dos computadores tradicionais. A criptografia, baseada em processos matemáticos complexos, poderia ser vulnerabilizada caso essa capacidade de processamento ultrapassasse certos limites, pois esses dispositivos, ao utilizarem princípios da mecânica quântica, têm o potencial de quebrar, ou seja, decifrar, certos algoritmos criptográficos que não foram projetados para resistir ao poder de processamento quântico.

Os algoritmos criptográficos mais amplamente usados hoje, como o RSA e o ECC (*Elliptic Curve Cryptography*) (Schneier, 2015), poderiam ser comprometidos por computadores quânticos suficientemente poderosos, uma vez que estes seriam capazes de resolver em um tempo viável problemas matemáticos complexos que atualmente garantem a segurança desses algoritmos. Isso colocaria em risco uma vasta quantidade de informações protegidas por algoritmos criptográficos que não foram projetados para resistir ao poder de processamento quântico.

Embora o custo da computação quântica ainda seja elevado, existe o potencial de que ela se torne acessível a Estados adversos ou grupos com grandes recursos. Esses atores poderiam usar essa tecnologia

para comprometer a segurança de dados sensíveis, expondo informações críticas a ataques cibernéticos. Essa possibilidade reforça a urgência no desenvolvimento e implementação de algoritmos de criptografia pós-quântica, capazes de resistir às ameaças trazidas por essa nova tecnologia.

Já existem diversas iniciativas avançadas em computação quântica, lideradas tanto por empresas privadas quanto por governos ao redor do mundo. Algumas das maiores empresas envolvidas incluem IBM, Google, Microsoft, Amazon e a chinesa Alibaba (Thompson, 2019), que estão na vanguarda da pesquisa e desenvolvimento de *hardware* e *software* quânticos. Essas empresas criam infraestruturas e plataformas que tornam a computação quântica mais acessível a pesquisadores e empresas, acelerando o progresso nessa área.

A IBM é amplamente reconhecida como uma das líderes do setor, oferecendo o *IBM Quantum*, que permite o acesso a seus sistemas de computação quântica via nuvem, e investindo em soluções de escalabilidade que tornam seus sistemas mais robustos. A Google, com seu *Google Quantum AI*, também fez avanços significativos (MIT, 2020), como a demonstração da viabilidade de *qubits* lógicos em 2023, um passo importante na correção de erros quânticos. Por sua vez, a Microsoft, por meio do *Azure Quantum*, está construindo um ecossistema quântico na nuvem, combinando computação quântica e clássica de forma híbrida para atender a diversos usos.

Além das iniciativas privadas, governos de mais de 30 países têm investido fortemente nessa tecnologia, estabelecendo estratégias nacionais de computação quântica (GQI, 2022). Entre esses países estão Estados Unidos, Reino Unido, China e Finlândia, que estão comprometidos com o desenvolvimento de centros de pesquisa quântica e o financiamento de projetos de longo prazo. A computação quântica é vista como uma tecnologia estratégica, tanto para a segurança nacional quanto para a competitividade econômica (MIT, 2023).

Esses investimentos públicos e privados são fundamentais, pois, embora a computação quântica ainda seja uma tecnologia cara e em estágio de desenvolvimento, seu potencial de transformação em diversas indústrias, incluindo a segurança cibernética, é imenso.

Reconhecendo essa necessidade, o Instituto Nacional de Padrões e Tecnologia (NIST), uma das principais entidades globais em padrões criptográficos, iniciou um processo de seleção e padronização de novos algoritmos capazes de resistir a essas ameaças (NIST, 2020). O NIST identificou e está atualmente testando vários algoritmos com o objetivo de estabelecer um padrão global para a próxima geração de criptografia, garantindo que os dados permaneçam protegidos em um cenário onde a computação quântica se torne uma realidade acessível.

Entre os algoritmos selecionados pelo NIST, destacam-se o *CRYSTAL-S-Kyber* e o *CRYSTALS-Dilithium*. O *Kyber* foi escolhido para a criptografia de chave pública, devido a sua eficiência e alta segurança em resistir a ataques quânticos. Já o *Dilithium* foi selecionado para a geração de assinaturas digitais, sendo reconhecido por sua capacidade de oferecer assinaturas seguras e eficientes. Além desses, o NIST também selecionou o *Falcon* como opção adicional para assinaturas digitais, devido a seu equilíbrio entre segurança e desempenho.

Esses esforços são cruciais para garantir a segurança de informações sensíveis em diversas áreas, como comunicações governamentais, transações financeiras e dados pessoais. O desenvolvimento da Criptografia de Estado pode se beneficiar significativamente das orientações e padrões estabelecidos pelo NIST, especialmente ao integrar algoritmos pós-quânticos. Isso proporcionaria soluções robustas e preparadas para enfrentar as futuras ameaças da computação quântica, garantindo maior segurança e resiliência dos sistemas criptográficos.

Desse modo, a evolução da computação quântica levanta a necessidade urgente de desenvolver e implementar criptografia resistente à computação quântica, também conhecida como “criptografia pós-quântica”, cujos algoritmos são projetados para oferecer segurança contra a capacidade de processamento massivo de computadores quânticos. Assim, enquanto a criptografia permanece uma ferramenta crucial para proteger dados sensíveis, é imperativo que se acompanhe de perto o avanço dessas novas tecnologias para garantir que as proteções vigentes sejam adaptadas e fortalecidas diante das novas ameaças emergentes.

Conclusão

Em resumo, o avanço das tecnologias emergentes, como a IA e a computação quântica, trouxe consigo uma série de benefícios, mas também impôs novos desafios no que tange à segurança cibernética e à soberania nacional. O anonimato no ambiente digital, combinado com a facilidade de execução e o baixo custo dos ataques cibernéticos, cria um cenário em que as ameaças são amplificadas e mais difíceis de conter. A partir disso, o desenvolvimento de tecnologias de segurança avançadas torna-se essencial para mitigar os riscos e proteger os interesses estratégicos dos Estados.

Nesse contexto, a Criptografia de Estado adquire uma importância central. À medida que as infraestruturas críticas e informações sensíveis estão cada vez mais conectadas, é a criptografia que fornece a última linha de defesa contra acessos indevidos. A criptografia de dados resguarda as informações, mesmo quando outros mecanismos de proteção falham, garantindo que agentes mal-intencionados não possam utilizá-las, mesmo que obtenham acesso aos sistemas. Além disso, com a iminente chegada da computação quântica, torna-se urgente o desenvolvimento de algoritmos pós-quânticos, que oferecem resistência aos poderes de processamento massivo desses novos sistemas. A implementação de tais algoritmos, conforme

destacado pelos esforços do NIST e outras instituições globais, assegura que as infraestruturas estatais e corporativas possam resistir às ameaças emergentes, preservando a confidencialidade e integridade das informações.

Outro ponto crucial para a Contraineligência é a detecção de atividades maliciosas com IA, como a criação de *deepfakes* e a disseminação de desinformação por meio de *bots*. O uso de sistemas de detecção baseados em IA que monitoram padrões anômalos em tempo real é vital para antecipar e neutralizar essas ameaças. Esses sistemas não apenas identificam ataques, como também agem de forma preventiva, fornecendo uma resposta rápida e coordenada contra tentativas de manipulação digital que possam comprometer processos políticos e sociais. Isso é especialmente relevante no combate a interesses adversos, que utilizam essas tecnologias para desestabilizar democracias, influenciar eleições ou minar a confiança pública nas instituições.

Portanto, a combinação de criptografia robusta, algoritmos pós-quânticos e sistemas de detecção de IA maliciosa constitui um tripé essencial para a proteção contra ameaças cibernéticas e a preservação da soberania. Esses elementos não só asseguram a integridade das informações sensíveis, mas também fornecem ferramentas para neutralizar ameaças externas e interferências adversas que buscam explorar vulnerabilidades no ambiente digital. Ao integrar essas soluções de maneira estratégica, Estados e instituições estarão mais preparados para enfrentar os desafios do cenário cibernético contemporâneo, garantindo tanto a segurança nacional quanto a confiança pública.

Referências

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA – ABIN (2023). Doutrina da Atividade de Inteligência. Brasília, DF, p.177.

BRANITSKIY, A.; KOTENKO, I. Applying Artificial Intelligence Methods to Network Attack Detection. In: SIKOS, L. (ed) **AI in Cybersecurity: Intelligent Systems Reference Library**, vol 151, 2019.

https://doi.org/10.1007/978-3-319-98842-9_5.

BROUCEK, V; TURNER, P. Technical, legal and ethical dilemmas: Distinguishing risks arising from malware and cyber-attack tools in the 'cloud'-a forensic computing perspective. In: **Journal of Computer Virology and Hacking Techniques**, 2013.

<https://doi.org/10.1007/s11416-012-0173-0>.

BURBACH, D.; WATTS, C. Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News. In: **Naval War College Review**: v.73, n.1, 2020. Disponível em: <https://digital-commons.usnwc.edu/nwc-review/vol73/iss1/17>. Acesso em: 22/10/2024.

CAWTHRA, J; EKSTROM, M; LUSTY, L; SEXTON, J; SWEETNAM, J. Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events. In: **NIST special publication**, 2020.

CERT.BR. **Cartilha de segurança para Internet**. Disponível em: <http://cartilha.cert.br>. Acesso em: 22/10/2024.

CLARKE, R. A. **Cyber War: The Next Threat to National Security and What to Do About It**. New York: Harper Collins, 2010.

CLEMENTE, D. Cybersecurity. In: DOVER, R; GOODMAN, M; HILLEBRAND, C. (Org.) **Routledge Companion to Intelligence Studies**. Londres: Routledge, 2013.

CUNLIFFE, K. S. **Hard target espionage in the information era: new challenges for the second oldest profession, Intelligence and National Security**, 36:7, 1018-1034. (2021)

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). Ransomware Guidance and Threat Awareness, In: **CISA**, 2023. Disponível em: <https://www.cisa.gov>. Acesso em: 22/10/2024.

GALINEC, D.; MOŽNIK, D.; GUBERINA, B. Cybersecurity and cyber defence: national level strategic approach. In: **Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije**, v. 58, n. 3, p. 273-286, 2017

GEER, D. Complexity is the enemy. In: **IEEE Security and Privacy**, ed.nov/dez, 2008. Disponível em: <http://ieeexplore.ieee.org>. Acesso em 22/10/2024.

GLOBAL QUANTUM INTELLIGENCE (GQI). Global Quantum Investments: A Country-by-Country Analysis. **Quantum Computing Report**, 2022. Disponível em: <https://quantumcomputingreport.com>. Acesso em: 24/10/2024.

GOLDMAN, J.; MARET, S. **Intelligence and Information Policy for National Security: Key Terms and Concepts**. Maryland: Rowman & Littlefield, 2016

HAUGHEY, H; EPIPHANIOU, G; AL-KHATEEB, H. Anonymity networks and the fragile cyber ecosystem. In: **Network Security**. p.10-18, 2016. [https://doi.org/10.1016/S1353-4858\(16\)30028-9](https://doi.org/10.1016/S1353-4858(16)30028-9).

KASPERSKY. Ransomware Attacks: Trends and Analysis. In: **Kaspersky Reports**, 2022. Disponível em: <https://www.kaspersky.com>. Acesso em: 22/10/2024.

LEMOS, A. **Cibercultura**. Porto Alegre: Sulina, v. 320, 2002.

LI, J.; QU, Y.; CHAO, F.; SHUM, H.P.H.; HO, E.S.L.; YANG, L. Machine Learning Algorithms for Network Intrusion Detection. In: SIKOS, L. (ed)

AI in Cybersecurity: Intelligent Systems Reference Library, vol 15, 2019.

https://doi.org/10.1007/978-3-319-98842-9_6.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY. Quantum computing is closer than you think. In: **MIT Technology Review**, 2020. Disponível em:

<https://www.technologyreview.com>. Acesso em: 22/10/2024.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY. The race for quantum supremacy: How governments are fueling the next computing revolution.

In: **MIT Technology Review**, 2023. Disponível em:

<https://www.technologyreview.com>. Acesso em: 22/10/2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). (2020).

Recommendation for Key Management Part 1: General. In: **NIST Special**

Publication, 2020. Disponível em: <https://csrc.nist.gov>. Acesso em

24/10/2024.

PANDA SECURITY LABS. **The hunter becomes the hunted: How cyber**

counterintelligence Works, 2018. Disponível em: <https://www.pandasecurity.com/mediacenter/panda-security/cyber-counterintelligence>.

Acesso em:

22/10/2024

SCHNEIER, B. **Applied Cryptography: Protocols, Algorithms, and Source Code**

in C. 20ª Edição. Nova Jersey: Wiley. 2015.

STALLINGS, W. **Cryptography and Network Security: Principles and Practice**,

8ª Edição. Londres: Pearson, 2020.

THOMPSON, C. Inside Google's quantum supremacy experiment. In: **Wired**,

2019. Disponível em: <https://www.wired.com>. Acesso em 22/10/2024.

TREVERTON, G. Risk and Riddles. In: **Smithsonian Magazine**, ed. junho,

2007. Disponível em: [http://smithsonianmag.com/history/risks-and-](http://smithsonianmag.com/history/risks-and-riddles-154744750/)

[riddles-154744750/](http://smithsonianmag.com/history/risks-and-riddles-154744750/). Acesso em 22/10/2024.

VENTRE, D. Artificial Intelligence, Cybersecurity and Cyber Defense. Nova Jersey: Wiley-ISTE, 2020. <https://doi.org/10.1002/9781119788195>.

WOOLLEY, S.; HOWARD, P. **Computational propaganda: political parties, politicians, and political manipulation on social media**. Oxford: Oxford University Press, 2018.



Os próximos 25 anos

Intelis

União dos Profissionais de Inteligência de Estado
Gestão 2022-2024

Todo profissional de inteligência está, de certo modo, voltado para o futuro. Os conhecimentos que produzimos têm dois propósitos: ou esclarecem, interpretam e explicam uma situação em curso, indicando tendências para o seu desenvolvimento; ou estimam cenários com os quais o país deverá lidar no médio ou longo prazos. Porém, nenhum de nós, profissionais de inteligência, foi agraciado com o dom da previsão, e antever o futuro não é uma tarefa fácil. Toda estimativa sobre o que virá depende do que estamos conseguindo enxergar agora, no presente. Se um aspecto determinante para a evolução de certa situação ainda não foi percebido, não será levado em consideração. Até que emerja e passe a ser.

Pensar como serão os próximos vinte e cinco anos para o nosso ofício não foge à regra. Embora a Atividade de Inteligência seja milenar, serviços de inteligência, tal como nós os conhecemos hoje em dia, são organismos recentes. As primeiras instituições contemporâneas desse tipo, voltadas à reunião, análise e interpretação de dados e informações para assessorar decisões relacionadas à defesa, à segurança e à consecução dos objetivos dos Estados, datam da primeira metade do século XIX. Contudo, a maioria foi estabelecida ou reformada após a Segunda Guerra Mundial. Antes, a Atividade de Inteligência era realizada setorialmente e de forma intermitente. Seus praticantes exerciam outros ofícios e eram apenas esporadicamente incumbidos de obter e difundir dados ou informações sobre aconte-

cimentos ou contextos que poderiam afetar o trajeto desejado para a nação.

Consolidados durante a Guerra Fria, a lógica dos serviços secretos estava, então, voltada para a obtenção de dados protegidos pelos adversários. A descoberta desses segredos, de forma sigilosa e oportuna, era a principal missão da maioria dos profissionais de inteligência. Outra vertente cuidava de produzir eventos que pudessem alterar o comportamento de adversários. Durante esse período, os organismos de inteligência começaram a ser utilizados como ferramenta de política externa, um meio velado de projetar poder e influenciar outros países a assumir posições e atitudes que beneficiassem os interesses do Estado patrocinador. Tudo isso dentro da lógica de uma disputa acirrada entre dois projetos de conformação mundial.

Com o abrupto colapso da União Soviética, essa lógica desmoronou. Os anos 1990 foram caracterizados por grandes incertezas para a Atividade de Inteligência. Não apenas no Brasil, onde a extinção do Serviço Nacional de Informações, ocorrida no âmbito das reformas administrativas do governo de Fernando Collor de Melo, tornou incerto o futuro da atividade e de seus profissionais, mas no mundo inteiro. Ao longo de toda a década, discutia-se não apenas qual seria a nova conformação mundial – unipolar, multipolar, unipolar na política e multipolar na economia, ou o contrário – mas também o que fazer com os vultosos aparatos de inteligência que haviam sido criados no período anterior e consumiam expressivos orçamentos nacionais.

Foi uma década de grande debate teórico nos estudos de inteligência, na qual se buscou compreender quais passariam a ser os principais temas de interesse dos Estados, qual é o peso que a descoberta dos segredos dos adversários teria e se era mais sábio investir em análises mais refinadas, capazes de inferir mistérios, ou seja, antecipar comportamentos e tendências. Foi também nessa década que atores

não estatais começaram a ganhar peso como objetos de acompanhamento da Atividade de Inteligência.

O que os profissionais de inteligência fariam a partir de então? Quais seriam os limites de sua atuação? Como eles seriam organizados e o que se esperava deles? Cada país buscou estabelecer seus parâmetros e paradigmas a partir não só das experiências que tivera durante a Guerra Fria, mas também do futuro que projetava. O espectro era amplo, e os países precisavam optar pela linha de conduta que entendiam ser a mais adequada.

No Brasil, esse debate se deu entre parlamentares e integrantes do Poder Executivo, logo no início do governo de Fernando Henrique Cardoso. Estudos e debates sobre como deveria ser o novo aparato de inteligência brasileiro foram realizados ao longo desse governo, com algumas propostas sendo apresentadas à apreciação parlamentar ainda no primeiro ano de governo. Teríamos um serviço voltado somente para fora? Cuidaríamos de temas internos? Qual seria o tamanho e a função das nossas equipes operacionais? Haveria um sistema ou os diversos órgãos comporiam uma comunidade?

Quando a Abin foi criada, no final de 1999, o Estado brasileiro havia feito suas opções. A Atividade de Inteligência brasileira é centrada na obtenção e análise de dados, informações e conhecimentos que possam auxiliar autoridades governamentais a gerenciar o país. Além disso, a agência é responsável pela proteção de conhecimento sensíveis, de nossos segredos, e pela contraposição a ações de inteligência adversa, podendo, portanto, produzir eventos que garantam ao país vantagens competitivas em relação aos seus adversários.

Essa opção não foi feita de modo leviano ou impensado. Ao contrário, debates e discussões sobre como seria o novo aparato de inteligência levaram quase uma década. Entre o primeiro normativo apresentado ao Congresso Nacional sobre o tema, no início de 1995, e a

publicação da Lei 9.883, em dezembro de 1999, quase cinco anos se passaram.

Foi também em 1995 que a primeira turma de profissionais de inteligência concursados ingressou nos quadros do serviço público do país. Na época, a Atividade de Inteligência estava sob a responsabilidade da Subsecretaria de Inteligência, que integrava a Secretaria de Assuntos Estratégicos da Presidência da República. E foi lá que esses profissionais foram lotados. Só após a criação do serviço de inteligência brasileiro, a Abin, esses concursados encontraram sua casa definitiva.

A adoção do concurso público como forma de seleção dos profissionais de inteligência garantiu melhor formação e pluralidade para os nossos quadros. Atualmente, as quatro carreiras de inteligência são compostas quase que integralmente por servidores concursados, formados por universidades gabaritadas, com graduações e experiências diversificadas. Pluralidade é uma característica basilar para um serviço eminentemente analítico, que deve ser capaz de olhar um objeto de acompanhamento sob diversos prismas.

Outra característica fundamental para o bom desempenho da Atividade de Inteligência é a sua especialização. Atualmente, os profissionais de inteligência da Abin são servidores de carreira formados na Atividade de Inteligência, capazes de compreender os meandros e as dificuldades não apenas do exercício dessa atividade, mas também da condução de uma nação como o Brasil em um contexto internacional complexo e volátil. Conseguimos abordar as questões de segurança de forma mais ampla que o olhar centrado na Defesa, típico das Forças Armadas, e que o olhar focado na segurança pública, preocupação precípua dos policiais. O que nos falta é um diálogo franco e aberto com a sociedade civil, a quem servimos.

No Brasil, estamos presos ao passado. Na introdução do livro que editaram sobre a formação dos aparatos de inteligência de Estados

européus, Bob De Graaff e James M. Nyce explicam que a cultura de inteligência de um país é geralmente moldada a partir do que é percebido como um evento traumático coletivo ou nacional¹. Segundo esses autores, a reação coletiva a esses eventos traumáticos e aos impactos que eles tiveram na sociedade determina o escopo, o propósito e a função da Atividade de Inteligência a ser exercida pelos diferentes países.

Mas essa é uma dificuldade brasileira. Não costumamos lidar com os nossos traumas históricos. Os empurramos para baixo do tapete na esperança pueril de que eles sumam por si sós. O que, é claro, nunca acontece. Falta-nos encarar com franqueza os impactos da escravidão, dos reincidentes golpes de Estado e da perseguição a "inimigos internos", prática antiga e reiterada da cultura política brasileira. Deixar de tratar seriamente esses assuntos não diminui os nossos conflitos internos, mas impede que nos desenvolvamos como país e adia a adoção de políticas que gerem efetiva evolução social.

Não há país no contexto internacional atual que possa almejar uma posição de relevância entre seus pares sem ter um serviço de inteligência atuante e eficaz. Nos últimos vinte e cinco anos, a importância da Atividade de Inteligência ficou mais nítida. A emergência de atores não estatais, transformações climáticas, demográficas, digitais e energéticas soma-se aos clássicos temas de acompanhamento político e econômico que exigem a obtenção, análise e interpretação oportuna de dados e informações que auxiliem na condução da nação. Esses novos temas, comuns à maioria dos países, têm fomentado intercâmbio e cooperação cada vez mais presentes entre serviços de inteligência. Mais do que nunca, o Brasil precisa de um serviço estável.

Em um mundo em constante transformação, não sabemos ao certo se o que entendemos hoje por Atividade de Inteligência será a mesma

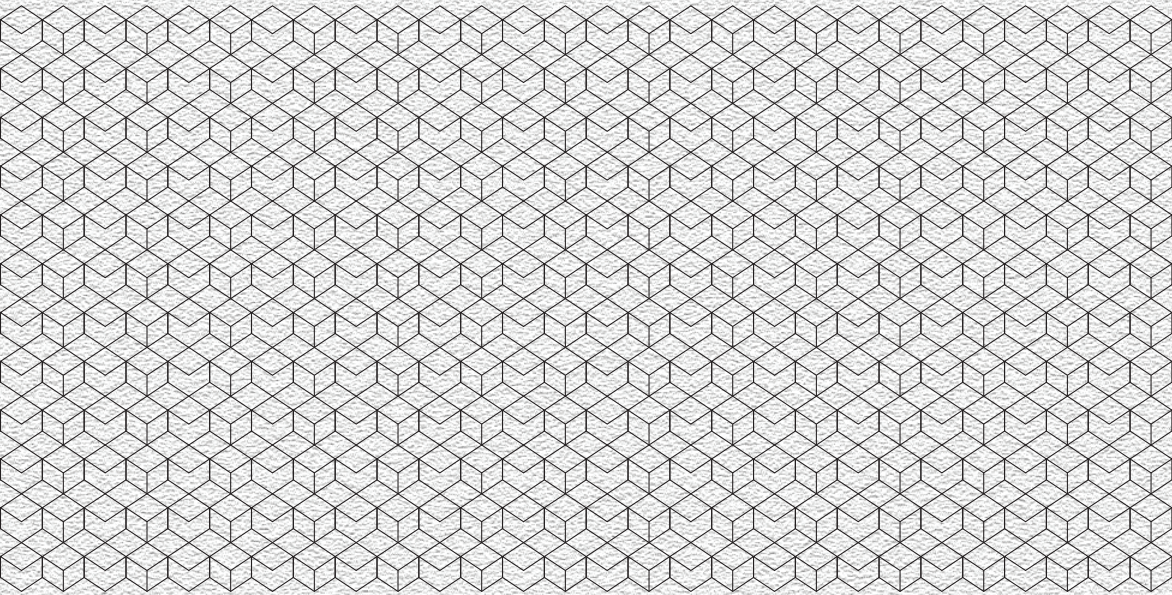
¹ DE GRAAFF, Bob e NYCE, James. Introduction. IN: DE GRAAFF, Bob e NYCE, James (eds). **The Handbook of European Intelligence Cultures**. Londres: Rowan & Littlefield, 2016 (ebook não paginado).

coisa a que iremos nos referir em 2049. Sabemos, contudo, que o que está por vir não pode ser construído apartado do diálogo com a sociedade. Serviços de inteligência são reflexo da cultura política da sociedade e do Estado a que servem. O que fazem, para que servem, como serão empregados não é uma decisão exclusiva de seus profissionais. Ao contrário, o exercício da Atividade de Inteligência de um país deriva das projeções e anseios trazidos pelos governantes e pelos cidadãos.

Temos, hoje, um corpo funcional integrado por profissionais comprometidos e competentes, que sabem, melhor do que quaisquer outras categorias, exercer essa atividade tão peculiar. É necessário, contudo, quebrar as justificáveis resistências da maior parte da população brasileira, ainda presa a representações fantasiosas sobre a nossa atividade. Precisamos conversar abertamente sobre o que desejamos que os profissionais de inteligência façam. E estabelecer mecanismos eficazes para controle e supervisão de suas atividades.

Não somos, como dito anteriormente, clarividentes. Não temos como prever como a Atividade de Inteligência brasileira se comportará no próximo quarto de século, mas temos como influenciar esse comportamento. Juntos podemos construir um futuro benéfico para a sociedade e o Estado brasileiros, que supere os atuais estereótipos e permita ao país caminhar de forma segura e firme.

Este livro foi composto na fonte Roboto corpo 10
e impressão em dezembro de 2024.



ISBN 978-65-86360-47-9



9 786586 360479