RBI

Revista Brasileira de Inteligência

Número 18 - Dezembro 2023

e-ISSN 2595-4717
ISSN1809-2632

PRESIDÊNCIA DA REPÚBLICA
CASA CIVIL
AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Revista Brasileira de Inteligência

ISSN 1809-2632 versão impressa
ISSN 2595-4717 versão online

Capa
Helen Santos Rigaud

Editoração Gráfica
Tiago Oliveira Baldasso

Revisão
Daniel Macedo de Almeida, Caio Lyrio e Regina Marques Braga Farias

Catalogação bibliográfica internacional, normalização e elaboração
Divisão de Conhecimento e Memória – DICOM/CGPE/ESINT

Disponível em
http://rbi.enap.gov.br

Contato
SPO Área 5, quadra 1, bloco D
CEP: 70610-905 – Brasília/DF
E-mail: revista@abin.gov.br

Tiragem desta edição
1000 exemplares

Impressão
Gráfica - Abin

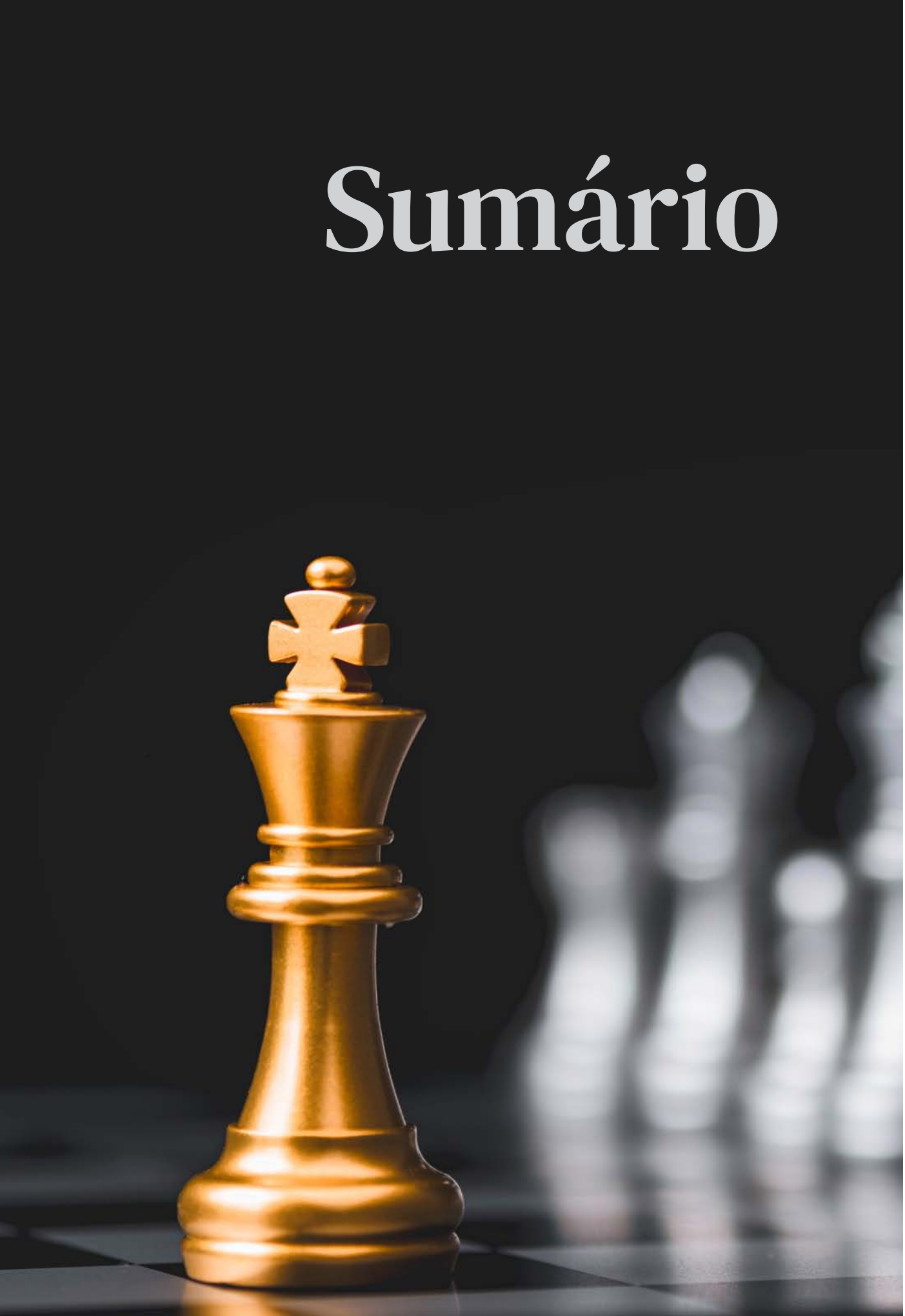
Organização:
Direção-Geral

Dados Internacionais de Catalogação na Publicação (CIP)

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência.
– n.18 (dez.2023) – Brasília: Abin, 2023.
316 p.
Anual
ISSN 1809-2632 versão impressa
ISSN 2595-4717 versão online
1. Atividade de Inteligência – Periódicos – Brasil. 1. Agência Brasileira de Inteligência.

CDU: 355.40(81)(051)

Sumário



Editorial

A Escola de Inteligência da ABIN tem a satisfação de apresentar a 18° edição da Revista Brasileira de Inteligência (RBI). Contando com 15 artigos científicos e 2 resenhas críticas sobre temas relevantes para a Atividade de Inteligência, esta edição é um marco para a RBI. A diversidade profissional e acadêmica dos autores, bem como a variedade de tópicos discutidos, são reflexo da crescente inserção da RBI nas universidades, no serviço público e na sociedade civil brasileira. Destacamos o cumprimento da missão da revista, no sentido de ser um veículo de debate amplo sobre a função da Inteligência no Brasil e em defesa do Estado Democrático de Direito.

O conjunto de textos publicados representa uma contribuição relevante para o debate sobre os desafios da Inteligência no Brasil e no mundo. Entre os assuntos abordados estão a centralidade dada à biossegurança e bioproteção laboratorial desde a pandemia de SARS-CoV-2; o uso de fontes humanas em missões de paz da ONU; a geoeconomia e segurança econômica do Brasil; a relação entre Inteligência e segurança pública no País, desdobrando-se em temas como as práticas, a tecnologia empregada e o arcabouço político e gerencial. Também se discute neste número a relação entre serviços de Inteligência e a mídia.

Essa edição da RBI traz textos que discutem a *práxis* da Atividade de Inteligência. A função analítica e interpretativa do profissional de Inteligência, por exemplo, é discutida em comparação com a atividade jurídica e com o ciclo de políticas públicas. A metodologia do processo de produção de conhecimento é tratada em artigo sobre a etapa de julgamento de fonte e checagem de informação, uma das partes mais críticas no ambiente de desordem informacional contemporâneo. A produção de conhecimento também é abordada do ponto de vista do impacto e das consequências dos vieses cognitivos na análise de Inteligência. A Inteligência de Alerta é encarada enquanto metodologia analítica específica, com potencial para aprimorar o assessoramento ao processo decisório governamental no Brasil. Neste número também se encontra uma discussão sobre como a Inteligência Artificial (IA) pode ser incorporada cuidadosa e criticamente aos desafios de coleta, análise e disseminação de conhecimentos produzidos pelas organizações de Inteligência.

As incertezas globais resultantes do reordenamento de poder no sistema internacional, bem como as ameaças e oportunidades para o Brasil nesse contexto, nos obriga a repensar os desafios internos e externos para a Atividade de Inteligência. Em todo o mundo, fica cada vez mais evidente que o secretismo exacerbado e o insulamento burocrático da Inteligência são prejudiciais para a efetividade e a legitimidade de sua missão institucional em contextos em que a própria manutenção e aperfeiçoamento dos regimes políticos

democráticos estão sendo questionados. A RBI continuará sendo um veículo para a publicação de resultados de pesquisas sérias sobre a Atividade de Inteligência em suas múltiplas dimensões e desafios, valorizando o debate racional de alto nível sobre os desafios concretos da paz, da segurança e do bem-estar das pessoas e instituições no Brasil.

Boa leitura!

Marco Cepik
Diretor da Escola de Inteligência da Abin

Artigo

1

POLÍTICA E REQUISITOS REGULATÓRIOS PARA BIOSSEGURANÇA E BIOPROTEÇÃO LABORATORIAL NO BRASIL *

DOI: https://doi.org/10.58960/rbi.2023.18.223

André de Oliveira Mendonça **
Cláudio Mafra ***

Resumo

O tema "Biossegurança e Bioproteção Laboratorial" vem se mostrando cada vez mais estratégico e, dada sua abrangência e importância para a saúde animal, humana e ambiental, a OMS publicou o documento "*Guidance on implementing regulatory requirements for biosafety and biosecurity in biomedical laboratories - a stepwise approach*", com orientações sobre como esse assunto deve ser regulamentado pelos diferentes países. O presente ensaio buscou avaliar o cenário nacional frente a essas recomendações. Verificou-se que nossas instituições alcançaram recentemente importantes avanços, com destaque para a inclusão da área "Biossegurança e Bioproteção" como estratégica no âmbito da CREDEN e para a publicação do "Plano Nacional de Segurança de Infraestruturas Críticas". Apesar destes avanços, algumas lacunas permanecem, tais como: ausência de um modelo de fomento do ensino, pesquisa, desenvolvimento tecnológico e inovação; carência de um arcabouço normativo abrangente e adequado à complexidade do tema; falta de um "Programa Nacional de Capacitação" em Biossegurança e Bioproteção Laboratorial; ausência de uma "Rede Nacional de Laboratórios de Alta Contenção"; carência de um planejamento estratégico que inclua a definição da infraestrutura desejável para o país no tocante ao quantitativo e aos níveis de biossegurança dos laboratórios; falta de mecanismos para certificação de laboratórios de alta contenção biológica e a necessidade de coordenar ações de colaboração nos níveis nacional e internacional. Será, ainda, necessário identificar papéis e responsabilidades dos entes governamentais envolvidos com o tema, assim como os mecanismos para prover continuamente os elevados recursos financeiros para a implementação das ações de mitigação das lacunas identificadas.

Palavras-chave: biossegurança; bioproteção; laboratórios de alta contenção biológica; regulação; Política Pública.

---

* Este artigo é produto da tese de doutorado de André O. Mendonça, desenvolvida no âmbito do Programa de Pós-Gradução em Bioquímica Aplicada da Universidade Federal de Viçosa (UFV), como parte do projeto "Gestão e Governança em Biossegurança", financiado pelo Edital PROCAD-Defesa, CAPES-Ministério da Defesa.

** Mestre em Medicina Veterinária pela Universidade Estadual Paulista (UNESP). Doutorando em bioquímica com ênfase em biossegurança laboratorial pela Universidade Federal de Viçosa (UFV). Auditor Fiscal Federal Agropecuário.

*** Mestre em Parasitologia pela Universidade Federal de Minas Gerais (UFMG). Doutor em Bioquímica pela Universidade Federal do Rio Grande do Sul (UFRGS). Professor Titular da Universidade Federal de Viçosa (UFV). Presidente da Sociedade Brasileira de Biossegurança e Bioproteção.

POLICY AND REGULATORY REQUIREMENTS FOR LABORATORY BIOSAFETY AND BIOSECURITY IN BRAZIL

Abstract

The subject "Laboratory Biosafety and Biosecurity" is becoming more and more strategic. Considering its broad scope and relevance to animal, human and environmental health, the WHO released the document "Guidance on implementing regulatory requirements for biosafety and biosecurity in biomedical laboratories - a stepwise approach" with recommendation about the regulation of this issue worldwide. The purpose of this essay is to evaluate the national scenario in face of this recent issued recommendations. It was showed that our institutions achieved relevant progress, such as the identification of this issue as strategic for CREDEN and the release of the "National Plan for Security of the Critical Infrastructure". Nevertheless, some critical gaps remain, such as: lack of a model to support instruction, research, technological development and innovation; lack of a wide and updated legal framework adequate to this complex subject; lack of a "National Training Plan" on Laboratory Biosafety and Biosecurity; lack of a "National Network for High Containment Laboratories"; lack of a strategic plan that includes the definition of the national desirable infrastructure in terms of number and biosafety level of laboratories; lack of procedures for high-containment laboratory certification; need to coordinate collaboration programs at national and international levels. It is also necessary identifying roles and responsibilities of the governmental bodies involved with this issue, as well as mechanisms to continuously provide the high financial resources needed to carry out the mitigation actions to address the gaps identified.

Keywords: *biosafety; biosecurity; high-containment laboratory; regulation; Public Policy.*

POLÍTICAS Y REQUISITOS REGLAMENTARIOS PARA LA BIOSEGURIDAD Y BIOSEGURIDAD DE LABORATORIO EN BRASIL

Resumen

El tema "Bioseguridad y Bioprotección en el Laboratorio" es cada vez más estratégico. Considerando su amplio alcance y relevancia para la salud animal, humana y ambiental, la OMS publicó el documento "Guía sobre la implementación de requisitos reglamentarios para la bioseguridad y la bioprotección en laboratorios biomédicos: un enfoque gradual" con recomendaciones sobre la regulación de este tema en todo el mundo. El propósito de este ensayo es evaluar el escenario nacional frente a las recomendaciones recientemente emitidas. Se demostró que nuestras instituciones lograron avances relevantes, como la identificación de este tema como estratégico para CREDEN y la liberación del "Plan Nacional de Seguridad de la Infraestructura Crítica". Sin embargo, persisten algunas brechas críticas, como: la falta de un modelo que apoye la instrucción, la investigación, el desarrollo tecnológico y la innovación; falta de un marco legal amplio y actualizado adecuado a este complejo tema; falta de un "Plan Nacional de Capacitación" en Bioseguridad y Biocustodia de Laboratorios; falta de una "Red Nacional de Laboratorios de Alta Contención"; falta de un plan estratégico que incluya la definición de la infraestructura nacional deseable en términos de número y nivel de bioseguridad de laboratorios; falta de procedimientos para la certificación de laboratorios de alta contención; necesidad de coordinar programas de colaboración a nivel nacional e internacional. También es necesario identificar roles y responsabilidades de los organismos gubernamentales involucrados en este tema, así como mecanismos para proporcionar continuamente los altos recursos financieros necesarios para llevar a cabo las acciones de mitigación para abordar las brechas identificadas.

Palabras clave: *bioseguridad; bioseguridad; laboratorio de alta contención; regulación; Política Pública.*

Introdução

O aparecimento ou o ressurgimento de doenças infectocontagiosas tem sido cada vez mais comum nas últimas décadas (ex.: Influenza H1N1, Zika vírus, Chikungunya e Ebola), o que indica que podemos estar vivendo uma nova era de pandemias (MORENS; FAUCI, 2020). As enormes dificuldades enfrentadas pelos países no combate à pandemia da COVID-19 (a doença do coronavírus) evidenciaram a necessidade de aperfeiçoamento, em todo o mundo, das políticas públicas voltadas para a promoção de biossegurança e bioproteção laboratorial. Mesmo antes da pandemia, a Organização Mundial de Saúde (OMS) vinha insistindo na necessidade de os países mobilizarem recursos financeiros nacionais e internacionais para melhorar a biossegurança laboratorial e o desenvolvimento de planos e programas para preparação e fortalecimento dos laboratórios (OMS, 2005).

Neste quesito, há laboratórios da área biológica internacionalmente classificados em quatro "Níveis de Biossegurança" (NB-1 a NB-4), conforme o risco ao trabalhador, à comunidade e ao meio ambiente. Laboratórios NB-3 (alta contenção biológica) são destinados principalmente a manipulação de agentes biológicos com potencial de transmissão respiratória ou por meio de aerossóis, o que pode causar infecções graves e potencialmente letais com forte impacto sobre a saúde humana, animal, vegetal ou ambiental, e colocar em risco o equilíbrio social e econômico nos níveis local, regional ou global. Laboratórios NB-4 (máxima contenção biológica), por sua vez, são destinados à manipulação de patógenos de máximo risco, exóticos ou desconhecidos, para os quais não existem tratamentos ou vacinas disponíveis (U.S. GOVERNMENT, 2020). Atualmente, o Brasil não possui nenhum laboratório com infraestrutura, equipamentos e sistemas para operação sob condições NB-4, e o número de laboratórios com característica NB-3 ou autodeclarados como se assim o fossem é desconhecido, mas estima-se que podem passar de uma centena (MAFRA, 2020). A ausência de um laboratório de máxima contenção e de uma rede estruturada de laboratórios de alta contenção representa uma fragilidade importante para o país, na medida em que coloca em risco a detecção e o controle de enfermidades ocasionadas por patógenos que demandam tais instalações (CARDOSO *et alii*, 2010).

Dada a importância do assunto, a OMS publicou recentemente o documento "*Guidance on implementing regulatory requirements for biosafety and biosecurity in biomedical laboratories - a stepwise approach*" (OMS, 2020), que alerta: os "laboratórios utilizados na identificação dos patógenos desempenham um papel fundamental na construção de uma gestão adequada dos riscos biológicos e na promoção de uma cultura de responsabilidade".

E, ainda, que "o controle dos riscos biológicos se inicia no nível nacional, a partir do estabelecimento de legislação e regulamentos que definem as medidas de controle a serem implementadas para laboratórios autorizados a realizar ensaios", e conclui que "a maioria dos países que desenvolveu essa estrutura legal também estabeleceu mecanismos para monitorar e supervisionar o atendimento das normativas por parte desses laboratórios".

Das políticas públicas para biossegurança e bioproteção

As últimas décadas têm sido marcadas por intensas e constantes transformações no Estado e na sociedade. Assim como em outras áreas das ciências sociais, os estudos sobre administração e políticas públicas vêm procurando compreender como e quanto complexas mudanças de caráter social, econômico, político e tecnológico impactaram o modelo de funcionamento e os resultados das ações governamentais implementadas (CAVALCANTE, 2017).

Alguns atores afirmam que o modelo de Estado tradicional vem se transformando de um Estado de serviço, produtor do bem público, em um Estado que serve de garantia à produção do bem público; de um Estado ativo, provedor solitário do bem público, em um Estado ativador, que aciona e coordena outros atores a produzir com ele; de um Estado dirigente ou gestor em um Estado cooperativo, que produz o bem público em conjunto com outros atores. Sobre a transição do Estado provedor para o Estado garantidor da produção dos serviços públicos, há um debate político que trata da amplitude das atividades estatais (KISSLER; HEIDEMANN, 2006).

Nesse sentido, serviços de alta relevância estratégica e de elevado custo (tanto para implantação como para operação) postam-se como de atribuição exclusiva do Estado. A temática da biossegurança laboratorial se enquadra perfeitamente nesses parâmetros e evidencia o papel inquestionável do Estado em prover esse serviço, conforme as tendências do novo modelo de atuação estatal, tendo em vista os elevados custos e demandas especializadas envolvidos em projeto, construção, operação e manutenção dos laboratórios de alta contenção biológica, que demandam processos de governança estatal bem estruturada (PASTORINO *et alii*, 2017).

Por sua complexidade e por seu potencial impacto econômico, o assunto exige a participação, de forma integrada e colaborativa, de inúmeros atores para o êxito das ações planejadas, tais como: representantes das áreas de saúde pública, defesa e segurança nacional, agricultura, comércio, inteligência, justiça, indústria e finanças, além de profissionais da academia, organizações não governamentais, instituições locais, imprensa e outras

representações da sociedade civil (CICERO *et alii*, 2019).

No intuito de contribuir para o avanço das políticas públicas nacionais afetas à biossegurança laboratorial, e com base na legislação vigente, na revisão de literatura e na experiência profissional dos autores com o referido tema, avaliamos as recomendações da OMS (OMS, 2020) que discutem o estágio de implementação dos requisitos regulatórios no Brasil e apresentam considerações quanto aos seus avanços e limitações.

Mobilização para um comprometimento nacional e definição de recursos para o desenvolvimento e a implementação de uma Política Nacional de Biossegurança e Bioproteção (PNBB)

A Lei nº 11.105/2005 (BRASIL, 2005a) estabelece normas de segurança e mecanismos de fiscalização de atividades que envolvam Organismos Geneticamente Modificados (OGMs) e seus derivados, cria o Conselho Nacional de Biossegurança, reestrutura a Comissão Técnica Nacional de Biossegurança (CTNBio) e dispõe sobre a Política Nacional de Biossegurança (PNB). Esta lei foi resultado da transferência de uma política estabelecida em âmbito internacional por meio do "Protocolo de Cartagena sobre Biossegurança para a Convenção sobre Diversidade Biológica (CDB) da Organização das Nações Unidas (ONU)". Entretanto, ainda que a atual PNB atenda satisfatoriamente os aspectos relacionados à regulamentação dos OGMs e a utilização de células-tronco embrionárias humanas para fins de pesquisa e terapia, não abrange, com a devida profundidade, outros aspectos relacionados a biossegurança e bioproteção laboratorial (FONTOURA; GUEDES, 2013), e é frequentemente confundida como se englobasse, em seu escopo, patógenos das mais variadas classes de risco, e mesmo não geneticamente modificados.

A despeito de tais limitações na formulação da PNB, deve ser reconhecido que o tema "Biossegurança e Bioproteção" vem assumindo uma importância cada vez maior no contexto das decisões estratégicas do governo brasileiro, mesmo antes do advento da pandemia da COVID-19, e, desde o ano de 2018, é considerada, juntamente com Energia, Transportes, Água, Telecomunicações e Finanças, como uma das áreas prioritárias de Infraestruturas Críticas (ICs) para o Estado Brasileiro (BRASIL, 2018). Esta situação reforçou este tema na agenda governamental e culminou com a criação de três Grupos Técnicos (GTs) nesta área prioritária: GT Infra[1], GT PNBB[2] e GT NB4[3] (BRASIL,

1 Segurança de ICs para pesquisa, identificação, levantamento e avaliação de ameaças e vulnerabilidades.
2 Elaboração da Política Nacional de Biossegurança e Bioproteção (PNBB).
3 Elaboração de Proposta de Construção do Laboratório NB4.

2020).

Como nas demais áreas prioritárias, essa determinação teve como premissa propor a implementação de medidas e ações relacionadas com a segurança das ICs para a Câmara de Relações Exteriores e Defesa Nacional (Creden) do Conselho de Governo. Esta decisão, algo até então inédito para a grande maioria das nações, trouxe para a agenda governamental brasileira o reconhecimento de biossegurança e bioproteção em seus mais diferentes vertentes e atores governamentais. Assim, estes GTs são compostos por servidores representantes dos seguintes órgãos: Ministério da Defesa (MD), Casa Civil da Presidência da República, Ministério da Justiça e Segurança Pública (MJSP), Ministério das Relações Exteriores (MRE), Ministério da Agricultura, Pecuária e Abastecimento (MAPA), Ministério da Saúde (MS), Ministério da Ciência, Tecnologia e Inovações (MCTI), Ministério do Meio Ambiente (MMA), Gabinete de Segurança Institucional da Presidência da República (GSI/PR), Agência Brasileira de Inteligência (ABIN) e Ministério da Educação (MEC).

Por esta estrutura organizacional de governança, verifica-se que a visão interministerial com que o tema foi abordado considera a biossegurança e a bioproteção não apenas um assunto de biodefesa ou, segundo a perspectiva laboratorial, de saúde e sanidade humana, animal e vegetal, como também de "Saúde Única", ótica abrangente e moderna. Logo, verifica-se que a representatividade alcançada atende aos requisitos preconizados pela OMS, com exceção da ausência de representantes das esferas públicas estaduais e municipais e de organismos não governamentais.

Condução de estudos e uma avaliação nacional

Ao revisar a literatura e documentos públicos nacionais relacionados ao tema, identificamos alguns estudos com resultados relevantes sobre diferentes aspectos de biossegurança e biocontenção laboratorial no Brasil (Quadro 1).

Quadro 1 - Estudos publicados sobre biossegurança e bioproteção laboratorial no Brasil

Título	Autoria	Ano	Formato
Biossegurança aplicada a laboratórios e serviços de saúde	MASTROENI	2006	Livro
Contribuição da arquitetura na qualidade dos espaços destinados aos laboratórios de contenção biológica	VIEIRA	2008	Tese
Projeto e construção de laboratórios de biossegurança NB3 de baixo custo	HERNANDES	2008	Dissertação
Análise da construção da competência do Brasil em direção ao laboratório de contenção máxima: realidades e perspectivas	CARDOSO	2008	Tese
Biossegurança em saúde: prioridades e estratégias de ação	MS	2010	Livro
Biossegurança: uma abordagem multidisciplinar	TEIXEIRA; VALLE	2010	Livro
Diretrizes gerais para o trabalho em contenção com agentes biológicos	MS	2010	Manual
Health surveillance, biosafety and emergence and re-emergence of infectious diseases in Brazil	CARDOSO *et alii*	2010	Artigo
Invisibilidade de situação de risco biológico no campo da Saúde Pública: desafios de biossegurança e biosseguridade	ROCHA	2011	Tese
Avaliação dos conhecimentos e procedimentos em biossegurança de trabalhadores de laboratórios nível de biossegurança 3	SIMONETTI	2014	Tese
Normativas internacionais de proteção contra bioterrorismo e biocrimes: lacunas e vulnerabilidades no Brasil	POMPEU	2014	Dissertação
Fundamentos Técnicos e o Sistema Nacional de Biossegurança em Biotecnologia	BINSFELD	2015	Livro
Biocontenção: o gerenciamento do risco em ambientes com alta contenção biológica NB3 e NBA3	MS	2015	Livro
O papel do Hospital de Força Aérea do Galeão (HFAG) no atendimento de vítimas de terrorismo químico	NEVES	2016	Dissertação
Emergências em saúde pública por eventos químicos, biológicos, radiológicos e nucleares (QBRN) na perspectiva da inteligência estratégica: recomendações em prol da intersetorialidade na segurança da saúde e na biodefesa	COELHO	2017	Dissertação
Biossegurança Laboratorial: consolidação e harmonização dos regulamentos e normas nacionais	CAMPOS *et alii*	2019	Livro
Biossegurança no desenvolvimento de vacinas, biofármacos e kits de diagnóstico	SENNA; MULLER	2020	Artigo
Pensando uma infraestrutura estratégica nacional: o laboratório NB-4 brasileiro	MAFRA	2020	Livro
Relatório final do seminário internacional: Laboratório Nacional de Máxima Contenção Biológica (LNMCB)	MCTI	2021	Relatório
Comparison of Brazilian High and Maximum Containment Laboratories Biosafety and Biosecurity Regulations to Legal Frameworks in the United States and Other Countries: Gaps and Opportunities	MENDONÇA *et alii*	2023	Artigo

Fonte: elaborado pelos autores

A despeito da relevância dos estudos citados, cabe destacar a escassez de publicações em revistas científicas, tanto nacionais como internacionais. Verificamos também marcada carência de estudos que abordem a situação da infraestrutura dos laboratórios de alta contenção instalados no Brasil, assim como aspectos relacionados a recursos humanos e financeiros, escopo de atividades, processos de comissionamento e certificação, governança etc.

Por outro lado, merecem destaque ações continuadas do MD, em parceria com a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes). Seus programas possuem como objetivo o avanço técnico-científico por meio da criação de cursos de pós-graduação voltados para a temática de biossegurança e bioproteção no contexto da Defesa. Neste sentido, destaca-se a publicação do Edital nº 15/2019 da CAPES, que viabilizou o financiamento da proposta para um curso de Doutorado com foco em "Gestão e Governança em Biossegurança e Bioproteção", oferecido pelo Programa de Pós-gradução em Bioquímica Aplicada da Universidade Federal de Viçosa (UFV) em parceria com a Universidade da Força Aérea (UNIFA), com o Instituto de Biologia do Exército (IBEx) e com a *University of Texas Medical Branch* (UTMB, Galveston, EUA).

Estabelecimento de instituições nacionais, mecanismos operacionais e desenvolvimento de normativas adequadas ao contexto de biossegurança e bioproteção laboratorial

Atualmente, verificamos diversas comissões formalmente constituídas que atuam na gestão da biossegurança laboratorial em diferentes ministérios, tais como MS, MD e MAPA. No âmbito do MS, destaca-se a responsabilidade pela publicação da classificação dos grupos de risco dos patógenos de interesse para a saúde pública. Das atribuições do MD, destaca-se a análise das questões técnicas referentes à biossegurança, que visam a identificar seus impactos e suas correlações com a defesa biológica e a segurança nacional. A comissão do MAPA tem como diferencial a participação de representantes consultivos de outros órgãos, como GSI/PR, Abin, Centro Pan-Americano de Febre Aftosa (PANAFTOSA/OPAS-OMS), Polícia Federal (PF), MS e MD, e mantém como consultores externos um representante da Sociedade Brasileira de Biossegurança e Bioproteção (SB3), além de um especialista internacional da Organização das Nações Unidas para Alimentação e Agricultura (FAO).

Esta iniciativa do MAPA em criar uma comissão com representação interinstitucional, além de consultores especialistas externos, tem trazido enormes benefícios, especialmente por possibilitar a integração do corpo técnico especializado

em biossegurança e bioproteção dos diferentes órgãos em suas diferentes abordagens, demandas e interesses. Este formato pode ser considerado um modelo para a criação de uma comissão nacional unificada.

Quanto à normatização de biossegurança e bioproteção, destacam-se as iniciativas da Associação Brasileira de Normas Técnicas (ABNT). Neste sentido, foram criados, nos últimos anos, os seguintes comitês encarregados pela revisão ou pela elaboração de normas técnicas na referida área: ABNT/CB-032 – Equipamentos de Proteção Individual; ABNT/CB-036 – Análises Clínicas e Diagnóstico *In Vitro*; ABNT/CB-046 – Áreas Limpas e Controladas (encarregado pela elaboração de requisitos para Áreas Biocontidas); ABNT/CEE-129 – Resíduos de Serviços de Saúde; ABNT/CEE-138 – Equipamento para Limpeza de Ar e Outros Gases; ABNT/CEE-244 – Biossegurança e Bioproteção; ABNT/CEE-276 – Comissão de Estudo Especial de Biotecnologia.

No tocante à regulação do tema, há que considerar o arcabouço legal vigente no país e que inclui diversas legislações específicas (Quadro 2).

Quadro 2 - Principais legislações brasileiras vigentes relacionadas à biossegurança e à bioproteção

Normativa	Escopo
Decreto nº 77.374/1976 (BRASIL, 1976)	Promulga a Convenção sobre a Proibição do Desenvolvimento, Produção e Estocagem de Armas Bacteriológicas (Biológicas) e à Base de Toxinas e sua Destruição
Lei nº 11.105/2005 (BRASIL, 2005a)	Estabelece normas de segurança e mecanismos de fiscalização sobre construção, cultivo, produção, manipulação, transporte, transferência, importação, exportação, armazenamento, pesquisa, comercialização, consumo e liberação no meio ambiente e descarte de OGM e seus derivados no país
Decreto nº 5.591/2005 (BRASIL, 2005b)	Regulamenta dispositivos da Lei nº 11.105 de 2005
Decreto nº 5.705/2006 (BRASIL, 2006)	Promulga o Protocolo de Cartagena sobre Biossegurança da Convenção sobre Diversidade Biológica
Lei nº 12.305/2010 (BRASIL, 2010a)	Institui a Política Nacional de Resíduos Sólidos
Portaria MS nº 3.204/2010 (BRASIL, 2010b)	Aprova Norma Técnica de Biossegurança para Laboratórios de Saúde Pública
Instrução Normativa MAPA nº 5/2012 (BRASIL, 2012a)	Estabelece o regulamento técnico de biossegurança para manipulação do vírus da febre aftosa
Decreto nº 7.722/2012 (BRASIL, 2012b)	Dispõe sobre a execução no território nacional das Resoluções nº 1540 (2004) e nº 1977 (2011), adotadas pelo Conselho de Segurança das Nações Unidas, as quais dispõem sobre o combate à proliferação de armas de destruição em massa e sobre a vigência do Comitê 1540
Portaria Normativa nº 585/2013 (BRASIL, 2013)	Aprova as diretrizes de biossegurança, bioproteção e defesa biológica do MD
Resolução RDC Anvisa/MS nº 20/2014 (BRASIL, 2014)	Dispõe sobre regulamento sanitário para o transporte de material biológico humano
Portaria GM/MS nº 3398 (BRASIL, 2021)	Aprova a classificação de risco dos agentes biológicos e dá outras providências.
Decreto nº 11.200 (2022)	Aprova o Plano Nacional de Segurança de Infraestruturas Críticas

Fonte: elaborado pelos autores

Verifica-se que a legislação nacional apresenta algumas lacunas, tais como: indefinição de uma autoridade máxima que regule o tema no país; ausência de critérios para comissionamento, certificação e autorização de funcionamento de laboratórios; ausência de critérios para realização de análises de risco em laboratórios de alta contenção; falta de obrigatoriedade da notificação de acidentes e incidentes em laboratórios de alta contenção biológica; falta de supervisão/auditagem dos laboratórios; ausência de requisitos construtivos para laboratórios de alta contenção; falta de publicação de uma lista abrangente de grupos de risco de patógenos de interesse para saúde, agricultura, pecuária e biodefesa; indefinição quanto a requisitos mínimos de capacitação; e, finalmente, internalização de normativas internacionais.

Fortalecimento da expertise para apoiar a implementação de um sistema regulatório adequado para instalações de alta e máxima contenção biológica

A atuação de comissões, academia e outras instituições de pesquisa, sociedades técnico-científicas e outras organizações tem sido fundamental para o fortalecimento da cultura de biossegurança e bioproteção no Brasil e, consequentemente, para a capacitação de profissionais que venham a contribuir para a implementação de um sistema regulatório adequado.

De algumas destas iniciativas adotadas nos últimos anos para a promoção de conhecimento em nosso país, destacamos: organização, pelo MD, de três seminários, de 2012 a 2017, que promoveram o debate sobre biossegurança e bioproteção em grandes eventos (Copa do Mundo, Jogos Olímpicos, Jogos Pan Americanos e Jornada Mundial da Juventude Católica); apoio na organização e no recebimento do *18th International Veterinary Biosafety Working Group* no Laboratório Federal de Defesa Agropecuária (LFDA-MG/MAPA), no ano de 2017; organização de seminários e simpósios pelo MS, especialmente nos anos de 2017 e 2018; participação na organização dos workshops promovidos pelo *Grupo Iberoamericano de Bioseguridad* (BIOGIB), do qual o Brasil é sócio fundador e atualmente ocupa a vice-presidência; organização de webinários pela Sociedade Brasileira de Biossegurança e Bioproteção (SB3) a partir de 2021; oferecimento continuado de disciplinas de pós-graduação com foco em biossegurança por diferentes universidades e instituições de ensino e pesquisa instalados no país. Para as diferentes iniciativas mencionadas acima, cabe destacar a participação frequente de especialistas internacionais, oriundos de instituições de referência mundialmente reconhecidas.

A instituição dos GTs pelo GSI/PR mencionados anteriormente,

representou, por si só, um incentivo para o desenvolvimento das capacidades técnicas sobre o tema. Exemplo disso foi a promoção do "Seminário Internacional – Laboratório Nacional de Máxima Contenção Biológica", organizado pelo GT NB4 e que contou com 19 palestrantes reconhecidos internacionalmente na área da biossegurança e da bioproteção associados a laboratórios NB-4 provenientes de oito países (BRASIL, 2021). Esse evento, primeiro deste nível realizado na América Latina, veio a demonstrar a transparência e o interesse do governo brasileiro no assunto.

Apesar destes avanços, a ausência de um ente central que assuma a responsabilidade pela coordenação das ações relacionadas à biossegurança e à bioproteção laboratorial nos mais diferentes níveis e áreas de atuação, dificulta o estabelecimento de um "Programa Nacional de Capacitação", que poderia prever o oferecimento regular de cursos com um currículo básico padronizado e estruturado para atender demandas específicas e contemplar cursos de formação básica de diferentes profissionais em biossegurança e bioproteção laboratorial (gestores, supervisores de biossegurança, pesquisadores, profissionais de manutenção e engenharia etc.) em formato *online.* Uma das vantagens desta proposta seria a geração de um cadastro de profissionais minimamente capacitados para atuar na área, além da constituição de uma rede de profissionais especializados, o que facilitaria o intercâmbio de informações e outras iniciativas de colaboração mútua.

Outro aspecto a ser considerado neste item é a falta de regulamentação profissional ou capacitação mínima exigida para atuação na rotina de laboratórios de alta e máxima contenção biológica. Atualmente, a função de supervisor de biossegurança desses laboratórios é exercida por profissionais de diversas formações, sem certificação oficialmente reconhecida, sem comprovação de bagagem acadêmica nem experiência profissional que abranjam o conhecimento e a experiência mínimos necessários, conforme preconizado pelos regulamentos e recomendações internacionais da área.

Implementação e cumprimento dos regulamentos

Espera-se que, a partir da publicação da PNBB e da elaboração pelo MS do Plano Setorial de Segurança de Infraestruturas Críticas para Biossegurança e Bioproteção, conforme previsto no Decreto nº 11.200/2022 (BRASIL, 2022b), o país avance satisfatoriamente na construção de um arcabouço normativo mais abrangente e adequado à complexidade do tema. Estratégias que podem ser adotadas no decorrer destes trabalhos abarcam as seguintes etapas: (a) criação de um GT multidisciplinar e interinstitucional responsável por estudar lacunas no

arcabouço legal; (b) avaliação da legislação de outros países que tratam do tema e de eventuais sobreposições ou conflitos em regulamentos publicados por diferentes órgãos nacionais; (c) internalização de recomendações preconizadas em manuais e normas publicados por organismos de referência internacional, além dos acordos estabelecidos por meio de convenções, protocolos, acordos, resoluções e tratados multilaterais; (d) padronização de listas nacionais de classificação de risco de patógenos, sejam estes de importância para a saúde humana, animal ou vegetal; (e) padronização de critérios para qualificação/verificação/certificação de equipamentos críticos como autoclaves, cabines de segurança biológica, eclusas, sistemas de descontaminação de efluentes etc.; (f) padronização de conteúdo mínimo a ser abordado nas avaliações de risco; (g) constituição de uma Comissão Técnica com ampla representatividade (nos moldes da CTNBio), com competência para publicar manuais, notas e comunicados técnicos e resoluções normativas com abrangência nacional; (h) definição de uma sistemática para revisão periódica da legislação e manuais técnicos de referência, bem como de ferramentas para sua divulgação; (i) criação de uma Comissão Técnica multidisciplinar, responsável pela realização de auditorias com foco em biossegurança e bioproteção; (j) definição de uma sistemática para certificação de laboratórios, com reavaliações periódicas.

Estabelecimento de redes para intercâmbio de informações e parcerias internacionais

A iniciativa mais concreta que ocorreu, no nível central, no sentido de se constituir uma rede de laboratórios de alta contenção foi a instituição do Sistema Nacional de Infraestruturas de Pesquisa com Biossegurança (SISNIPE-BIO MCTI) (BRASIL, 2022a). A gestão deste sistema caberá ao MCTI, porém, como os trabalhos estão em fase de implantação, ainda não se sabe ao certo qual será sua abrangência. A ausência de um monitoramento oficial traz incertezas até mesmo em relação ao quantitativo de laboratórios de alta contenção instalados no Brasil e a situação operacional de cada um deles. Muitas vezes, o nível de biossegurança é definido pelo próprio coordenador do laboratório ou pela empresa responsável por sua construção, sem uma avaliação externa e imparcial, como a que ocorreu, por exemplo, nos LFDAs de SP e MG, que foram certificados por especialista da FAO em Gestão de Riscos Biológicos. Dos laboratórios de alta contenção biológica instalados no país, estes foram os únicos com reconhecimento e certificação oficial quanto a padrões internacionais de biossegurança e bioproteção. Neste contexto, Mafra (2020) relacionou os laboratórios de alta contenção biológica ligados aos diferentes órgãos públicos e instituições privadas nacionais, e ressaltou a possibilidade de

erros eventuais na classificação quanto ao nível operacional em que se encontra cada uma das instalações listadas e quanto à inclusão indevida ou mesmo não inclusão de estruturas equivalentes. O autor destacou a provável existência de outras estruturas NB-3 e NBA-3 não identificadas em operação em instituições públicas e privadas, porém sem registro oficial em uma agência ou sistema central. Essa situação havia sido previamente reconhecida em publicação acadêmica, com a afirmativa de que "o governo federal brasileiro desconhece o número total de laboratórios que atuam no país, bem como os agentes biológicos neles manipulados" (COELHO, 2017).

Desta maneira, temos que, sem a constituição formal de uma Rede Nacional, faltam mecanismos para manter um sistema de informações não somente a respeito das estruturas existentes, como, também, sobre a capacitação de seus colaboradores, registros e procedimentos frente a incidentes e acidentes, condições de armazenamento, inventário e transporte de patógenos trabalhados, métodos disponíveis para diagnóstico e produção de imunorreagentes, pesquisas em andamento, condições de bem-estar animal, periodicidade de manutenções etc.

A ausência dessas informações devidamente organizadas, documentadas e prontamente disponíveis dificulta o desenvolvimento de uma estratégia nacional para a identificação de fragilidades estruturais, de oportunidades de parceria, de lacunas para diagnóstico e pesquisas de interesse do Governo, o que dificulta a aplicação adequada dos recursos públicos e mesmo o delineamento de planos de contingenciamento e o enfrentamento de eventuais emergências (ZHIMING, 2019).

Revisão de desempenho e adequação ao contexto nacional dos laboratórios de alta contenção biológica

A partir da publicação da PNBB, deve-se pensar no estabelecimento de um mecanismo de avaliação de sua implementação, de acordo com as premissas do ciclo PDCA (*Plan, Do, Check and Act*), o que será possível mediante a criação de comissões técnicas multidisciplinares e interministeriais e/ou outras estruturas centralizadas, com condições de atuar em diferentes órgãos e esferas de governo. Tais estruturas deverão fazer uso de ferramentas de gestão que permitam a identificação de vulnerabilidades e, consequentemente, o planejamento de ações para sua mitigação, assim como a identificação de oportunidades para o aprimoramento da infraestrutura da biossegurança no país como um todo.

Como exemplo, podemos mencionar a Chamada Pública MCTI/FINEP/ Infraestrutura NB-3, publicada em julho de 2020, cujo objetivo foi:

> Selecionar propostas para apoio financeiro à execução de projetos institucionais para adequação/implantação de infraestrutura física de Laboratórios e Biotérios de Nível de Biossegurança 3 (NB-3) destinados à Pesquisa e Desenvolvimento para o desenvolvimento de vacinas, tratamentos e estudos da patogênese do vírus SARS-CoV2 e outras viroses emergentes e reemergentes.

Iniciativas como essa são sempre muito bem-vindas, ainda mais no contexto urgente do enfrentamento da pandemia da COVID-19, porém, certamente os objetivos poderiam ser alcançados de forma mais assertiva se o país já tivesse definido previamente sua PNBB, bem como implementado ferramentas para sua gestão.

Considerações finais

Podemos afirmar que o Brasil implementou, de forma bastante satisfatória, as recomendações internacionais emanadas a partir do Protocolo de Cartagena a respeito da utilização e da realização de pesquisas relacionadas a OGMs. Entretanto, a PNB não contempla aspectos relacionados a biossegurança e bioproteção laboratorial para situações que não se relacionam especificamente a OGMs e células-tronco. Logo, ao se analisar as recomendações da OMS para implementação dos requisitos regulatórios para o tema (OMS, 2020), foi possível identificar avanços e algumas lacunas que merecem atenção.

Os maiores avanços se deram a partir da criação de três GTs interministeriais e multidisciplinares para avaliar e definir questões fundamentais relacionadas à biossegurança e à bioproteção laboratorial, assim como a aprovação do Plano Nacional de Segurança de Infraestruturas Críticas. Espera-se que, com a continuidade desses trabalhos algumas lacunas venham a ser preenchidas, a partir das seguintes iniciativas, entre outras: estabelecimento de modelo de fomento a ensino, pesquisa, desenvolvimento tecnológico e inovação relacionados ao tema; incremento do arcabouço legal e normativo; implementação de um "Programa Nacional de Capacitação" em biossegurança e bioproteção laboratorial; criação e monitoramento de uma "Rede Nacional de Laboratórios de Alta Contenção"; desenvolvimento de um planejamento estratégico que inclua a definição da infraestrutura desejável para o país no tocante ao quantitativo e aos níveis de biossegurança dos laboratórios; definição de mecanismos para certificação de laboratórios de alta contenção biológica; e coordenação de ações de colaboração nos níveis nacional e internacional.

Também é questão fundamental a necessidade de se identificar os recursos financeiros necessários para a implementação destas ações. Reforçamos as recomendações de que o incremento da biossegurança e da bioproteção laboratorial seja tratado como prioritário, por ser área estratégica e crítica, de que sua condução continue com Governo Federal e órgãos vinculados, e de que ela não seja afetada por

cortes orçamentários lineares e, tampouco, seja transferida ao setor privado, uma vez que serviços relacionados ao diagnóstico e à pesquisa da manipulação de agentes biológicos de elevado risco representam ameaças importantes não somente à saúde pública, como também à biodefesa, ao agronegócio e, consequentemente à segurança nacional.

Referências

BRASIL. *Decreto nº 11.200*, de 15 de setembro de 2022. Aprova o Plano Nacional de Infraestruturas Críticas. Brasília, DF: Presidência da República, 2022b. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11200.htm. Acesso em 4 out. 2022.

BRASIL. *Portaria do Ministério da Ciência, Tecnologia e Inovações nº. 6.212*, de 17 de agosto de 2022. Institui o Sistema Nacional de Infraestruturas de Pesquisa com Biossegurança (SISNIPE-BIO MCTI), no âmbito do Ministério da Ciência, Tecnologia e Inovações. Brasília, DF: MCTI, 2022a. Disponível em: https://antigo.mctic.gov.br/mctic/opencms/legislacao/portarias/Portaria_MCTI_n_6212_de_17082022.html. Acesso em 4 out. 2022.

BRASIL. *Portaria do Ministério da Saúde nº 3.398*, de 07 de dezembro de 2021. Aprova a Classificação de Risco dos Agentes Biológicos e dá outras providências. Brasília, DF: MS, 2021. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2021/prt3398_29_12_2021.html. Acesso em 25 set. 2023.

BRASIL. *Resolução do Gabinete de Segurança Institucional da Presidência da República nº. 7*, de 20 de agosto de 2020. Dispõe sobre os Grupos Técnicos da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo. Brasília, DF: GSI/PR, 2020. Disponível em: https://in.gov.br/web/dou/-/resolucao-gsi/pr-n-7-de-20-de-agosto-de-2020-273467871. Acesso em 4 out. 2022.

BRASIL. *Portaria nº 53*, de 4 de julho de 2018. Constitui, no âmbito da CREDEN, Grupo de Trabalho de Biossegurança e Bioproteção. Brasília, DF: GSI/PR, 2018. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/31548323/do1-2018-07-16-portaria-n-53-de-4-de-julho-de-2018-31548279. Acesso em 4 out. 2022.

BRASIL. *Resolução de Diretoria Colegiada – RDC da ANIVSA nº 20,* de 10 de abril de 2014. Dispõe sobre regulamento sanitário para o transporte de material biológico humano. Brasília, DF: ANVISA/MS, 2014. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/anvisa/2014/rdc0020_10_04_2014.pdf. Acesso em 4 out. 2022.

BRASIL. *Portaria Normativa do Ministério da Defesa nº. 585*, de 7 de março de 2013. Aprova as Diretrizes de Biossegurança, Bioproteção e Defesa Biológica do Ministério da Defesa. Brasília, DF: MD, 2013. Disponível em: https://www.in.gov.br/materia/-/

asset_publisher/Kujrw0TZC2Mb/content/id/30415391/do1-2013-03-11-portaria-normativa-n-585-md-de-7-de-marco-de-2013-30415387-30415387. Acesso em 4 out. 2022.

BRASIL. *Decreto nº 7.722*, de 20 de abril de 2012. Dispõe sobre a execução no Território Nacional das Resoluções nº 1540 (2004), e nº 1977 (2011), adotadas pelo Conselho de Segurança das Nações Unidas em 28 de abril de 2004 e em 20 de abril de 2011, as quais dispõem sobre o combate à proliferação de armas de destruição em massa e sobre a vigência do Comitê 1540. Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7722.htm. Acesso em 4 out. 2022.

BRASIL. *Instrução Normativa da Secretaria de Defesa Agropecuária nº 5*, de 28 de março de 2012. Estabelece o regulamento técnico de biossegurança para manipulação do Vírus da Febre Aftosa. Brasília, DF: MAPA, 2012. Disponível em: https://www.legisweb.com.br/legislacao/?id=239761. Acesso em 4 out. 2022.

BRASIL. *Portaria do Ministério da Saúde nº 3.204, de 20 de outubro de 2010*. Aprova Norma Técnica de Biossegurança para Laboratórios de Saúde Pública. Brasília, DF: MS, 2006. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2010/prt3204_20_10_2010.html. Acesso em 4 out. 2022.

BRASIL. *Lei nº 12.305*, de 2 de agosto de 2010. Institui a Política Nacional de Resíduos Sólidos; altera a Lei n º 9.605, de 12 de fevereiro de 1998; e dá outras providências. Brasília, DF: Presidência da República, 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/l12305.htm. Acesso em 4 out. 2022.

BRASIL. *Decreto nº 5.705*, de 16 de fevereiro de 2006. Promulga o Protocolo de Cartagena sobre Biossegurança da Convenção sobre Diversidade Biológica. Brasília, DF: Presidência da República, 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/decreto/d5705.htm. Acesso em 4 out. 2022.

BRASIL. *Decreto nº 5.591*, de 22 de novembro de 2005. Regulamenta dispositivos da Lei nº 11.105, de 24 de março de 2005, que regulamenta os incisos II, IV e V do § 1º do art. 225 da Constituição, e dá outras providências. Brasília, DF: Presidência da República, 2005. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5591.htm. Acesso em 4 out. 2022.

BRASIL. *Lei nº 11.105*, de 24 de março de 2005. Regulamenta os incisos II, IV e V do

§ 1º do art. 225 da Constituição Federal, estabelece normas de segurança e mecanismos de fiscalização de atividades que envolvam organismos geneticamente modificados – OGM e seus derivados, cria o Conselho Nacional de Biossegurança – CNBS, reestrutura a Comissão Técnica Nacional de Biossegurança – CTNBio, dispõe sobre a Política Nacional de Biossegurança – PNB, revoga a Lei nº 8.974, de 5 de janeiro de 1995, e a Medida Provisória nº 2.191-9, de 23 de agosto de 2001, e os arts. 5º, 6º, 7º, 8º, 9º, 10 e 16 da Lei nº 10.814, de 15 de dezembro de 2003, e dá outras providências. Brasília, DF: Presidência da República, 2005a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/lei/l11105.htm. Acesso em 4 out. 2022.

BRASIL. *Decreto nº 77.374*, de 1º de abril de 1976. Promulga a Convenção sobre a Proibição do Desenvolvimento, Produção e Estocagem de Armas Bacteriológicas (Biológicas) e à Base de Toxinas e sua Destruição. Brasília, DF: Presidência da República, 1976. Disponível em: https://www2.camara.leg.br/legin/fed/decret/1970-1979/decreto-77374-1-abril-1976-426054-publicacaooriginal-1-pe.html. Acesso em 4 out. 2022.

CARDOSO, Telma Adalla de Oliveira; NAVARRO, Marli B. M. de Albuquerque *et alii.* Health surveillance, biosafety and emergence and re-emergence of infectious diseases in Brazil. *The Brazilian Journal of Infectious Diseases*, v. 14 (5), p. 526-535, 2010.

CAVALCANTE, Pedro. *Gestão Pública Contemporânea*: do movimento gerencialista ao Pós-NPM. Brasília e Rio de Janeiro: Instituto de Pesquisa Econômica Aplicada, 2017.

CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS- CGEE. *Seminário internacional Laboratório Nacional de Máxima Contenção Biológica (LNMCB)* Relatório final. Brasília, DF. CGEE, 2021 72 p.

CICERO, Anita; MEYER, Diane *et alii*. Southeast Asia Strategic Multilateral Dialogue on Biosecurity. *Emerging Infectious Diseases*, v. 25 (5), p. 5-10, 2019.

COELHO, Danilo Nery. *Emergências em saúde pública por eventos químicos, biológicos, radiológicos e nucleares (QBRN) na perspectiva da inteligência estratégica*: recomendações em prol da intersetorialidade na segurança da saúde e na biodefesa. Dissertação (Mestrado). Fundação Oswaldo Cruz, Brasília, DF, 2017.

FONTOURA, Yuna; GUEDES, Ana Lucia. Governança global e transferência de política: influências do Protocolo de Cartagena na Política Nacional de Biossegurança. *Revista de Administração Pública*, v. 47 (1), p. 3-23, 2013.

KISSLER, Leo; HEIDEMANN, Francisco. G. Governança pública: novo modelo regulatório para as relações entre Estado, mercado e sociedade? *Revista de Administração Pública*, v. 40 (3), p. 479-499, 2006.

MAFRA, Claudio. *Pensando uma infraestrutura estratégica nacional*: o laboratório NB-4 brasileiro. Visconde do Rio Branco, MG: Suprema Gráfica, 2020.

MORENS, David M.; FAUCI, Anthony S. Emerging Pandemic Diseases: How We Got to COVID-19. *Cell*, v. 182, p. 1077-1092, 2020.

OMS. *World Health Assembly, 58. Enhancement of laboratory biosafety*. Organização Mundial da Saúde, Genebra, 2005.

OMS. *Guidance on implementing regulatory requirements for biosafety and biosecurity in biomedical laboratories* - a stepwise approach. Organização Mundial da Saúde, Genebra, 2020.

PASTORINO, Boris; LAMBALLERIE, Xavier *et alii*. Biosafety and Biosecurity in European Containment Level 3 Laboratories: Focus on French Recent Progress and Essential Requirements. *Frontiers in Public Health*, 2017. Disponível em: https://doi:10.3389/fpubh.2017.00121. Acesso em 4 out. 2022.

U.S. GOVERNMENT. *Biosafety in Microbiological and Biomedical Laboratories*. Atlanta e Bethesda: U.S. Department of Health and Human Services, 2020.

ZHIMING, Yuan. Current status and future challenges of high-level biosafety laboratories in China. *Journal of Biosafety and Biosecurity*, v. 1, n.2 p. 123-127, Elsevier, 2019.

Artigo

2

GEOECONOMIA E SEGURANÇA ECONÔMICA
A Inteligência e a Contrainteligência Econômicas na logística e mobilização nacional *

DOI: https://doi.org/10.58960/rbi.2023.18.224

Kael Weingartner Chagas **
Peter Loeb Caldenhof ***

Resumo

Este artigo explora, sob a perspectiva da Geoeconomia e da Segurança Econômica do Brasil, as funções e especificidades da Inteligência Econômica e da Contrainteligência Econômica e suas aplicações no âmbito da Logística e Mobilização Nacional (LMN). A análise demonstra que as relações de poder e as disputas econômicas entre Estados e organizações definem os problemas abordados pela Inteligência Econômica e as ameaças específicas que a Contrainteligência tem de combater, seja no contexto de guerra econômica global, seja na lógica da economia de guerra e da continuidade das atividades produtivas e de abastecimento. Por fim, o texto explora as sinergias e limites da combinação de ambos os ramos da Inteligência na produção e na proteção de conhecimentos estratégicos e de infraestruturas críticas.

Palavras-chave: geoeconomia; segurança econômica; Inteligência Econômica; Contrainteligência; Logística e Mobilização Nacional.

GEOECONOMY AND ECONOMIC SECURITY
Economic Intelligence and Counterintelligence in Logistics and National Mobilization

Abstract

This paper explores, from a geoeconomic perspective of the Economic Security in Brazil, the functions and specificities of the Economic Intelligence and the Economic Counterintelligence and their applications in the scope of Logistics and National Mobilization (LNM). The analysis demonstrates that power relations and economic disputes between States and organizations define the problems addressed by Economic Intelligence and the specific threats that Counterintelligence must fight, whether in the context of global economic warfare, or in the logic of a war economy and the continuity of production and supply activities. Finally, the text explores the synergies and limits of combining both branches of Intelligence in the production and protection of strategic knowledge and critical infrastructures.

---

* Este artigo é resultado de pesquisa realizada no âmbito do Curso de Logística e Mobilização Nacional (CLMN) da Escola Superior de Defesa (ESD), sob orientação do Professor Doutor Ivan Carlos Soares de Oliveira.

** Graduado em Ciências e Tecnologia e em Engenharia de Petróleo pela Universidade Federal do Rio Grande do Norte (UFRN). Pós-graduado em Logística e Mobilização Nacional pela Escola Superior de Defesa (ESD). Servidor Público Federal.

*** Bacharel em Direito pela Universidade de São Paulo (USP). Pós-graduado em Logística e Modais de Transportes pela AVM Educacional, em Economia Brasileira Contemporânea pela Faculdade Método de São Paulo (FAMESP) e em Logística e Mobilização Nacional pela Escola Superior de Defesa (ESD). Mestre em Desenvolvimento Socioeconômico pela Universidade Federal do Maranhão (UFMA). Analista vinculado à Casa Civil/PR.

Keywords: *geoeconomy; economic security; Economic Intelligence; Counterintelligence; Logistics and National Mobilization.*

GEOECONOMÍA Y SEGURIDAD ECONÓMICA
La Inteligencia y la Contrainteligencia Económicas en la logística y movilización nacional

Resumen

Este artículo explora, desde la perspectiva de la Geoeconomía y de la Seguridad Económica en Brasil, las funciones y especificidades de la Inteligencia Económica y de la Contrainteligencia Económica y sus aplicaciones en el ámbito de la Logística y Movilización Nacional (LMN). El análisis demuestra que las relaciones de poder y las disputas económicas entre Estados y organizaciones definen los problemas que aborda la Inteligencia Económica y l las amenazas específicas que tiene que combatir la Contrainteligencia, ya sea en el contexto de la guerra económica global, o en la lógica de la economía de guerra y de la continuidad de las actividades productivas y de abastecimiento. Por último, el texto explora las sinergias y límites de combinar ambas ramas de la Inteligencia en la producción y protección de conocimientos estratégicos e infraestructuras crítica.

Palabras clave: *geoeconomía; seguridad económica; Inteligencia Económica; Contrainteligencia; Logística y Movilización Nacional.*

Introdução

O mundo atual é marcado pela continuidade das disputas políticas, militares e econômicas entre Estados e poderosos atores não estatais, em uma "condição sistemática de instabilidade dos relacionamentos entre os países e a emergência de novas ameaças no cenário internacional" (BRASIL, 2020, p. 7). Ao mesmo tempo em que a globalização acarretou uma enraizada interdependência entre países, economias e sociedades, essa competição por poder não descarta as relações de força e de imposição de vontade nas relações internacionais (KHANNA, 2016; OLIER, 2012; BRASIL, 2020). "O conflito prossegue, mesmo num mundo de interdependência. Como as coligações são mais complexas e são utilizadas diferentes formas de poder, os conflitos são como jogar xadrez em vários tabuleiros ao mesmo tempo" (NYE, 2002, p. 224).

Esse xadrez multidimensional e com vários jogadores impõe aos países a necessidade de uma visão estratégica de desenvolvimento para enfrentarem a competição mais instável e imprevisível em um ambiente definido por profundas e constantes transformações de suas conjunturas e estruturas internas e internacionais (BRASIL, 2020; BRASIL, 2017). Os diversos tabuleiros e atores do jogo são apenas parcialmente visíveis através de uma névoa de opacidade, indisponibilidade e incerteza das informações, o que aumenta os riscos de erros e reduz as chances de êxito das políticas nacionais (FINGAR, 2011). Do mesmo modo, a própria informação é disputada em um tabuleiro transversal, em que os serviços de Inteligência competem pela capacidade de compreensão sistêmica do jogo como um todo[1], ao mesmo tempo em que protegem seus próprios segredos (BRITO, 2011; POTTER, 1998).

Nesse cenário político e geoeconômico, um dos campos fundamentais de necessidade de embasamento do processo decisório estratégico é o da Logística e Mobilização Nacional (LMN), marcado por sua complexidade e pelas conexões das dimensões logístico-econômica e político-militar. Aqui, entende-se logística com um conceito amplo, que ultrapassa a definição estrita do âmbito empresarial e engloba toda a capacidade de manutenção e suprimento do país em situação de guerra ou grave crise, e inclui não apenas transportes, armazéns e infraestruturas correspondentes, mas questões como o abastecimento de energia elétrica, o setor de saúde e até as comunicações e motivação psicossocial. Mobilização, por sua vez, é a capacidade de transformação do potencial total do país em caso de agressão externa para suprir as necessidades que vão além da

1 Um dos papéis centrais da Inteligência Estratégica é alimentar o processo decisório e o planejamento estratégico com conhecimentos analíticos, percepções, cenários e estimativas. Entende-se aqui a estratégia como um método de pensamento que categoriza, prioriza e escolhe os meios mais eficazes para a consecução de objetivos em dadas circunstâncias. Não é um conceito apenas de ordem militar: inclui os domínios político, econômico, diplomático, entre outros, no que se denomina de estratégia total (BEAUFRE, 1998).

logística nacional existente, e envolve todo o processo de geração dessas capacidades, do planejamento à desmobilização (VIDEIRA, 2019; BRASIL, 1983; BRASIL, 2007).

Sob essa lógica, qual é o papel da Inteligência de Estado para a Segurança Econômica do Brasil? Com escopo mais específico, quais são as funções e especificidades das vertentes de Inteligência Econômica (IE) e Contrainteligência Econômica (Contra-IE) na seara da Logística e Mobilização Nacional (LMN)? E quais as implicações decorrentes para a Atividade de Inteligência no Brasil? Apesar da marcada relevância do problema sob a ótica da Segurança Nacional brasileira, a pesquisa acadêmica em IE e, sobretudo, de pesquisas com um tratamento conjunto de IE e Contra-IE, é particularmente escassa (RIBEIRO, 2016). Igualmente escassa é a literatura que trata o campo da LMN sob uma ótica estratégica de segurança econômica e da geoeconomia.

Assim, este artigo visa, sob o ponto de vista da Geoeconomia e da Segurança Econômica do Brasil, a explorar as funções e características definidoras da IE e da Contra-IE no âmbito da LMN, e as identificar e explicar a partir da natureza de seu objeto de atuação, *i.e.*, economia, logística, cadeias de suprimentos e mobilização. Por fim, exploram-se as conexões, sinergias e limites da IE e Contra-IE, especialmente ao se considerar que, no Brasil, são executadas pela mesma instituição de Estado, a Agência Brasileira de Inteligência (Abin), órgão central do Sistema Brasileiro de Inteligência (Sisbin) (BRASIL, 1999).

Marco teórico de referência

Nos termos da Política Nacional de Defesa (PND) de 2020 e da Estratégia Nacional de Defesa (END) de 2020, a Segurança Nacional[2]: "É a condição que permite a preservação da soberania e da integridade territorial, a realização dos interesses nacionais, a despeito de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais" (BRASIL, 2020, p. 78). A segurança do Estado e de sua sociedade é eminentemente política, mas composta de setores diversos, como a economia, o meio-ambiente, a cultura etc., que suportam essa estrutura política e a continuidade das sociedades nacionais e de seus membros (DCAF, 2015).

Para garantir a Segurança Nacional e a consecução de nossos interesses nacionais contra ameaças e vulnerabilidades externas e internas, essa diversidade de fatores deve ser articulada por uma Grande Estratégia ou pela Política de Segurança Nacional (RUDZIT e NOGAMI, 2010), que tem a segurança econômica como uma parte constituinte fundamental (POTTER,

2 Ao se adaptar às mudanças teóricas das últimas décadas e à Constituição Federal, o conceito trata a segurança do Estado e a segurança humana em conjunto (DCAF, 2012).

1998; RODRIGUEZ, 2011). Seja pela centralidade da manutenção da atividade econômica para o sustento da Defesa em tempos de paz e de guerra, seja pela utilização de instrumentos econômicos na competição estratégica em busca de poder e bem-estar de suas populações (NYE, 2002; FOLGADO, 2009), a economia tem de ser levada em conta nos cálculos estratégicos.

Por sua vez, a geoeconomia constitui a junção dos aspectos geopolíticos de poder, território e atores com a ótica da economia (OLIER, 2012), e reflete o deslocamento do campo da disputa para a esfera de produção e distribuição das bases materiais e de serviços essenciais à existência dos Estados e sociedades (FOLGADO, 2009; POTTER, 1998). Blocos e organizações econômicas, recursos naturais, finanças, pesquisa e desenvolvimento (P&D) e as conexões territoriais de logística e de cadeias de suprimentos (KHANNA, 2016), que funcionam como as artérias da complexa economia globalizada, assumem destaque para a Segurança e a Defesa nacionais (OLIER, 2012) e para o subsistema de LMN. Essas características do sistema internacional implicam a necessidade de provimento dos decisores com conhecimentos e estimativas que analisem os numerosos fatores, reduzam-nos a seus aspectos essenciais e expliquem a conjuntura em que as escolhas estratégicas têm de ser feitas (BEAUFRE, 1998; BRITO, 2011), ao mesmo tempo em que se mantém os adversários[3] no estado de incerteza, e se semeia dúvidas sobre nossas intenções (BEAUFRE, 1998).

O assessoramento informacional oportuno, amplo e seguro à formulação e à execução das estratégias de Estado, ou seja, o conhecimento posto ao serviço da tomada de decisões competitivas (OLIER, 2012) relacionadas a ameaças e oportunidades à Segurança Nacional, é a função precípua da Atividade de Inteligência de Estado (GONÇALVES, 2016; FINGAR, 2011) e está no cerne da efetividade das ações governamentais (BRASIL, 2017; CHUTER, 2011). No Brasil, a Atividade de Inteligência se divide em dois grandes ramos, a Inteligência e a Contrainteligência, definidos na Lei nº 9.883/1999, que instituiu o Sisbin e criou a Abin, e na Política Nacional de Inteligência (PNI)[4].

3 Outro aspecto fundamental é o caráter adversarial em que o conceito de estratégia é utilizado no contexto da Segurança Nacional e da Inteligência de Estado. O raciocínio estratégico pressupõe uma grande capacidade de análise e síntese em situação de incerteza, aprecia a realidade em transformação constante e procede sobre hipóteses (BEAUFRE, 1998; BRITO, 2011). A Inteligência Estratégica tem implicações a longo prazo, geralmente vinculadas a formulação de cenários prospectivos (ABRAIC *apud* GONÇALVES, 2018). Platt, ao enfatizar o aspecto de adversidade, considera "possibilidades, vulnerabilidades e linhas de ação prováveis das nações estrangeiras (...). Busca, principalmente, guiar a formulação e a execução de medidas de segurança nacional" (1974, p. 31).

4 Enfatiza-se a obtenção, a análise e a difusão de conhecimentos para o processo decisório nacional, a salvaguarda, a segurança da sociedade e do Estado brasileiros, bem como a neutralização da Inteligência adversa e a proteção de informações e instalações sensíveis (BRASIL, 1999; BRASIL, 2016).

Funções e especificidades da IE na lógica da geoeconomia e da segurança econômica

O estudo da Inteligência Econômica como ramo específico[5] da Inteligência de Estado toma corpo a partir do fim da Guerra Fria e da percepção de deslocamento da competição interestatal da esfera político-estratégica e militar para a seara econômica (CHUTER, 2011), inclusive entre aliados políticos (POTTER, 1998), com ênfase para o viés da guerra econômica, isto é, do conflito entre Estados e empresas por vantagens econômicas, financeiras e competitivas (POTTER, 1998; RIBEIRO, 2016). No entanto, a atividade de coleta, busca e análise de informações de natureza econômica e logística para problemas de segurança nacional é muito mais antiga, e consubstancia parte das informações estratégicas desde que grupos e Estados apresentam interesses conflitantes (PLATT, 1974; CHUTER, 2011; RIBEIRO, 2016; FOLGADO, 2009).

Diversos autores analisados por Ribeiro (2016) ressaltam o sentido da IE como instrumento de promoção do desenvolvimento econômico e social do país por meio de informações sobre atores, fatores, fenômenos e cenários de conteúdo econômico para a determinação da economia política dos Estados, e integra o planejamento econômico com as questões de segurança.

Em sua essência, a IE de Estado tem a mesma função de identificação de ameaças e antecipação de problemas e tendências para embasar o processo decisório governamental que a Inteligência Estratégica de Estado em geral (RIBEIRO, 2016; BRITO, 2011; SOUZA, 2018), mas diferencia-se pelo tipo de problemas e ameaças sob análise, isto é, a economia e a segurança econômica nacional (OLIER, 2012).

Concretamente, os problemas analisados pela IE dizem respeito aos processos de produção e distribuição de todos os bens e serviços que satisfazem as necessidades de indivíduos, organizações e Estados, e são elucidados com fundamento nas categorias técnico-científicas[6] das ciências econômicas e da geoeconomia. Dessa forma, uma especificidade da IE é a necessidade de boa compreensão da economia política e da teoria econômica pelas equipes de analistas (RIBEIRO, 2016), que viabilize sua interlocução com colaboradores, fontes e

5 Apesar de a Inteligência Econômica (IE) apresentar pontos de conexão com outros tipos de atividades de coleta e processamento analítico de informações, como a produção de conhecimentos técnicos setoriais e as Inteligências financeira, comercial e competitiva (Glossário de Inteligência Competitiva, ABRAIC *apud* GONÇALVES, 2018; FOLGADO, 2009), a IE de Estado constitui um ramo separado que se distingue dos demais por seu escopo estratégico de segurança nacional, seus clientes, métodos, meios e temas de análise específicos (SOUZA, 2018).

6 Tais quais oferta, demanda, renda, investimentos, estruturas de mercado, eficiência alocativa, custos de oportunidade e de transação, elasticidade, desenvolvimento, efeitos difusores, entre outras.

usuários dos conhecimentos[7]. Igualmente, o domínio da matéria pela equipe de IE possibilita a integração interdisciplinar dos conhecimentos de Inteligência e o surgimento de *insights* (PLATT, 1974; FINGAR, 2011).

De um ponto de vista da economia de guerra ou de crise, a IE visa a compreender e antecipar, à alta cúpula decisória, ameaças, oportunidades e vulnerabilidades econômicas e logísticas para a capacidade de os Estados sustentarem suas populações e suas expressões de Poder em tempos de crise ou de guerra (PLATT, 1974). Para isso, analisa fenômenos e tendências críticas de inflação, recessão, desabastecimento[8] de bens e insumos estratégicos, riscos de interrupção de cadeias produtivas ou de infraestruturas críticas, efeitos sistêmicos de crises financeiras[9], etc. Sob o aspecto da guerra econômica, objetiva, por sua vez, apoiar o setor produtivo de seus respectivos países, o que configura, por si só, uma vantagem econômica aos Estados em disputa (VIEIRA, 1999; RIBEIRO, 2016; OLIER, 2012).

Há questões mais específicas que definem a competitividade nacional ou apresentam potencial de afetar a segurança econômica dos países e que devem ser apreciados para a compreensão sistemática do entorno competitivo (OLIER, 2012). Vejam-se, exemplarmente, tópicos como os fluxos de capital, variações cambiais e de taxas de juros, avanços tecnológicos e científicos, comércio e investimentos internacionais, base industrial, competição interempresarial, condições fiscais, migrações, meio ambiente, crimes transnacionais, pandemias e seus respectivos impactos econômicos (POTTER, 1998; CHUTER, 2011). Ao se considerar o caráter essencialmente político e estratégico do olhar sobre a economia da IE, especial atenção tem de ser dada à possibilidade de utilização deliberada[10] dessas variáveis econômicas por governos ou grupos estrangeiros (DCAF, 2003; RICKARDS, 2009). Nesse contexto, a produção de conhecimentos de IE também precisa iluminar as capacidades e intenções de competidores, adversários, aliados e quaisquer atores relevantes nos sistemas econômicos global e nacional (POTTER, 1998).

Por fim, ressalta-se que essa apreciação política da análise das relações de poder e das estratégias econômicas dos Estados e de seus grupos econômicos (OLIER, 2012) tem de incluir também os aspectos espaciais e territoriais da ótica

7 Um sistema coordenado de Inteligência Econômica com a participação de entes públicos e privados é considerado pela literatura como uma característica fundamental da Inteligência Econômica na comparação com outras áreas da Inteligência de Estado (POTTER, 1998; RIBEIRO, 2016; FOLGADO, 2009, SOUZA, 2018).

8 Para o caso brasileiro, um objeto de interesse estratégico especial são as condições de segurança energética ligadas à produção *offshore* de hidrocarbonetos em caso de uma Mobilização Nacional (COSTA e GÓES, 2023).

9 Destaca-se o papel dos índices de risco soberano, que podem servir como sensores de IE (BRANCO, 2017).

10 Ressalta-se aqui o *Lawfare, i.e.*, a condução da guerra econômica por meios jurídicos como ações de especial interesse da IE e Contra IE, mas que ultrapassam o escopo deste trabalho e merecem aprofundamento específico.

geoeconômica, em que se destacam as cadeias de suprimentos globais e seus elos regionais e locais (RODRIGUEZ, 2011; KHANNA, 2016), as condições e potenciais das economias estrangeiras, as tendências econômicas mundiais, bem como a obtenção de Inteligência para apoiar as negociações comerciais do país (DCAF, 2003). A proteção das próprias economias, o acesso a matérias primas industriais e energéticas, à água e a alimentos, assim como o domínio de tecnologiaschave e a conquista de mercados e produtos sensíveis não ocorrem em um vácuo, mas no mundo concreto de Estados territoriais, que utilizam tais fatores como elementos de projeção internacional e de reforço do próprio potencial econômico e social (OLIER, 2012).

Assim, sob o ponto de vista da geoeconomia e da segurança econômica, e diferentemente dos trabalhos econômicos técnicos[11] de órgãos como o Instituto de Pesquisas Econômicas Aplicadas (IPEA) e o Banco Nacional de Desenvolvimento Econômico e Social (BNDES), a produção de conhecimentos da IE no Brasil integra transversal e interdisciplinarmente os fundamentos das ciências econômicas e da economia política com conhecimentos de ordem geopolítica, social e militar (OLIER, 2012; BRITO, 2011; SOUZA, 2018), baseados em dados obtidos em fontes abertas ou com meios especializados de acesso a dados negados, normalmente com tratamento sigiloso.

Funções e especificidades da Contrainteligência Econômica

Segundo a PNI, as peculiaridades dos atuais cenários nacional e internacional induzem a Atividade de Inteligência a redefinir suas prioridades em prol de questões como as econômico-comerciais e científico-tecnológicas. Para impedir que serviços de Inteligência estrangeiros se envolvam em atividades clandestinas direcionadas a interesses econômicos e comerciais, faz-se necessário o desenvolvimento de ações defensivas, como as de proteção dos conhecimentos sensíveis e das infraestruturas críticas nacionais (POTTER org., 1998). O desenvolvimento dessas ações e a contraposição a essas ameaças são funções precípuas da Contrainteligência.

A Contrainteligência tem os objetivos de fazer frente à Inteligência adversa e salvaguardar os ativos, interesses e conhecimentos sensíveis do país. Suas ações se contrapõem às ações de Inteligência ofensiva, e protegem o país contra ameaças como a espionagem, a interferência externa, o terrorismo, a sabotagem e o vazamento de informações. No contexto da Inteligência de Estado, o propósito da Contrainteligência é proteger o Estado e a

11 A capilaridade nacional e internacional da Abin, aliada ao amplo horizonte de suas diversas áreas de coleta e análise, formam um diferencial para este tipo de integração informacional e para o estabelecimento de conexões entre os aspectos técnicos da economia com o escopo da segurança do Estado e da sociedade.

sociedade, e seus segredos, contra outros Estados e organizações (BRUNEAU, 2000). Dessa forma, contribui para a salvaguarda do patrimônio nacional de áreas consideradas de interesse estratégico para a segurança e o desenvolvimento nacional, a partir de ações de sensibilização, capacitação, avaliações de risco, operações de Inteligência e outras ações especializadas. Na esfera da segurança econômica, a Contra IE é o ramo da Contrainteligência que se contrapõe às ações adversas que visam a prejudicar a competitividade econômica do Estado, bem como a proteger as tecnologias sensíveis e ativos estratégicos das cadeias produtivas do país.

No Brasil, a atuação da Inteligência com enfoque na Contra IE costuma estar vinculada a ações de Contrainteligência em sentido amplo, visto que o viés econômico dificilmente se separa das outras ameaças que exigem atuação da Contrainteligência de Estado. Apesar disso, outros países já possuem programas específicos nesse ramo. O Departamento Federal de Investigação dos Estados Unidos (FBI), por exemplo, possui um programa de Contra-IE desde 1994, com o objetivo de coletar informações e engajar em atividades para detectar e neutralizar ameaças e atividades patrocinadas ou coordenadas por potências estrangeiras dirigidas contra os interesses econômicos dos Estados Unidos, especialmente atos de espionagem econômica (FRAUMANN, 1997).

No atual contexto geoeconômico global, deparamo-nos com a existência de Inteligências Econômicas agressivas com grande capilaridade de aquisição de Inteligência de fontes humanas, aptidão técnica sem precedentes e crescente capacidade de influência no âmbito das redes sociais e dos meios de comunicação. Consequentemente, cabe aos países reforçarem seus trabalhos de Contrainteligência destinados a neutralizar a espionagem econômica, a antecipar os movimentos dos fluxos econômicos de caráter assimétrico e a prevenir a intrusão tecnológica nas infraestruturas críticas relacionadas com a economia (RODRÍGUEZ, 2011).

Uma ameaça que merece destaque para a atuação da Contrainteligência é a espionagem. A espionagem industrial, por exemplo, que tem como objetivo roubar propriedades intelectuais e tecnológicas de um Estado para obter vantagem competitiva, possui grande potencial de prejudicar a produção nacional e a economia (BONUCCI, 2016). Além disso, a espionagem também pode objetivar outros tipos de informações comerciais, como posições de barganha, disposição máxima de pagar por contratos e outras informações de posicionamento que possam ser úteis a um concorrente, comprador ou fornecedor (POTTER, 1998). Assim, a defesa das indústrias nacionais é primordial para a manutenção da competitividade econômica do país

no cenário global, com parcerias bem estabelecidas entre governo e empresas para a proteção dos segredos industriais, tecnologias estratégicas e informações comerciais.

A Abin possui dois programas que merecem destaque no combate à espionagem e na proteção de setores estratégicos e de tecnologias sensíveis: o Programa Nacional de Proteção de Conhecimento Sensível (PNPC) e o Programa de Articulação Nacional entre Governo, Empresas e Instituições Acadêmicas para a Prevenção e Mitigação do Risco de Eventos Químicos, Biológicos, Radiológicos e Nucleares selecionados (Pangeia). O primeiro promove, por meio de parcerias com instituições estratégicas, a proteção de conhecimentos sensíveis relativos aos interesses e à segurança do Estado e da sociedade. O segundo possui enfoque na proteção de bens e tecnologias sensíveis relacionadas à proliferação de armas de destruição em massa, por meio de ações como o fomento à cultura de proteção e o assessoramento no controle do comércio de bens sensíveis.

Outra área de preocupação da Contrainteligência, de grande importância para a segurança econômica do País, é o setor de biodiversidade e meio ambiente. Por meio de biopirataria, roubo de conhecimento tradicional associado, tráfico, desmatamento, extração ilegal e espionagem, o Brasil sofre danos enormes à sua economia[12] e à sua imagem perante a comunidade internacional. Diversas espécies brasileiras de plantas e animais foram objeto de registros de patentes no exterior, o que causou problemas para o governo brasileiro (FARIAS e CARVALHO, 2022).

Além disso, um Estado pode ser seriamente prejudicado por um ataque às próprias infraestruturas críticas[13] (ICs), cujo funcionamento contínuo é essencial para o desenvolvimento, a segurança e a qualidade de vida do país. São infraestruturas que envolvem os setores de comunicação, de transporte, de energia, setor financeiro e o fornecimento de suprimentos essenciais, como água e combustíveis.

IE e Contra-IE na Logística e Mobilização Nacional

O fundamento teórico e doutrinário da Mobilização Nacional (MN) se encontra no advento da nação armada ou guerra total, em que todos os recursos e o conjunto de forças ativas de um país são mobilizados e amalgamados para a vitória sobre o adversário. Gerada pela capacidade

12 A borracha, por exemplo, extraída de seringueira nativa da Amazônia, teve um peso significativo na economia brasileira no século XIX, até que ingleses contrabandearam suas sementes para a Ásia, que paulatinamente dominou o comércio mundial do produto.

13 Segundo o Decreto nº 9.573/2018, que aprova a Política Nacional de Segurança de Infraestruturas Críticas, são consideradas infraestruturas críticas as instalações, os serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provocará sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade.

industrial e científica e sustentada pelos recursos naturais e econômicos do país, a MN faz a máquina bélica funcionar, ao sair da situação de preparo em tempos de paz para a execução com eficiência e prontidão em tempos de guerra (VIDEIRA, 2019; BRASIL, 1983). Chama-se a atenção para a importância do tempo de resposta da MN, pois há enorme vantagem para o beligerante que mais prontamente transformar seu potencial nacional em Poder[14]. Essa capacidade de reação depende da capacidade logística, da conscientização do país, (VIDEIRA, 2019; SILVA, 2011) e do grau de assessoramento prévio de IE aos planejadores e decisores.

Em termos jurídicos, a MN pode ser definida como um instrumento legal decretado pelo Presidente da República, em caso de agressão estrangeira, para obter, reunir e distribuir os recursos e meios disponíveis no Poder e Potencial Nacionais[15], ou no exterior, ao complementar a Logística Nacional, para preservar ou restabelecer a Defesa e a Segurança da Nação (BRASIL, 2007). Esses recursos e meios deverão ser preparados com uma visão de planejamento integrado de longo prazo dos diversos setores competentes (BRASIL, 1983; BRASIL, 1987; BRASIL, 1988), hoje organizados no Sistema Nacional de Mobilização (Sinamob). Visa-se a capacitar o país para a realização de ações estratégicas e a consequente desmobilização com um mínimo de impactos negativos. Logística Nacional[16], por sua vez, para fins de MN, é o conjunto de atividades relativas à previsão e à provisão dos recursos e meios necessários à realização das ações decorrentes da END (BRASIL, 2007).

Da mesma forma que as funções e especificidades da IE em geral estão relacionadas com as lógicas e categorias de seu objeto de coleta e análise, seu papel para a LMN depende das variáveis próprias desse sistema inerente à Segurança Nacional. Já nos documentos doutrinários de LMN dos anos 1970 e 1980, havia o estabelecimento de lacunas de conhecimento a serem supridas por levantamentos e estudos, o que incluía funções para o Serviço Nacional de Informações (SNI). A Inteligência de Estado procederia a levantamentos estratégicos, forneceria informações e estimativas sobre a conjuntura nacional e internacional e sobre situações de emergência, proporcionaria a atualização do planejamento da MN e superintenderia os cadastros de dados de interesse (BRASIL, 1987; BRASIL, 1988).

Mesmo com a mudança do contexto

14 Na expressão econômica, a mobilização corresponde essencialmente à transformação da economia de paz em economia de guerra, e passa pela fase organizada da economia de transição (BRASIL, 1987).

15 Poder Nacional, compreendido como a capacidade que tem a Nação para alcançar e manter os objetivos nacionais, e se manifesta em cinco expressões: a política, a econômica, a psicossocial, a militar e a científico-tecnológica (BRASIL, 2020). Potencial Nacional é o conjunto de Homens e Meios de que dispõe a Nação, em estado latente, passível de ser transformado em Poder (BRASIL, 2019).

16 A Logística Nacional corresponde às capacidades nacionais existentes de suprir, manter e movimentar forças e recursos militares e civis. Envolve tanto a logística empresarial, de fluxos de mercadorias e informações, quanto a logística mais ampla no sentido militar, que inclui também funções de saúde, pessoal e engenharia, prevê e provê os meios necessários às ações estratégicas (EM 006/87).

político do Brasil e do mundo, essa lógica de atuação da Inteligência para a LMN permanece atual. No que tange à possibilidade de suprir, manter e movimentar as forças para a Defesa e de manter a própria sobrevivência da população, ou seja, a economia de guerra (BRASIL, 1988; COSTA E SILVA, 2011), os aspectos econômicos das capacidades da logística, da mobilização e também da desmobilização (BRASIL, 1987; BRASIL, 1988; BRASIL, 2007; VIDEIRA, 2019) assumem destaque e são objeto de produção de conhecimentos de IE. Nas bases doutrinárias da Mobilização de 1983, previam-se elementos como níveis de estocagem e de preços, racionamento de itens críticos, padronizações e estímulos produtivos, transferências de capacidades produtivas, comércio exterior e atividades creditícias, monetárias e fiscais, assim como a mobilização específica do setor industrial (COSTA E SILVA, 2011), e consideravam-se questões como insumos, mão-de-obra, infraestruturas e energia. (BRASIL, 1983; BRASIL, 1987; BRASIL, 1988).

Um conceito central em que deve haver apoio informacional da IE é o de hipótese de guerra (BRASIL, 1983; BRASIL, 1987), hoje denominado de hipótese de emprego, que representa as situações de potenciais agressões externas ensejadoras de uma decretação de MN, e que decorrem do estudo de cenários da conjuntura internacional e das vulnerabilidades e dos compromissos internacionais do Brasil (CHAGASTELES, 2003). É função da Inteligência central de Estado suprir os decisores do Ministério da Defesa (MD) e dos Estados-Maiores com análises interdisciplinares (geo)políticas, (geo) econômicas, sociais e jurídicas mais amplas, que reduzam as incertezas e ruídos (PLATT, 1974; FINGAR, 2011), atinjam vantagem informacional (OLIER, 2012) e embasem os diversos planos setoriais de Mobilização Nacional (BRASIL, 1983; BRASIL, 1988; VIDEIRA, 2019). Aqui, cabe ressaltar que os aspectos propriamente militares dos levantamentos estratégicos dessas hipóteses, como conhecimentos sobre as forças de países relevantes e conhecimentos de apoio operacional e tático, são estudados e definidos pelo Ministério da Defesa e pelas forças singulares, com apoio de seus respectivos serviços de Inteligência militar (CEPIK, 2003), e não há, assim, superposição, mas complementariedade dos diversos tipos de Inteligência envolvidos.

Na fase de estabelecimento das hipóteses de emprego e do planejamento estratégico[17], a IE pode contribuir com apreciações explicativas da conjuntura e das estruturas (geo)econômicas internas e externas, o que inclui as capacidades e intenções dos atores relevantes e as tendências, os cenários e consequências econômicas prováveis

17 Especificamente no que Beaufre (1998) chamou de "guerra logística", desenrolada em tempo de paz e com a aplicação de estratégias indiretas, os prazos de execução e maturação das decisões são de longa duração, o que torna a capacidade prospectiva do Estado diferencial vital de sua segurança nacional.

decorrentes das hipóteses de conflito (BRITO, 2011). Esses elementos de IE podem ter aplicação na fundamentação do planejamento estratégico e preditivo no âmbito do Planejamento Baseado em Capacidades (PBC), do MD, na definição de políticas da Base Industrial de Defesa, bem como na preparação e na execução de Operações de Paz da ONU. Questões como problemas de abastecimento e inflação, a imposição de sanções e o comportamento de países quanto à continuidade de fornecimento de bens militares e econômicos ao Brasil e ao país agressor seriam especialmente relevantes no contexto da LMN.

No mesmo sentido, em seus eixos de atuação para garantia da segurança econômica nacional, a Contrainteligência se mostra essencial para a manutenção e efetivação das atividades logísticas e de eventual MN do País. Ameaças como sabotagem, espionagem e interferência externa, além de prejudicar o desenvolvimento econômico nacional necessário para a atuação da LMN de forma efetiva, têm o potencial de romper as bases necessárias para o funcionamento dessas operações. Ademais, um ataque às ICs do país pode prejudicar todo o suporte e as cadeias de suprimentos necessárias para o desdobramento dessas atividades.

É importante ressaltar que o setor de Defesa é um alvo primordial para as atividades de Inteligência hostis. Assim, faz-se necessária a adoção de medidas especiais de proteção de suas infraestruturas, tecnologias e informações. Comumente, existem seções com especialistas em Inteligência no setor de Defesa, cujo principal objetivo é avaliar as ameaças e os riscos ao pessoal, às instalações e às informações nacionais da Defesa (CHUTER, 2011).

Considerações finais

Este artigo procurou explicar o papel da Inteligência de Estado para a Segurança Econômica do Brasil, ao explorar as funções e especificidades da Inteligência e da Contrainteligência econômicas para a Logística e a Mobilização Nacional sob o paradigma da Geoeconomia. Nessa lógica, a análise das funções e características definidoras da IE e da Contra-IE demonstrou a conexão existente entre a atividade meio e o objeto específico das análises. A economia, sobretudo em um olhar de economia política e geoeconomia, em que as relações de produção e distribuição dos bens da vida são também relações de poder e de disputas estratégicas entre Estados e organizações, define os problemas a serem abordados pela IE e as ameaças mais especificas que a Contra-IE tem de combater.

Na LMN, a expressão econômica é fundamental e suas necessidades levam, por sua vez, a novas questões e produtos de IE, com foco em questões logísticas estratégicas, como infraestruturas críticas, cadeias de suprimentos globais, acesso a

matérias primas, capitais e tecnologias, entre outros, com o correspondente reflexo na Contra-IE. Em uma guerra ou grave crise, como pandemias e problemas nas cadeias de suprimentos globais, a IE confere consciência e compreensão situacionais à LMN e à proteção da Segurança Econômica Nacional. Especificamente na LMN, a IE contribui com a análise de problemas econômicos e logísticos para os processos decisórios estratégicos nacionais relativos à capacidade de desenvolvimento, manutenção e mobilização da atividade econômica do Brasil. Ressalta-se os levantamentos e análises conjunturais e estruturais para os planejamentos do Sinamob, da Base Industrial de Defesa, do PBC e das hipóteses de emprego, tanto para a fase de preparo quanto durante a execução da LMN.

Por sua vez, essas mesmas capacidades apresentam vulnerabilidades que podem ser exploradas pelos diversos adversários e competidores do País. Assim, a Contra-IE, de forma espelhada, é responsável pela proteção dos conhecimentos sensíveis nas searas econômica e da LMN e se contrapõe às ameaças de ações clandestinas de serviços e organizações adversas, como espionagem, ações de influência e a sabotagem de infraestruturas críticas, aspecto de especial relevância no contexto da LMN.

Desta forma, para a criação de uma efetiva capacidade de LMN e, consequentemente, efetiva capacidade de Defesa e de Segurança do Estado e da sociedade brasileiros, cabe à Inteligência de Estado conhecer os ambientes e atores estratégicos, reduzir incertezas e antecipar tendências econômicas e logísticas, ao mesmo tempo em que protege os conhecimentos e estruturas críticas do país. As especificidades técnicas da matéria implicam a necessidade de pessoal especializado em IE e Contra-IE no Sisbin e na Abin, capazes de compreender sistemicamente o funcionamento dessas esferas da LMN, integrá-los transversalmente com outras áreas da Inteligência e gerar apreciações úteis aos decisores do Sinamob e ao próprio Sisbin.

O exercício das funções de IE e Contra-IE pela mesma agência pode facilitar a interação e a troca interna de informações e a obtenção de vantagem informacional na guerra econômica global em curso. Os produtos de análise explicativa conjuntural e estrutural da IE servem de embasamento à identificação de ameaças e ao planejamento e ao monitoramento das ações da Contra-IE. Igualmente, o conhecimento especializado sobre os atores que representam ameaças típicas tratadas pela Contrainteligência é um elemento diferencial sensível que precisa ser levado em consideração nas atividades de coleta, busca e análise de IE. Em conjunto, IE e Contra-IE formam o substrato informacional para que o país possa participar do complexo jogo multidimensional geoeconômico e político-militar do mundo atual.

Referências

BEAUFRE, André. *Introdução à estratégia*. Trad. Luiz de Alencar Araripe. Rio de Janeiro, Biblioteca do Exército ed., 1998.

BONUCCI, Lorenzo. *Economic Intelligence as National Security Issue, A Brief Study*. Dipartimento di Scienze Politiche e Sociali, Università degli Studi di Firenze, 2016.

BRASIL, *Proposta de Política Nacional de Defesa e Estratégia Nacional de Defesa*, 2020. Encaminhadas, em 22 de julho de 2020, para apreciação do Congresso Nacional.

BRASIL. *Fundamentos do Poder Nacional*. Rio de Janeiro, RJ: Escola Superior de Guerra, 2019. Disponível em: https://www.gov.br/esg/pt-br/centrais-de-conteudo/publicacoes/fundamentos-do-poder-nacional/FPN2022.pdf.

BRASIL, Decreto nº 9.573, de 22 nov. 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. *Diário Oficial da União*: seção 1, Brasília, DF, nº 225, 23 nov. 2018.

BRASIL. Decreto de 15 dez. 2017. Aprova a Estratégia Nacional de Inteligência. *Diário Oficial da União*: seção 1, Brasília, DF, n. 241 p. 36, 18 dez. 2017.

BRASIL. Decreto nº 8.793, de 29 jun. 2016. Fixa a Política Nacional de Inteligência. *Diário Oficial da União*: seção 1, Brasília, DF, ano 124, p. 5, 30 jun. 2016.

BRASIL. Lei nº 11.631, de 27 dez. 2007. Dispõe sobre a Mobilização Nacional e cria o SINAMOB. *Diário Oficial da União*: seção 1, Brasília, DF, ano 144, n. 249, p. 1, 28 dez. 2007.

BRASIL. Lei nº 9.883, de 7 dez. 1999. Institui o SISBIN, cria a ABIN e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, ano 137, n. 234, p. 49-50, 8 dez. 1999.

BRASIL, Portaria nº 73/1988. *Manual Básico de Mobilização Nacional*.

BRASIL. *Exposição de Motivos nº 6*, de 14 de setembro de 1987, SG/CSN.

BRASIL. *Exposição de Motivos nº 2*, 1983. Bases da doutrina de Mobilização Nacional, SG/CSN.

BRITO, Vladimir de Paula. *O papel informacional dos serviços secretos*. 2011. Dissertação

(Mestrado) - UFMG, 2011.

BRUNEAU, Thomas. Intelligence and democratization: the challenge of control in new democracies. *In: occasional paper #5*. Monterey/California: *The Center for Civil-Military Relations – Naval Postgraduate School*, Março, 2000.

BRANCO, E. C. C. Indicadores Econômicos na Análise de Inteligência – Estudo sobre os índices de risco soberano. *Revista Brasileira de Inteligência*, n. 12, p. 91-105, dez. 2017.

CEPIK, Marco. Inteligência militar e política de defesa. In: *Seminário de Política de Defesa para o século XXI*. Brasília: Câmara dos Deputados, Coordenação de Publicações, 2003. Pp. 111- 123

CHAGASTELES, Sérgio. Hipóteses de emprego na determinação da estrutura militar: custos, organização e dimensões na Marinha. *In: Seminário de Política de Defesa para o século XXI*. Brasília: Câmara dos Deputados, Coordenação de Publicações, 2003. p. 145 – 153.

CHUTER, David. *Governing & Managing the Defence Sector. Institute for Security Studies*, Africa do Sul, 2011.

COSTA, Manom Tavares da; GÓES, Guilherme Sandoval. Sistema de Mobilização Nacional frente uma ameaça externa e a segurança energética (marítima). *In: Cadernos do Desenvolvimento Fluminense*. Rio de Janeiro, n. 24, Edição especial, jan.- jun. 2023.

COSTA e SILVA, A indústria de Defesa – sua importância estratégica para o Brasil. *Caderno de Estudos Estratégicos de Logística e Mobilização Nacionais*. Rio de Janeiro: Escola Superior de Guerra, Divisão de Assuntos de Logística e Mobilização, v. 1, n. 3 , p. 137-153, jan./dez. 2011.

DCAF Intelligence Working Group. Intelligence Practice and Democratic Oversight. *In: A Practitioner's View Occasional Paper n. 3*, Geneva, July 2003.

DCAF – Geneva Centre for Security Sector Governance. SSR in a Nutshell. *In: Manual for Introductory Training on Security Sector Reform*. ISSAT, 2012.

DCAF – Geneva Centre for Security Sector Governance. *National Security Policies*. SSR Backgrounder Series Geneva: DCAF, 2015.

FARIAS, Antônio Cláudio Fernandes; CARVALHO, Antônio Augusto Muniz.

Biodiversidade, biopirataria e inteligência. *Diálogos Soberania e Clima*, Brasília, Centro Soberania e Clima, ano 1, v. 1, n. 5. 2022.

FINGAR, Thomas. *Reducing uncertainty: intelligence analysis and national security*. Stanford University: Stanford University Press, 2011.

FOLGADO, Pedro. A Segurança Económica e a Necessidade de um Sistema de Informações Económicas. *ResPublica*, n. 15, p. 87-99, 2015.

FRAUMANN, Edwin. Economic Espionage: Security Missions Redefined. *Public Administration Review*, v. 57, n. 4, p. 303-308, Jul/Aug. 1997.

GONÇALVES, Joanisval Brito. *Atividade de Inteligência e Legislação Correlata*, 6. ed. Niterói, RJ: Impetus, 2018. 472p.

KHANNA, Parag. *Connectography*: mapping the future of global civilization. New York, Random House, 2016.

NYE, Joseph. *Compreender os conflitos internacionais. Uma introdução à teoria e à história*. Lisboa: Gradiva, 2002.

OLIER, Eduardo. *Geoeconomía*: las claves de la economía global. Madrid: Ed. Pearson., 2012.

PLATT, Washington. *Produção de informações estratégicas*. Trad. Major Álvaro Galvão Pereira e Capitão Heitor Aquino Ferreira. Rio de Janeiro: Biblioteca do Exército: Livraria Agir Editora, 1974.

POTTER, Evan H. (org.). *Economic Intelligence & National Security*. Canada: Carleton University Press, 1998.

RIBEIRO, Anna Carolina Mendonça Lemos. *Sistema brasileiro de inteligência econômica*: reflexões para o estabelecimento de uma rede inicial de atores. 2016. Dissertação (Mestrado) - UnB, Brasília, 2016.

RICKARDS, James G. Economic Security and National Security: interaction and synthesis. *Strategic Studies Quarterly*, Air University Press, v. 3, n. 3, p. 8-49, Fall 2009), p. 8-49.

RODRIGUEZ, Juan Ferrer. Seguridad Económica e Inteligencia Estratégica de España. *Documento Opinión*, Instituto Español de Estudios Estratégicos, n. 85, 5 dic. 2011.

RUDZIT, Gunther; NOGAMI, Otto. Segurança e Defesa Nacionais: conceitos básicos para uma análise. *Rev. Bras. Polít. Int.*, v. 53, n. 1, p. 5-24, 2010.

SOUZA, Delanne Novaes de. Inteligência Econômica de Estado: necessidade estratégica para o Brasil. *Revista Brasileira de Inteligência*, Brasília: Agência Brasileira de Inteligência, n. 13, p. 129 – 148, dez. 2018.

VIDEIRA, Antonio Celente. *Da industrialização militar à Mobilização Nacional*. Rio de Janeiro: Ed. Luzes: Comunicação, Arte & Cultura, 2019.

Artigo

3

USO DE FONTES HUMANAS (HUMINT) EM OPERAÇÕES DE PAZ: OPORTUNIDADES E DESAFIOS.

DOI: https://doi.org/10.58960/rbi.2023.18.225

Fillipe Augusto da Silva *
Rafael Rodrigo da Silva **

Resumo

As operações de manutenção da paz são implementadas com o objetivo de ajudar países assolados por conflitos a criarem condições para uma paz duradoura. Dada a relevância dessas missões para o Brasil e para as relações internacionais contemporâneas, este artigo analisa como a Atividade de Inteligência e, mais especificamente, o uso de fontes humanas (Humint) podem auxiliar no efetivo cumprimento do mandato da ONU em missões de paz. Para isso, explorou-se, além das oportunidades de ação, os conflitos éticos e políticos a serem considerados, de modo que a adoção dessas práticas não afete negativamente a legitimidade das missões. Em face de uma visão de que a segurança internacional representa um pré-requisito essencial para as seguranças nacionais, o fortalecimento das estruturas de Inteligência da ONU ganha relevância. Apesar dos avanços tecnológicos, as fontes humanas continuam sendo um ativo crítico no fornecimento de informações. No âmbito das operações de paz, a ONU pode engajar-se na coleta extensiva de informações por meio de fontes humanas para prevenir e administrar conflitos, desde que mantenha rígidos princípios éticos e atue nos limites do direito internacional.

Palavras-chave: operações de manutenção da paz; Inteligência; fontes humanas; Humint.

USE OF HUMAN INTELLIGENCE (HUMINT) IN PEACE OPERATIONS: OPPORTUNITIES AND CHALLENGES.

Abstract

Peacekeeping operations are implemented with the aim of helping conflict-ridden countries create the conditions for lasting peace. Given the relevance of these missions for Brazil and for contemporary international relations, this article analyzes how the Intelligence Activity, and more specifically the use of human intelligence (Humint), can help in the effective fulfillment of the UN mandate in peacekeeping operations. For this, in addition to the opportunities for action, ethical and political conflicts to be considered were explored, so that the adoption of these practices does not negatively affect the legitimacy of the missions. Considering that international security represents an essential prerequisite for national security, the strengthening of UN Intelligence structures becomes relevant. Despite technological advances, human intelligence remains a critical asset in providing information. In the context of peacekeeping operations, the UN can engage in the extensive collection of information through human intelligence to prevent and manage conflicts, provided that it maintains strict ethical principles and acts within the limits of international law.

Keywords: *peacekeeping operations; Intelligence; human intelligence; Humint.*

* Mestre em Segurança Internacional e Defesa pela Escola Superior de Guerra (ESG). Servidor público federal.
** Mestrando em Ciências do Comportamento, pela Universidade de Brasília (UnB). Servidor público federal.

LA UTILIZACIÓN DE INTELIGENCIA DE FUENTES HUMANAS (HUMINT) EN OPERACIONES DE PAZ: OPORTUNIDADES Y DESAFÍOS.

Resumen

Las operaciones de mantenimiento de la paz se implementan con el objetivo de ayudar a los países en conflicto a crear las condiciones para una paz duradera. Dada la relevancia de estas misiones para Brasil y para las relaciones internacionales contemporáneas, este artículo analiza cómo la Actividad de Inteligencia, y más específicamente el uso de inteligencia de fuentes humanas (HUMINT), puede ayudar en el cumplimiento efectivo del mandato de la ONU en las misiones de mantenimiento de la paz. Para ello, además de las oportunidades de acción, se exploraron los conflictos éticos y políticos a considerar, para que la adopción de estas prácticas no afecte negativamente la legitimidad de las misiones. En vista de que la seguridad internacional representa un requisito previo esencial para la seguridad nacional, el fortalecimiento de las estructuras de inteligencia de la ONU se vuelve relevante. A pesar de los avances tecnológicos, las fuentes humanas siguen siendo un activo fundamental para proporcionar información. En el contexto de las operaciones de mantenimiento de la paz, la ONU puede involucrarse en la recopilación extensiva de información a través de fuentes humanas para prevenir y gestionar conflictos, siempre que mantenga principios éticos estrictos y actúe dentro de los límites del derecho internacional.

Palabras clave: *operaciones de mantenimiento de la paz; Inteligencia; fuentes humanas; humint.*

Introdução

As operações de manutenção da paz (PKO, do inglês *peacekeeping operations*) são implementadas com o objetivo de ajudar países assolados por conflitos a criarem condições para uma paz duradoura. A partir de mandatos definidos pelo Conselho de Segurança das Nações Unidas (CSNU), o emprego dessas missões está de acordo com os capítulos VI e VII da Carta da Organização das Nações Unidas (ONU). Na estrutura organizacional da ONU, as PKO são coordenadas pelo Departamento de Operações de Paz (DPO) e pelo Departamento de Apoio Logístico (DSF), subordinados ao Secretariado da entidade (ONU, 2008).

Três princípios básicos diferenciam as PKO como uma ferramenta para manutenção da paz e da segurança internacional: (a) consentimento das partes; (b) imparcialidade; e (c) não uso da força, exceto em legítima defesa ou defesa do mandato (ONU, 2008). No entanto, desde o fim da Guerra Fria, a agenda de paz e segurança no âmbito das Nações Unidas vem mudando, para se caracterizar, principalmente, pela adoção de "mandatos robustos", ou seja, com autorização para que os comandos das missões de paz empreguem os meios necessários para que suas finalidades sejam cumpridas (CEPIK; KUELE, 2016).

Nas últimas décadas, as PKO também têm se tornado multidimensionais, e abarcam missões que incluem do monitoramento de acordos de paz e da proteção de civis ao acompanhamento de eleições e ao apoio em desastres naturais (CEPIK; KUELE, 2016). Neste contexto, as forças de manutenção da paz estão sujeitas a atuarem em países marcados pela instabilidade política e institucional, que, muitas vezes, envolvem uma ordem social abalada ou à beira do colapso, com hostilidades declaradas ou iminentes às forças empregadas na missão (SMITH, 1994). Este cenário exige, por parte das forças de PKO, o conhecimento detalhado das condições do terreno, tanto para permitir a eficaz manutenção da paz, quanto para garantir sua própria segurança (CARNEGIE; CARSON, 2021).

Para o Brasil, a participação em missões de paz está baseada em princípios constitucionais, mais especificamente no artigo 4º da Constituição Federal de 1988, que menciona, nos incisos VI, VII e IX, respectivamente, "defesa da paz", "solução pacífica dos conflitos" e "cooperação entre os povos para o progresso da humanidade" (BRASIL, 1988). Em consonância com os princípios constitucionais, a Política Nacional de Defesa (PND) destaca que o país pode ser estimulado a incrementar sua participação neste tipo de missão, o que permite ao Brasil estreitar laços de cooperação, bem como ampliar sua projeção no concerto internacional (BRASIL, 2020).

Como marco da participação brasileira

em PKO, destaca-se o comando militar da Missão das Nações Unidas para Estabilização do Haiti (Minustah) pelo General Augusto Heleno Ribeiro Pereira, em 2004. Outro importante marco foi o comando exercido pelo General Carlos Alberto dos Santos Cruz, em 2013, da Missão das Nações Unidas para Estabilização da República Democrática do Congo (Monusco). O Brasil também assumiu tarefas de comando militar e de coordenação da Força Interina das Nações Unidas no Líbano (Unifil), estabelecida em 2006 por solicitação do governo libanês.

Em 2010, o país investiu na criação do Centro Conjunto de Operações de Paz do Brasil (CCOPAB), que visou a apoiar a preparação de militares, policiais e civis, brasileiros e de nações amigas, para as missões de paz. Por meio de sua participação em operações de paz, o Brasil tem buscado uma inserção internacional mais assertiva, relacionada ao interesse do país em desempenhar um papel mais relevante no campo da segurança internacional, bem como buscar legitimidade em seu pleito por um assento permanente no Conselho de Segurança da ONU (KUELE, 2014).

Dada a relevância das PKO para o Brasil e para as relações internacionais contemporâneas em geral, a hipótese inicial deste estudo é de que a Atividade de Inteligência representa ferramenta essencial para o cumprimento dos mandatos modernos definidos às PKO. Diante do contexto apresentado, este artigo busca avaliar, por meio de uma análise baseada na legislação vigente e na revisão de literatura, como o uso de ferramentas de Inteligência – e, mais especificamente, da Inteligência de fontes humanas (Humint, do inglês *Human Intelligence*) – podem auxiliar no efetivo cumprimento das missões de paz da ONU. Além disso, busca-se avaliar os limites éticos e políticos a serem considerados, de modo que a adoção dessas práticas não afete negativamente a legitimidade das missões.

ONU e Atividade de Inteligência

Por Atividade de Inteligência, entenda-se aqui o conceito abordado pela Política Nacional de Inteligência (PNI), que a define como "o exercício permanente de ações especializadas, voltadas para a produção e difusão de conhecimentos, com vistas ao assessoramento de autoridades nos respectivos níveis e áreas de atribuição" (BRASIL, 2016). No âmbito das Nações Unidas, no entanto, a Inteligência assume uma forma distinta, tendo em vista que a atividade implica, necessariamente, a existência de inimigos ou rivais, fato a que a ONU evita estar associada (SMITH, 1994). Nesse sentido, o uso de Inteligência no âmbito das Nações Unidas pode criar alguns dilemas.

Um primeiro dilema se refere à coleta de informações sensíveis, uma vez que

governos nacionais se mostram hesitantes em compartilhá-las com a ONU, pelo risco de expor fontes ou métodos de coleta. Essa exposição, de fato, pode colocar em risco os interesses nacionais, ao passo que alvos poderiam evitar a detecção assim que entendessem como são monitorados (CARNEGIE; CARSON, 2021). Uma alternativa seria a coleta direta de Inteligência pela estrutura da ONU. No entanto, esta proposta tende a receber oposição de Estados-membros, com a preocupação de que nações mais poderosas a utilizem para seu benefício próprio, em detrimento da soberania nacional dos demais países (CEPIK; KUELE, 2016).

Um segundo dilema surge quando as informações são coletadas, por vezes, secretamente. Este fato se torna um problema, pois a ONU é historicamente pautada pela transparência e pela imparcialidade em suas ações. O uso de métodos encobertos para coleta de informações poderia manchar sua imagem como mediadora imparcial de conflitos internacionais. Por seu caráter institucional, portanto, a ONU não admite a utilização de ferramentas convencionais da Atividade de Inteligência, como a infiltração de agentes disfarçados, estória cobertura, suborno ou uso de agentes duplos (DORN, 1999; CEPIK; KUELE, 2016).

Outro fato relevante a ser considerado é a capacidade relativamente fraca da ONU para a integração de Inteligência. Existe, por parte dos países, uma percepção generalizada da falta de confiança nos sistemas de confidencialidade existentes na organização. Casos anteriores de irregularidades, negligência e corrupção, incluindo má conduta de tropas em PKO, que abandonaram seus postos e deixaram documentos confidenciais desprotegidos, acabam por alimentar preocupações sobre a gestão de Inteligência pela ONU e deixam os países cautelosos em delegar essa capacidade à entidade (CARNEGIE; CARSON, 2021).

Nas últimas décadas, no entanto, o desconforto generalizado com a ideia de Inteligência na ONU está gradualmente dando lugar a sua aceitação pela comunidade internacional. Em parte, considera-se que a produção de Inteligência pela ONU não envolve necessariamente métodos dissimulados ou ilegais, como roubo de informações ou subversão (SHETLER-JONES, 2008). Além disso, o fim da Guerra Fria permitiu à ONU assumir um papel mais assertivo na resolução dos complexos conflitos internacionais e admitir sua necessidade de uso da Inteligência. Desde então, nota-se um esforço no sentido de institucionalização da Atividade de Inteligência no âmbito da ONU (KUELE; CEPIK, 2015).

Inteligência e operações de paz

Fato é que as Nações Unidas representam um ator relevante, embora inicialmente relutante, no jogo de Inteligência global. Ao aceitar esse papel e de posse de mandatos reconhecidamente mais robustos em suas missões de paz, a ONU está gradualmente desenvolvendo estruturas de Inteligência em suas missões (DORN, 2010). Com mais de 90 mil pessoas empregadas atualmente em campo pelas PKO, incluindo militares, policiais e civis, a ONU possui acesso privilegiado a muitas das principais zonas de conflito do mundo, p. ex., Líbano, Sudão do Sul e República Democrática do Congo (ONU, 2023).

No âmbito das PKO, os primeiros esforços concretos pela institucionalização da Atividade de Inteligência ocorreram a partir da década de 1990, com a criação das estruturas *Department of Peacekeeping Operations* (DPKO) e *Situation Centre* (SITCEN). Entre os objetivos do SITCEN, está a coleta de informações civis e militares no nível estratégico para auxiliar os tomadores de decisões (KUELE, 2014). O centro monitora as PKO em campo, com especial atenção para situações potencialmente ameaçadoras ao pessoal da ONU, e atua como um ponto de contato na sede das Nações Unidas, em Nova York, para todas as missões em campo (EKPE, 2007).

Além dos avanços observados no âmbito do Secretariado, as mudanças organizacionais chegaram também ao nível operacional. Em 2006, a diretriz para criação de um *Joint Mission Analysis Centre* (JMAC) para cada PKO demonstrou o desejo da ONU em produzir avaliações de Inteligência de qualidade em suas missões, desde que detivesse o mandato e os recursos necessários (CEPIK; KUELE, 2016). A criação dos JMAC representou o início das chamadas "*Intelligence-led operations*", ou seja, operações conduzidas com base em evidências produzidas pela Atividade de Inteligência. A MINUSTAH foi uma das missões pioneiras entre as operações da ONU conduzidas por Inteligência (DORN, 2009).

Como missão, os JMAC devem garantir que todas as PKO tenham um monitoramento efetivo e integrado de operações, relatórios e análise de informações no quartel-general da operação. O objetivo central é apoiar o desenvolvimento da consciência situacional em campo, com informações de segurança e análise para a tomada de decisões gerenciais. Para isso, o JMAC conta com uma equipe multidisciplinar, o que reflete o amplo espectro encontrado nas PKO atualmente e com a tarefa de produzir resultados equilibrados, oportunos e sistemáticos (SHETLER-JONES, 2008).

Para além do trabalho tático desenvolvido nos JMAC, a Atividade de Inteligência se faz necessária também no nível estratégico, mesmo antes do envolvimento da ONU

em algum conflito, principalmente para se entender a situação política entre as partes. Uma vez que as forças de paz sejam mobilizadas, a Inteligência estratégica mantém sua relevância ao auxiliar na antecipação de movimentos políticos de governos ou facções, especialmente se houver risco de violência. Em um contexto operacional, a Inteligência é necessária no planejamento mais eficaz de recursos, para otimizar o cumprimento de seu mandato. Neste contexto, a capacidade de avaliar o nível de armamentos, os movimentos, as estratégias e o potencial militar das facções em conflito é obviamente importante (SMITH, 1994).

Cabe ressaltar, no entanto, que o ciclo de Inteligência em uma PKO difere em aspectos importantes do processo tradicional, pois, inclui certas limitações na escolha dos métodos de coleta. Em geral, as principais limitações à coleta de informações são de base legal ou ética. A ONU, por ser uma organização cumpridora e criadora da lei internacional, atua estritamente nos limites legais impostos em suas missões de campo (DORN, 1999). Os limites éticos, por sua vez, dizem respeito à situação de vulnerabilidade em que se encontram as populações civis envolvidas em situações de conflito.

Além disso, a coleta de informações em PKO é uma atividade repleta de dificuldades políticas. Neste aspecto, a principal preocupação é que a obtenção de informações pela ONU possa ser vista como comprometedora da imparcialidade da organização em relação às partes em conflito, aspecto essencial em uma PKO (SMITH, 1994). Em contraponto, a Inteligência destinada à proteção das forças de paz é bastante incontroversa. Poucas partes questionariam – pelo menos não abertamente – o direito de uma unidade de manutenção da paz de localizar campos minados, por exemplo (ERIKSSON, 1997).

Humint e operações de paz

Diante das limitações expostas e pelo fato de as Nações Unidas não serem tecnologicamente equipadas para conduzir vigilância secreta, a Inteligência Humana (Humint) se consolida como o método de coleta mais prevalente em PKO (DORN, 2010). Uma das vantagens de uma operação de paz é o acesso direto a áreas específicas de conflitos e seus habitantes. As relações próximas e amigáveis entre os membros de uma PKO e os civis locais fornecem não apenas uma avaliação contínua dos humores, mas também componentes de Inteligência mais sólidos. Essas informações seriam difíceis de se obter pelos meios tradicionais de Inteligência militar, cujo uso pode gerar tensões (ERIKSSON, 1997).

Oportunidades

Os seres humanos são essenciais para todos os processos e operações da sociedade, sejam eles públicos ou privados. Como tal, eles são a primeira e última linha de segurança e, consequentemente, são os primeiros e últimos pontos de entrada na arena da Inteligência. (SANO, 2015). Assim, Humint pode ser definida como "qualquer informação que possa ser coletada de fontes humanas", seja abertamente ou secretamente, e que pode incluir uma variedade de fontes, desde uma fonte humana secreta e infiltrada, a contatos abertos com governos estrangeiros e habitantes de uma área de conflito (BERNARD; SULLIVAN, 2020). Além disso, a Humint é a forma mais antiga de Inteligência e continua sendo uma das mais valiosas para a tomada de decisões em questões de segurança. A Humint pode ser usada para se obter informações sobre indivíduos, grupos, organizações e países (TSANG, 2008).

De modo geral, as missões de paz envolvem forças militares e civis de várias nacionalidades. Essas forças precisam trabalhar em conjunto para alcançar objetivos comuns. Além de ser essencial para garantir a cooperação entre essas forças, a Humint pode ser usada para coletar informações sobre a situação política, econômica e social da região em que a missão está ocorrendo; obter informações sobre grupos armados ou criminosos que possam representar uma ameaça à segurança da missão; identificar líderes comunitários e outros indivíduos que possam ajudar a estabelecer a paz e a estabilidade na região; e obter informações sobre a população local, incluindo suas necessidades e desejos (LANUBILE, 2010).

A missão no Haiti, conduzida de 2004 a 2017, foi um exemplo em que a Humint foi amplamente utilizada. Na ocasião, a ONU foi capaz de explorar o descontentamento da população local com as gangues para obter informações estratégicas. A missão tinha fundos especiais para construir relacionamentos com ela, fato incomum no âmbito das PKO. Por vezes, pessoas próximas aos líderes de gangues ofereciam voluntariamente evidências incriminatórias e informações para ajudar as tropas da Minustah a efetuarem as prisões. Para isso, foi criada, em 2005, uma linha direta gratuita, que funcionava 24 horas por dia e permitia que haitianos compartilhassem informações anônimas sobre atividades de gangues, crimes e violações de direitos humanos, especialmente sequestros. O serviço provou ser valioso e ajudou a localizar e libertar reféns e capturar membros de gangues, ainda que grande parte das ligações tenha sido enganosa (DORN, 2009).

Os refugiados, tanto aqueles que permanecem em zonas de conflito quanto aqueles que fugiram para outros países, também podem ser uma valiosa

fonte de informações. No Congo (1960-64), missão pioneira no uso de coleta de Inteligência, oficiais realizavam interrogatórios de solicitantes de refúgio, o que, ocasionalmente, representava uma maneira inestimável de coletar informações. Criminosos ou suspeitos detidos pelas forças de paz também podem ser submetidos a procedimentos formais de interrogatório, desde que garantidos seus direitos individuais. No Congo, por exemplo, não há indicação de que os interrogatórios conduzidos envolvessem qualquer tipo de violência e, como resultado, foram fonte de informações valiosas, incluindo a descoberta dos nomes de mercenários e a localização de depósitos de armas (DORN, 2010).

As organizações não-governamentais (ONGs), apesar de não serem Humint propriamente ditas, são outra fonte importante de informações. Presentes em grande parte das PKO, essas organizações realizam atividades extensas em áreas de conflito e, portanto, são detentoras de conhecimento sobre a situação local (BERNARD; SULLIVAN, 2020). Como desafio, no entanto, muitas delas se mostram relutantes em serem associadas às operações militares, inclusive às PKO. Em parte, isso ocorre pela sua natureza em rejeitar aspectos militares ou para evitar dividir os créditos de seu esforço com outro ator. Independentemente desse obstáculo, ainda há oportunidades para diálogo e troca de informações entre o ramo militar da PKO e uma ONG, especialmente sobre a situação de segurança local.

Por fim, cabe acrescentar que a Humint permite que as forças de paz entendam a cultura e a história locais, o que pode ajudá-las a tomar decisões que são mais facilmente aceitas pela população local. Desse modo, a Humint pode ajudar a estabelecer uma relação de maior confiança entre as forças de paz e os residentes da área em conflito, o que pode facilitar a cooperação e o maior sucesso das ações planejadas (JOHNSON, 2010).

Em suma, a implantação efetiva de uma estrutura de Inteligência baseada em Humint representa uma oportunidade para se evitar a implantação de uma operação militar mais complexa, que, além de ser mais cara, pode dificultar as atividades das forças de paz. Quanto mais coesa a relação das forças de paz com a população local, mais efetiva é a coleta de informações e, consequentemente, os produtos da Inteligência têm mais qualidade e potencial aproveitamento (CEPIK; KUELE, 2016).

Desafios

É importante destacar, no entanto, que o uso da Humint, no âmbito das PKO, apresenta alguns desafios. Primeiramente, há o desafio de recrutar e manter informantes confiáveis, especialmente em regiões onde a violência e o conflito são comuns. Além disso, a Humint pode ser influenciada pelo preconceito, pelo

viés pessoal ou por interesses ocultos dos informantes. Ainda, o trabalho de Inteligência Humana pode ser perigoso para os informantes e suas famílias, uma vez que podem ser alvo de retaliação por parte dos grupos ou indivíduos investigados. Esses desafios são relevantes e devem ser levados em consideração ao se planejar o uso da Humint em missões de paz (LANUBILE, 2010).

As mesmas limitações impostas à ONU em relação à fundação de uma rede institucional de Inteligência também se estendem ao uso de Humint no âmbito das PKO. Com o uso de fontes humanas, há o temor de que a integridade e a legitimidade das ações das operações de paz sejam comprometidas. Um importante fator a ser considerado são os riscos envolvidos e a qualidade das informações obtidas. No Haiti, por exemplo, sabia-se que chefes de gangues canalizavam informações falsas por meio de informantes. Diante da grande quantidade de rumores, as Nações Unidas tiveram de verificar e cruzar as informações recebidas. Os informantes podem oferecer informações não-verificadas ou falsas para receber pagamentos, incriminar inimigos ou até mesmo para constranger deliberadamente a ONU (DORN, 2009).

As barreiras legais para o uso de ativos humanos em situações de vulnerabilidade são limitadas por diferentes paradigmas de segurança internacional. As condições para que fontes humanas sejam utilizadas são que seu uso seja proporcional à ameaça representada e que a prática tenha evidentes ganhos acionáveis que não poderiam ser fornecidos por outros meios (BERNARD; SULLIVAN, 2020). Neste contexto, a institucionalização da atividade ganha relevância, o que inclui diretrizes para implantação de recursos e as questões de proporcionalidade e necessidade. A criação das JMAC representa um importante passo alcançado no rumo desta institucionalização.

A deficiência no fluxo de informações também pode ser apontada como causa das desconfianças relacionadas ao uso de fontes humanas pela ONU (CEPIK; KUELE, 2016). A difusão de informações obtidas por Humint deve ocorrer de maneira seletiva, de modo a se evitar vazamento de informações que possam colocar as fontes em risco. Além da proteção às identidades, as informações coletadas devem ser tratadas com cuidado para que os métodos utilizados na obtenção não sejam expostos. Em circunstâncias de alto risco, a ONU deve ajudar a fornecer proteção e asilo em outro Estado disposto a receber informantes cujas vidas estejam em risco. No Haiti, por exemplo, informantes eram levados às zonas de conflito vestidos com uniformes militares da ONU e com os rostos protegidos, para que pudessem apontar suspeitos sem que fossem identificados (DORN, 2009).

Outros limites são impostos por razões

éticas válidas. Por envolver pessoas vulneráveis que vivem em área de conflito, a Humint em operações de paz requer limites específicos a serem seguidos. Por fim, a gama de atividades aceitáveis dependerá do mandato e das circunstâncias da missão. O oferecimento regular de pagamentos a fontes humanas, por exemplo, é considerado imprudente no âmbito das PKO. No entanto, a ONU deve ser livre para receber informações voluntárias de informantes em circunstâncias de maior risco. A experiência da missão na Somália (1993-95), por exemplo, mostrou que mulheres e crianças, que geralmente sofrem mais com o conflito, fornecem informações mais confiáveis quando comparadas a informantes pagos (ERIKSSON, 1997).

Além disso, cabe ressaltar que as informações obtidas por meio de Humint podem ser influenciadas pelo preconceito, pela emoção e pela subjetividade do informante. Acrescenta-se o fato de que as informações podem ser imprecisas ou desatualizadas, uma vez que as fontes humanas podem não ter acesso a todas as informações relevantes. Dessa forma, a coleta de informações por meio da Humint pode ser perigosa para os informantes, que podem ser expostos a represálias por parte dos grupos ou indivíduos investigados (HARTHCOCK, 1999).

As reações políticas adversas à coleta de informações por meio de fontes humanas são causadas, em partes, pela falsa relação da Humint como uma espécie de "vigilância secreta". Essas críticas surgem do pressuposto de que as Nações Unidas devem ser totalmente pautadas pela transparência e, de acordo com essa visão, não devem se envolver em nenhuma atividade de Inteligência que possa prejudicar sua imparcialidade. Neste contexto, o uso de fontes humanas não deve envolver o uso de certas práticas comuns na espionagem, a saber, suborno, chantagem e uso de agentes duplos. Em muitos casos, pode ser dada ênfase à coleta aberta de informações (BERNARD; SULLIVAN, 2020).

Em geral, os Estados tendem a relutar à possibilidade de dar à ONU um mandato maior de Inteligência, com base em temores de conceder poder excessivo à entidade. Países menos desenvolvidos também podem estar preocupados com que uma função de Inteligência mais robusta, autorizada a organizações internacionais, coloque em risco sua própria integridade nacional. Ainda que haja relutância dos Estados-membros no emprego de técnicas clássicas de coleta de informações, os civis locais em áreas onde as operações de manutenção da paz são conduzidas sempre serão uma importante fonte de informação.

Considerações finais

Nas últimas décadas, ganhou relevância a importância dada à coleta e à análise de informações, tanto de natureza secreta

quanto aberta, para a efetividade das PKO e a segurança de suas tropas. No campo, a coleta de informações estratégicas auxilia na tomada de iniciativas, no controle do "campo de batalha" e na minimização dos riscos, tanto para as tropas quanto para os civis da região (DORN, 2009). Nessas missões, os objetivos das unidades de Inteligência podem ser, portanto: aumentar a segurança do pessoal empregado na missão; prover suporte para operações específicas; antecipar possível eclosão de conflito; e estabelecer estimativas de interferências externas (DORN; BELL, 2003).

No entanto, por parte dos Estados-membros, há certa hesitação em dar autonomia de Inteligência a organizações internacionais, a exemplo das Nações Unidas. Entre os principais obstáculos apontados, estão: (I) a ausência de rotinas para lidar com material sensível de maneira adequada nessas entidades; (II) o temor de que a integridade e a legitimidade das PKO sejam questionadas; e (III) as barreiras impostas pelo direito internacional sobre o uso de ativos humanos em situações de vulnerabilidade.

Como resposta à capacidade relativamente fraca da ONU para a integração de Inteligência, a entidade deve dedicar-se a melhorar seu sistema de confidencialidade de maneira concreta. Outras organizações internacionais, p. ex., a Agência Internacional de Energia Atômica (AIEA) e a Organização Mundial do Comércio (OMC), foram capazes de lidar efetivamente com obstáculos semelhantes à coleta de informações. Para isso, foram implementados sistemas de confidencialidade fortes, que incluem computadores autônomos, sistemas de classificação de documentos e penalidades por vazamentos, entre outras medidas. Como alternativa, a ONU poderia recorrer a modelos semelhantes (CARNEGIE; CARSON, 2021).

Em geral, missões de PKO requerem informações detalhadas sobre movimentos rebeldes e outras condições do local de atuação. Por isso, uma operação de paz eficaz requer a aquisição proativa e a análise prudente de informações sobre as condições dentro da área da missão. Isso é especialmente verdadeiro se a operação for conduzida em um ambiente imprevisível e a segurança da força de paz estiver ameaçada. No entanto, métodos encobertos não são necessários para que a ONU se mantenha engajada na obtenção de informações. Em grande parte, esse tipo de informação pode ser obtido em fontes abertas ou na relação com os civis locais.

De maneira geral, experiências históricas deixaram a lição às Nações Unidas de que é arriscado engajar-se em operações de paz complexas sem ter acesso a uma Inteligência sólida, acionável e secreta (KUELE; CEPIK, 2015; DORN, 2010). Em um ambiente operacional complexo,

em razão de mandatos robustos e dos próprios ambientes conflituosos, tanto a segurança das forças de manutenção da paz quanto o sucesso de suas missões dependem fortemente da coleta de Inteligência. Em face de uma visão de que a segurança internacional representa um pré-requisito essencial para as seguranças nacionais, o fortalecimento das estruturas de Inteligência da ONU ganha relevância.

Apesar dos avanços tecnológicos, as fontes humanas continuarão a ocupar um papel crítico no fornecimento de informações. No âmbito das PKO, as relações com civis locais podem resultar em elementos sólidos de Inteligência. Neste sentido, a ONU pode engajar-se na coleta extensiva de informações por meio de fontes humanas, para prevenir e administrar conflitos, desde que mantenha rígidos princípios éticos e atue nos limites do direito internacional. Assim, a ONU pode lançar mão desta importante ferramenta sem que sua reputação seja questionada pela comunidade internacional.

Referências

BRASIL. Ministério da Defesa. *Política Nacional de Defesa e Estratégia Nacional de Defesa*. Brasília, 2020.

BRASIL. Decreto no 8.793, de 29 de junho de 2016. *Fixa a Política Nacional de Inteligência*. Brasília, 2016.

BRASIL. *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BERNARD, Rose; SULLIVAN, Richard. The use of HUMINT in epidemics: a practical assessment. *Intelligence And National Security*, v. 35, n. 4, p. 493-501, jun. 2020.

CARNEGIE, Allison; CARSON, Austin. UN Peacekeeping After the Pandemic: an increased role for intelligence. *Survival*, v. 63, n. 2, p. 77-83, mar. 2021.

CEPIK, Marco; KUELE, Giovanna. Inteligência em Operações de Paz da ONU: déficit estratégico, reformas institucionais e desafios operacionais. *Dados*, Rio de Janeiro, v. 59, n. 4, p. 963-993, out. 2016.

DORN, Walter; BELL, David. Intelligence and peacekeeping: the un operation in the Congo 1960-64. *International Peacekeeping*, v. 2, n. 1, p. 11-33, mar. 1995.

DORN, Walter; BELL, David. Intelligence and Peacekeeping: The UN Operation in the Congo, 1960-64. *In*: JONG, Ben de; PLATJE, Wies; STEELE, Robert D. (org.). *Peacekeeping Intelligence*: emerging concepts for the future. Oakton, Virginia: OSS International Press, 2003. p. 253-280.

DORN, Walter. The Cloak and the Blue Beret: limitations on intelligence in un peacekeeping. *International Journal Of Intelligence And Counterintelligence*, v. 12, n. 4, p. 414-447, out. 1999.

DORN, Walter. Intelligence-led Peacekeeping: the United Nations stabilization mission in Haiti (Minustah). *Intelligence And National Security*, v. 24, n. 6, p. 805-835, dez. 2009

DORN, Walter. United Nations Peacekeeping Intelligence. In: JOHNSON, Loch K. (ed.). *The Oxford Handbook of National Security Intelligence*. Oxford: Oxford University Press, 2010. p. 275-295.

EKPE, Bassey. The Intelligence Assets of the United Nations: sources, methods, and

implications. *International Journal Of Intelligence And Counterintelligence*, v. 20, n. 3, p. 377-400, 2007.

ERIKSSON, Pär. Intelligence in peacekeeping operations. *International Journal Of Intelligence and Counterintelligence*, v. 10, n. 1, p. 1-18, mar. 1997.

HARTHCOCK, Clyde. *Peace Operations from an Intelligence Perspective*. Army War College Carlisle Barracks, PA, 1999.

JOHNSON, Loch. Evaluating "Humint": the role of foreign agents in US security. *Comparative Strategy*, v. 29, n. 4, p. 308-332, oct. 2010.

JOHNSTON, Paul. No cloak and dagger required: intelligence support to un peacekeeping. *Intelligence and National Security*, v. 12, n. 4, p. 102-112, out. 1997.

KUELE, Giovanna. *Atividade de Inteligência em Operações de Paz da ONU: rumo à institucionalização?* 2014. 80 f. Trabalho de Conclusão de Curso (Graduação) – Curso de Relações Internacionais, Ciências Econômicas. Universidade Federal do Rio Grande do Sul (UFRGS), Porto Alegre, 2014.

KUELE, Giovanna; CEPIK, Marco. Inteligência em Operações de Paz da ONU (1945-2000). *Carta Internacional*, v. 10, n. 1, p. 21-38, 15 abr. 2015.

LANUBILE, Luca. *The Intelligence Gathering Activity in Peace Support Operations*. Marine Corps Command and Staff Coll Quantico VA, 2010.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). *United Nations Peacekeeping Operations*: principles and guidelines. Nova York: Department of Peacekeeping Operations, 2008.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). *UN Peacekeeping Operations. Department of Peacekeeping Operations*, 2022. Disponível em: https://peacekeeping.un.org. Acesso em: 30 abr. 2023.

SANO, John. The Changing Shape of HUMINT. *Intelligencer Journal*, Washington, v. 21, n. 3, p. 77-80, jan. 2015.

SHETLER-JONES, Philip. Intelligence in Integrated UN Peacekeeping Missions: the joint mission analysis centre. *International Peacekeeping*, v. 15, n. 4, p. 517-527, ago. 2008.

SMITH, Hugh. Intelligence and UN Peacekeeping. *Survival*, v. 36, n. 3, p. 174-192, set. 1994.

TSANG, Steve (ed.). *Intelligence and Human Rights in the Era of Global Terrorism*. Stanford: Stanford University Press, 2008. 240 p.

Artigo

4

A ATIVIDADE DE INTELIGÊNCIA E OS DESAFIOS DE UMA SOCIEDADE CONECTADA PELO CAOS: aprendizado de máquina e análise de redes como um recurso auxiliar

DOI: https://doi.org/10.58960/rbi.2023.18.226

Caroline Lira *

Resumo

As redes sociais são capazes de impactar positiva e negativamente cenários sociais, políticos e econômicos de um país. O grande fluxo de informações que circulam nesses ambientes impossibilita que, por ação unicamente humana, sejam realizadas operações de combate à desinformação e a *fake news*. A Atividade de Inteligência também precisa se adequar ao novo desafio de coletar, analisar e disseminar conhecimento em meio a uma qualidade duvidosa de conteúdo produzido por Inteligência Artificial. O objetivo deste artigo é explorar os modelos de aprendizado de máquina que representam ferramentas auxiliares valiosas para monitorar, em tempo real, oportunidades e ameaças de desinformação.

Palavras-chave: aprendizagem de máquina; Inteligência; *fake news*.

INTELLIGENCE ACTIVITY AND THE CHALLENGES OF A SOCIETY CONNECTED BY CHAOS: machine learning and network analysis as an auxiliary resource

Abstract

Social networks are capable of impacting positively and negatively on a country's social, political and economic scenarios. The large flow of information that circulates in these environments makes it impossible to conduct operations to combat disinformation and fake news by human action alone. In this context, the goal of this article is to explore the models and tools that can be used by the intelligence community to collect, analyze, and disseminate knowledge in the midst of a dubious quality of content produced by Artificial Intelligence. The aim of this article is to explore machine learning models that represent valuable auxiliary tools to monitor in real time opportunities and disinformation threats.

Keywords: *machine learning; Intelligence; fake news.*

* Advogada. Mestranda em Ciências da Computação e Matemática Computacional pela Universidade de São Paulo (USP). Especialista em *Big Data e Cybersercurity.*

LA ACTIVIDAD DE INTELIGENCIA Y LOS RETOS DE UMA SOCIEDAD CONECTADA POR EL CAOS: el aprendizaje automático y el análisis de redes como recurso auxiliar

Resumen

Las redes sociales son capaces de impactar positiva y negativamente en los escenarios sociales, políticos y económicos de un país. El gran flujo de información que circula en estos entornos hace imposible llevar a cabo operaciones de lucha contra la desinformación y las fake news únicamente mediante la acción humana. En este contexto, el objetivo de este artículo es explorar los modelos y herramientas que pueden ser utilizados por la comunidad de inteligencia para recopilar, analizar y difundir conocimiento en medio de una dudosa calidad de los contenidos producidos por la Inteligencia Artificial. El objetivo de este artículo es explorar los modelos de aprendizaje automático que representan valiosas herramientas auxiliares para vigilar en tiempo real oportunidades y las amenazas de desinformación.

Palabras clave: *aprendizaje automático; Inteligencia; noticias falsas.*

Introdução

O cinema dos anos 1980 e 1990 projetava 2023 como um mundo futurista, com carros voadores e robôs que andavam entre seres humanos com normalidade, como o desenho "Os Jetsons". Não havia dúvida, na utopia projetada nas telas, os problemas da humanidade seriam com a própria tecnologia, em que o dilema moral e ético giraria em torno de robôs e seus conflitos, como na obra "Eu, Robô" e "AI Inteligência Artificial".

A realidade é que os dilemas atuais, embora envolvam a tecnologia, tornaram-se mais complexos, pois ainda têm a ver com como os humanos estão utilizando, por exemplo, as redes sociais para manter-se conectados, devido à desordem informacional, desinformação e caos de algoritmos com vieses.

Em qualquer país, a preocupação com a interferência estrangeira é um fato. O Parlamento Europeu, em relatório de 2023, expôs considerações sobre a manipulação maliciosa de informações realizada por estrangeiros e sobre *bots* e contas falsas utilizadas para minar a confiança nos processos eleitorais democráticos (UE, 2023). As mídias sociais têm sido instrumento importante para manter pessoas, governos e causas conectadas; todavia, também tornaram-se um campo de guerra da desinformação.

Dessa forma, a ciência do comportamento e a matemática aplicada são importantes áreas para se entender como grupos comportam-se, polarizam-se, propagam doenças e até *fake news*, e para entender a capacidade de cooperação para se transformar qualquer coisa em uma pandemia (SMALDINO, 2023).

A tecnologia, em sua essência – em especial, o aprendizado de máquina (ML, de *machine learning*, em inglês) e a Inteligência Artificial (IA) –, é, muitas vezes, ignorada no processo de evolução dos métodos de entendimento do comportamento humano. A produção de conhecimento, o enfrentamento e a neutralização de discursos de ódio, extremismo e crises que envolvam processos sensíveis são possíveis apenas por meio do conhecimento das vozes nas redes sociais.

Não há dúvida que a Inteligência Artificial impactará o futuro da segurança dos países (ALLEN, 2017). O setor militar, as agências de Inteligência e as organizações privadas já precisam lidar com o futuro em seus cenários prospectivos sobre os possíveis danos. Não só em uma corrida na capacidade robótica e cibernética, como também na criação de medidas contra *deepfake*, desinformação, ChatGPT, manipulação e *fake news* que desgastam a imagem de políticos, governos e empresas.

Os modelos matemáticos propostos neste trabalho, bem como algoritmos de aprendizagem de máquina, objetivam demonstrar que recursos simples costumam

trazer resultados mais objetivos e menos custosos.

Atividade de Inteligência e a Inteligência Artificial

A produção de conhecimento tornou-se desafiadora na era da desinformação, uma vez que a sociedade está sendo diariamente projetada para as pessoas estarem conectados de alguma forma, muitas vezes, por ferramentas de IA generativa (p. ex., ChatGPT), que transformarão as redes sociais muito em breve em ambientes com conteúdo "sintético" e com a confiança ainda mais questionável (GRUPPO, 2023).

Há um novo desafio em exercer, em meio à desordem informacional, a Atividade de Inteligência, que visa obter, analisar e disseminar conhecimento sobre fatos e situações, ou possíveis influências no processo decisório de ações governamentais (GONÇALVES, 2003).

Para Daphone Ippolito, pesquisadora do Google Brain, apenas retirar textos cegamente da internet pode resultar em vieses e falsidades nos próprios modelos futuros de IA. E reforça que a construção de ferramentas para detectar esses textos gerados por IA será essencial, uma vez que essa tecnologia pode ser usada para criar notícias falsas e desinformação (HEIKKILA, 2022).

Pesquisadores do *Copenhagem Institute for Futures Studies* afirmam que o cenário atual do GPT-3 *(Generative Pre-trained Transformer)*, com 175 bilhões de parâmetros, é irreversível e apontam que a combinação de IA com a dinâmica do metaverso será a criação de cenários distópicos e alucinantes, como *deepfakes, fake news* e desinformação (HVITVED, 2022).

Um dos desafios é que a Inteligência Artificial tradicionalmente conhecida permite extrair padrões e *insights* dos dados coletados e moldá-los em novos conhecimentos, mas a IA generativa, que tem dominado as discussões acadêmicas, ultrapassa esse limite, pois usa dados para gerar mais dados (ALBERTO, 2022).

Destaca-se que a análise de dados objetiva fornecer informações úteis, oportunas e relevantes para a tomada de decisões , ou seja, para a qualidade dessa informação, é preciso redobrar as aplicações de *sourcing tradecraft*, definido como um conjunto de estruturas mentais e linguísticas para auxiliar a entender melhor a qualidade dessas informações (GRUPPO, 2023).

Newbery e Kaunert (2023) propõem que a Inteligência deve ser abordada como fenômeno social e, embora existam outras abordagens, a Atividade é detentora de um propósito específico. O fato é que, na prática, alguns especialistas afirmam que uma boa Inteligência envolve reduzir a incerteza em relação aos adversários e ao contexto do conflito em questão, e o aprendizado de máquina, assim como

alguns modelos matemáticos são capazes de auxiliar em coleta, análise, processamento e distribuição desse conhecimento de uma forma rápida e eficiente.

Conectados pelo Caos: Desinformação e *Fake News*

Notícias falsas e desinformação são temas complexos e transitam da segurança nacional à saúde pública; embora não sejam novos, as redes sociais proporcionaram uma forma mais rápida de disseminação. Segundo os dados do *Statista*, em 2019, 47% dos estadunidenses presenciaram alguma notícia falsa em jornais e revistas impressos (WATSON, 2019). A diferença é que, nos meios tradicionais de comunicação, muitas vezes, a desinformação fica limitada quanto a sua circulação, mas, nas vias digitais, a propagação é imediata e instantânea em seus efeitos.

O *Statista*, em uma pesquisa em 2020, apontou que 38,2% das pessoas já compartilharam notícias falsas em suas redes sociais, sem saber que não eram verdadeiras. Em 2018, cerca de 52% dos estadunidenses já haviam percebido que os sites de notícias *online* relatam, de forma regular, notícias falsas, mas cerca de 9% dos adultos não acreditam que existem notícias falsas *online (ibidem)*.

Uma estratégia adotada nas operações de influência nas mídias sociais é o uso de mensagens que combinam a qualidade informacional e parábolas políticas. Ela é usada por atores estatais, atores não estatais ou alguma combinação de ambos, influenciadores ou grupos específicos (JARDINE, 2019). Esse esforço de influência pode ser visto em Facebook, Twitter, Instagram, WhatsApp e outros ambientes. Eles favorecem o efeito-escala, impulsionam ações de grupos extremistas e disseminam instantaneamente desinformações por ações humanas ou *bots* (JARDINE, 2019). Como os seres humanos estão conectados, tornam-se potencializados pelas bolhas de filtro (ARGUEDAS, 2017). Essas redes de conexões formadas pelas redes sociais moldam opiniões e o cotidiano de uma sociedade.

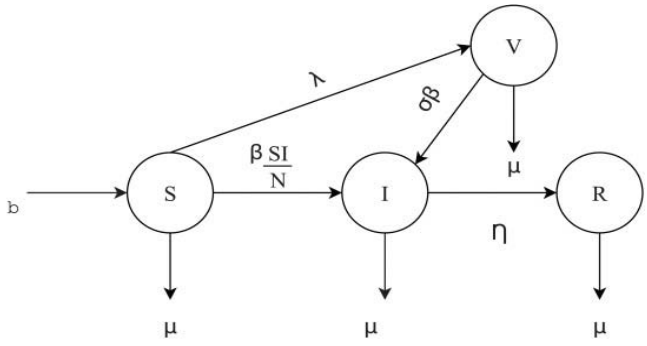
Análise de Redes Sociais

Os métodos de análise de redes sociais têm atraído a atenção da comunidade de Inteligência, pois contribuem para se entender as relações sociais e os padrões comportamentais em ambientes e temas diversos, p. ex., sociais, políticos e econômicos. Nessa perspectiva sobre o tema, é importante destacar que a análise de redes sociais mostra a importância dos relacionamentos entre as unidades que interagem. Ou seja, nessa visão, para a análise de redes sociais acontecer, deverá englobar teorias, modelos matemáticos e um estudo relacional, em que os atores sejam vistos como interdependentes e não como unidades autônomas independentes

(WASSEMAN, 1994). Assim, pode-se definir modelos para descrever como a desinformação sobre alguns temas é disseminada em grupos com influência diferente, além de ser possível observar tendências reais e mecanismos de propagação de mensagens não confiáveis (SHIVASTAVA *et al.* 2020).

Shrivastava *et al.*(2020) propõem, em estudo, que se use, para detecção e controle de desinformação (boato) em redes sociais *online*, o modelo SVIR *(suscetível-verificado-infectado-recuperado)*, inspirado na mesma modelagem epidêmica de disseminação de vírus na população como a COVID-19. Os usuários podem ser divididos em diferentes subclasses: suscetível *S(t)*, o indivíduo que ainda não se tornou vítima de boato/desinformação/*fake news*, mas está suscetível a eles; infeccioso I(t), o que acredita nos textos não confiáveis/*fake news*/desinformação; também é ativo como disseminador de boatos; verificado, V(t), significa aquele indivíduo que é usuário autenticado, e não um disseminador de boatos; o recuperado, R(t), é o indivíduo que não acredita no boato. Mas o disseminador pode ser bloqueado ou removido, e, a qualquer momento, os usuários podem trocar de posição. O modelo proposto pelos autores é apresentado na figura 1.

Figura 1 - Modelo SVIR



Fonte: (SHIVASTAVA *et al.* 2020)

Modelo representado como: N*(t)* = S*(t)* + I*(t)*+V*(t)*+R*(t)*

Ainda sobre a modelagem da desinformação, Brody e Meier (2021) propõem dois modelos que podem ser aplicados em cenários de polarização, p. ex., eleições. O primeiro modelo está baseado na ideia de um representante-eleitor, em uma compreensão qualitativa dos fenômenos associado a notícias falsas/desinformação/boatos em um nível macroscópico do cenário. O segundo, baseada na ideia de uma análise de uma microestrutura eleitoral, descreve o comportamento coletivo do eleitorado, pode modelar as preferências de eleitores

individuais, usa a teoria da comunicação, com as *fake news*/desinformação como ruído.

Pode-se aplicar o classificador *Bayesiano Naive* ou a análise dos nós de origem sobre a propagação de boato, ou notícia nas redes sociais, sobre a credibilidade dos *tweets* no Twitter (atual X) ou, ainda, sobre o impacto das mensagens para se traçar e detectar um rumor em fase inicial (SIVASANKARI e VADIVU, 2022).

Aprendizado de máquina contra *fake news*

As modelagens assistidas por computador e a análise preditiva de dados comportamentais são recursos auxiliares aos métodos analíticos na coleta de dados e para o compartilhamento de Inteligência (como produto), disponíveis também aos analistas de Inteligência (LOKHHANDE, 2023).

Mediante o processamento de linguagem natural, o computador consegue entender, analisar e manipular a linguagem humana, por exemplo, a autocorreção do celular ou um filtro de *spam* no e-mail. Para a preparação de um texto para análises que serão apresentadas abaixo, é necessário um conjunto de ações disponibilizada em uma biblioteca (NLTK) no Python (linguagem de programação), para remover pontuações, converter dados textuais em vetores, remover palavras que podem ser ignoradas e reduzir palavras flexionadas (HARDY, 2023).

No âmbito das notícias falsas, processamento de linguagem natural (PLN)[1] pode se mostrar útil na detecção automática; as redes sociais, os sites de notícias, as comunicações oficiais e notícias verificadas por agências de checagem são fontes para a construção de um *corpus* para o *dataset* (OSHIKAMA, QUIAN e WANG, 2020). Zervopoulos *et al.*(2020), em estudo, usaram PLN para detectar notícias falsas no Twitter; em *corpus* de 13.856.454 *tweets*, e concluíram que existe diferencia morfológica, lexical e vocabular entre *tweets* que espalham notícias falsas e reais.

Thota *et al.* (2018), em estudo, após perceberem lacuna na classificação binária e na capacidade de detecção de notícia real, apresentaram uma arquitetura de redes neurais com precisão de 94,21% nos testes. Kresnaková *et al.* (2019), assim como Thota *et al.*, realizaram estudo com modelos de redes neurais. Usaram, primeiramente, o texto do título das notícias (com acurácia de 91%) e, na segunda parte, textos completos (89%) foram treinados com um conjunto de dados obtidos no *Kaggle*. A conclusão foi que as redes neurais representam modelos

1 (...) uma área da ciência da computação e da Inteligência Artificial que se ocupa das interações entre computadores e as interações entre os computadores e as línguas humanas (naturais) e a forma de programar os computadores para processarem grandes quantidades de dados em linguagem natural. (THOTA *et al.*, 2018)

de aprendizado profundo.

No Brasil, o Instituto de Ciências de Computação e Matemática Computacional (ICMC) da Universidade de São Paulo (USP) é pioneiro no *corpus* em português, com uma precisão maior que 90%, implementado na ferramenta *FakeCheck* (SANTOS e PARDO, 2021). Atualmente, essa universidade possui, além do *FakeCheck*, a Ada[2], ferramenta com um *corpus* atualizado até junho de 2023 com 2.849 textos de notícias, documentos oficiais da página do Ministério das Relações Exteriores brasileiro e de outros portais oficiais nacionais e internacional; tem acurácia de 82%.

Chitra e Jain (2023), em estudo, testaram o classificador *Naive Bayes* para detecção de *fake news*; é derivado do Teorema de Bayes; na prática, é utilizado para calcular probabilidade condicional (probabilidade de algo acontecer, dado que outra coisa já ocorreu). Trata-se de um algoritmo de aprendizado de máquina supervisionado e pode ser usado em um conjunto de dados pequeno ou grande.

Na coleta de dados de redes, p. ex., o Twitter, com interações instantâneas sobre fatos importantes, pode ser realizada a análise de sentimento como um recurso, para os setores público e privado, para extrair emoções favoráveis ou impressões. Essas emoções não fornecem informações objetivas sobre a verificação de uma notícia, mas é possível localizar desinformação, e a sua origem, em debates e comunidades em que se propaga certos conteúdos com desinformação (BHUTANI *et al.* 2019).

Em estudo sobre a possibilidade de detecção de *fake news* com análise de sentimentos, Bhutani *et al.* incorporaram os sentimentos como recurso importante para a precisão. Os autores consideraram sentimentos por trás de declarações falsas e verdadeiras. Para eles, os sentimentos são expostos ao se escrever um texto na rede social; depois da aplicação do método *tf-idf*, para ver a frequência de palavras nos textos e sua importância, houve o uso do algoritmo de *Naive Bayes*. Esse estudo é importante, pois, segundo os dados apresentados pela *"Our World in Data"*, somente o Facebook, em 2019, tinha 2,4 bilhões de usuários, isso significava uma em cada três pessoas no mundo. Das redes sociais mais comuns entre os jovens e adultos, estão YouTube, Facebook, Instagram e TikTok. Somente nos Estados Unidos da América (EUA), adultos passam mais de 6 horas diárias conectados em mídias digitais (OSPINA, 2019). Ainda, segundo estudo do *Pew Research Center*, adultos de 18 a 29 anos nos EUA são mais propensos a receber notícias indiretamente pelas mídias sociais do que diretamente pelos jornais tradicionais *(ibidem).*

Isso faz com que as redes sociais sejam

2 A ferramenta foi selecionada para o Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais(IHC) de 2023 em Maceió-AL/Brasil.

um terreno fértil para que conteúdo manipulado e pseudoinformativo se dissemine rapidamente. Um estudo de 2022 do *Pew Research Center*, aponta que os adolescentes têm apreço pela conectividade social nessas plataformas, mas também preocupações com dramas. O grupo do estudo também revelou questões sobre suas próprias expectativas e as dos outros: ansiedade, negatividade nas redes sociais e como o ativismo os atrai (ANDERSON *et al.* 2022).

Dessa forma, a análise de redes sociais não deve ser totalmente ignorada, ou seja, seu público, por exemplo, costuma expressar mais suas emoções por se sentirem superconectados uns aos outros (EHMAKE, 2023) e, em uma situação como ataque em escola, *bullying* e situações de ódio, é possível identificar grupos ativos e agentes influenciadores com o auxílio de modelos analíticos preditivos para neutralizar novos ataques.

Considerações Finais

Os recursos tecnológicos e a potencialidade da Inteligência Artificial que conhecemos hoje ainda não representam nem o início de todo seu potencial. Todavia, suas infinitas ferramentas viabilizam que corridas por poder e segurança nacional de um Estado sejam realizadas com melhor desempenho do que a realizada exclusivamente por humanos. O número crescente de dados que circulam nas redes impossibilita que haja controle de desinformação e manipulação derivadas de interferência estrangeira ou grupos extremistas.

Ao contrário do pensamento humano com tendências aos vieses cognitivos e políticos, *fake news* deve ser tratado de forma multidisciplinar; todavia, nas lentes da Atividade de Inteligência, não pode significar nebulosidade. Os modelos de aprendizado de máquina, servem como uma ferramenta adicional para precisão na tomada de decisão.

Referências

ALLEN, Greg; CHAN, Taniel. *Artificial Intelligence and National Secururity*. Cambridge: Harvard Kennedy School. Belfer Center for Science And International Affairs, July 2017.

ANDERSON, Monica *et al. Focus groups:* Social media stirs a range of emotions and reactions in teens. Pew Research Center, Washington, DC, 16 nov. 2022.

ARGUEDAS, Amy Ross *et al. Echo chambers, filter bubbles, and polarisation:* a literature review. Oxford: Reuters Institute, Jan. 2022.

BHUTANI, Bhavika *et al.* Fake News Detection Using Sentiment Analysis. *In: Twelfth International Conference on Contemporary Computing* (IC3), Noida, 2019.

BRODY, Dorje C.; MEIER, David M. *Mathematical models for fake news.* Disponível em: https://arxiv.org/pdf/1809.00964. Acesso em: 19 out. 2023.

CHITRA, Jain, Arihant. Fake News detection using naive bayes classifier. *Journal of Analysis and Computation (JAC)*, vol. XIV, issue -VI, 2020. Disponível em: www.ijaconline.com. Acesso em: 19 out. 2023.

EHMAKE, Rachel. *How Using Social Media Affects Teenagers.* Child Mind Institute. Disponível em: Social Media Effects on Teens | Impact of Social Media on Self-Esteem (childmind.org). Acesso em: maio 2023.

GONÇALVES, Joanisval Brito. *A Atividade de Inteligência no combate ao crime organizado: o caso do Brasil.* Disponível em: http://www2.senado.leg.br/bdsf/handle/id/103. Acesso em: 19 out. 2023.

GRUPPO, Meaghan. *Intelligence Sourcing Basics:* A Primer as Generative AI Pollutes the Internet to Death. Disponível em: https://substack.com. Acesso em: maio 2023.

HARDY, John. Hunters and Gatherers: the evolution of strike and Intelligence functions in special operations forces. *International Journal of Intelligence and CounterIntelligence,* v. 36, n. 4, p 1143-1163. 2023.

HEIKKILA, Melissa. How AI-generated text is poisoning the internet. *MIT Technology Review.* Dez. 2022.

HVITVED, Sophie. What if 99% of the metaverse is made by AI? *Scenario magazine,* Copenhagen, 24 fev. 2022.

JARDINE, Érico. Beware Fake news. *Platform governance, security,* Centre for International Governance Innovation. Disponível em: https://www.cigionline.org/aticles/beware –fake-news/. Acesso em: abril 2023.

KRESNAKOVA, Viera Maslej *et al.* Deep learning methods for Fake News detection. *In: IEEE International Symposium on Computational Intelligence and Informatics.* Hungria, 2019.

LOKHANDE, Samiksha. Noções básicas de PNL (Processamento de Linguagem Natural). Disponível em: medium.com. Acesso em: maio 2023.

NEWBERY, Samantha; KAUNERT, Christian. Critical Intelligence Studies: a new framework for analysis. *Intelligence and National Security,* v. 38, n. 5, p. 780-798, 21 feb. 2023.

ORTIZ-OSPINA, Esteban. The rise of social media. *Our World in Data,* 18 sept 2019. Disponível em: https://ourworldindata.org/rise-of-social-media. Acesso em: 19 out 2023.

OSHIKAMA, Ray; QUIAN, Jing; WANG, William Yang. A Survey on Natural Language Processing for Fake News Detection: computation and language. *In: Conferência de Recursos e Avaliação Linguística,* 2020. Disponível em: https://doi.org/10.48550/arXiv.1811.00770. Acesso em: 19 out. 2023.

ROMERO, Alberto. *Generative AI Could Pollute the Internet to Death.* Disponível em: substack.com. Acesso em: maio 2023.

SANTOS, Roney Lira de Sales; PARDO, Thiago Alexandre Salgueiro. Structural Characterization and Graph-based Detection of Fake News in Portuguese. *In: Simpósio Brasileiro de Tecnologia da Informação e da Linguagem Humana.* Porto Alegre: Sociedade Brasileira de Computação, 2021.

SHRIVASTAVA, Gulshan et al. Defensive Modeling of Fake News Through Online Social Networks. *IEEE Transactions on Computational Social Systems,* vol. 7, n. 5, pp. 1159-1167. 2020.

SIVASANKARI S.; VADIVU, G. Tracing the fake News propagation path using social network analysis. *Soft Comput,* v. 26, n. 23, p. 12883–12891, 2022.

SMALDINO, Paul E. *v* Princeton University Press.2023

THOTA, Aswini *et al.* Fake News Detection: a deep learning approach. *SMU Data Science Review,* v. 1, n. 3, 2018. Disponível em: https://scholar.smu.edu/datasciencereview/vol1/iss3/10/. Acesso em: 19 out. 2023.

WASSERMAN, Stanley; FAUST, Katherine. *Social Network Analysis:* methods and applications. Cambridge University Press, 1994.

WATSON, Amy. Encountering fake news in print media worldwide 2019, by country. *Statista,* 03 Jun. 2022a.

WATSON, Amy . Share of adults who have witnessed fake news in print media worldwide as of January 2019, by country. *Statista,* 03 Jun. 2022b.

WATSON, Amy . Perceived frequency of online news websites reporting fake news stories in the United States as of March 2018. *Statista,* Abr. 2018.

ZERVOPOULOS, A. *et al.*. Hong Kong Protests: using natural language processing for fake News detection on twitter. *In:* MAGLOGIANNIS, I.; ILIADIS, L.; PIMENIDIS, E. (ed.). Artificial Intelligence Aplications and Innovations. AIAI 2020. *IFIP Advances in Information and Communication Technology,* v. 584. Springer, Cham. Disponível em: https://doi.org/10.1007/978-3-030-49186-4_34. Acesso em: 19 out. 2023

Artigo

5

O TRABALHO DE INTELIGÊNCIA E O OFÍCIO DOS JUÍZES: UMA COMPARAÇÃO ENTRE SERVIDORES PÚBLICOS

DOI: https://doi.org/10.58960/rbi.2023.18.227

Anna Cruz *
Andrey Corrêa **
Arthur Machado ***

Resumo:

O artigo discute papeis e expectativas sobre servidores de duas funções interpretativas distintas: juízes e analistas de Inteligência. Inicialmente, são examinadas as semelhanças e diferenças no exercício dos ofícios, e sublinha-se que, embora as atividades sejam congêneres por lidarem com a interpretação de fatos e ideias presentes na sociedade, o resultado de suas análises é marcadamente diverso: espera-se um produto tão imparcial e objetivo quanto possível do analista de Inteligência, isto é, produção de juízos meramente enunciativos; na atividade do juiz, são admitidos desacordo teórico e juízos valorativos. O artigo aborda, ainda, a imparcialidade no serviço público e argumenta que, na Atividade de Inteligência, o referido valor é fundamental para a manutenção de seu diferencial no assessoramento ao processo decisório.

Palavras-chave: Atividade de Inteligência de Estado; assessoramento de Inteligência; serviço público brasileiro; princípio da imparcialidade.

INTELLIGENCE WORK AND THE CRAFT OF JUDGES: A COMPARISON BETWEEN PUBLIC SERVANTS

Abstract:

The article discusses public servant's roles and expectations on two distinct interpretative functions: judges and intelligence analysts. Initially, similarities and differences are examined in each office practices, underlining that, although both activities are likewise since they deal with the interpretation of facts and socially present ideas, its analysis results are markedly diverse: for an intelligence analyst, a most impartial and objective product is expected, i.e., the production of purely enunciative judgments; for the judge's activities, theoretical disagreement and value evaluations are admitted. Thus, the article debates public service impartiality, arguing that, in the intelligence activity, such a value is fundamental for maintaining its differential in aiding the decision-making process.

Keywords: *State Intelligence Activity; Intelligence aiding; Brazilian public service; impartiality principle.*

* Mestre em Direitos Humanos pela Universidade Federal do Pará (UFPA). Oficial de Inteligência da Agência Brasileira de Inteligência (Abin).

** Mestre em História Política pela Universidade Federal de Uberlândia. Servidor público federal.

*** Bacharel em Relações Internacionais pela Universidade de São Paulo (USP). Servidor público federal.

EL TRABAJO DE INTELIGENCIA Y EL OFICIO DE JUECES: UNA COMPARACIÓN ENTRE SERVIDORES PÚBLICOS

Resumen:

El artículo analiza los roles y expectativas de los servidores públicos en dos funciones interpretativas distintas: jueces y analistas de inteligencia. Inicialmente, se examinan similitudes y diferencias en las prácticas de cada oficio, subrayando que, si bien ambas actividades lo son similares por tratarse de la interpretación de hechos e ideas socialmente presentes, los resultados de sus análisis son marcadamente diversos: un producto lo más imparcial y objetivo posible se espera del analista de inteligencia, es decir, la producción de juicios puramente enunciativos; para las actividades del juez, desacuerdos teóricos y valoraciones de valor se admiten. Incluso, el artículo debate la imparcialidad del servicio público, argumentando que, en la actividad de inteligencia, tal valor es fundamental para mantener su diferencial en el asesoramiento en la toma de decisiones.

Palabras Clave: *Actividad de Inteligencia estatal; asesoramiento de inteligencia; servicio público brasileño; principio de imparcialidad.*

Introdução

No cumprimento da missão da Atividade de Inteligência (AI) – isto é, produção de conhecimento estratégico para auxiliar a tomada de decisão (BRASIL, 2016) –, analistas realizam diversos julgamentos: juízos sobre evidências, que expressam certeza, inferem probabilidades, admitem, muitas vezes, a impossibilidade de afirmar algo a respeito de fatos ou situações porque não se superou o estado de dúvida ou de ignorância; julgamentos sobre fontes e conteúdos, que avaliam aspectos relativos a confiança, competência e autenticidade daquelas e semelhança, coerência e compatibilidade desses; e raciocínios, elaborando associações entre juízos gerais (BRASIL, 2016).

Há proximidade com o que Eros Grau (2005) anota sobre o Direito: quando um julgador realiza a compreensão de textos e fatos para deles produzir norma (ela, portanto, a própria interpretação) a ser aplicada num caso concreto. De forma parecida, um conjunto de elementos da realidade é também um conjunto de possibilidades de interpretação sobre eles, colocado à disposição do profissional de Inteligência – é assim que conhecimentos produzidos pela Atividade buscam conclusões sobre o passado ou, até mesmo, apontam tendências para o futuro. No Direito, o julgamento faz norma; na AI, o julgamento sobre fatos produz raciocínios e conclusões.

No Direito, a confecção de norma (isto é: o ato interpretativo) por juízes é balizada por princípios (LAJUS DOS SANTOS, 2021), observa o ordenamento jurídico de determinado país em sua inteireza e todas as informações fáticas disponíveis e vale-se de estudos sobre precedentes e da experiência na magistratura. Contudo, as decisões judiciais são também altamente influenciadas por vieses e circunstâncias não-cognitivas (por exemplo, fome[1] e inabilidade tecnológica), pouco sujeitas a fórmulas estruturadas ou guias de passo a passo.

Por seu turno, na AI, para se alcançar as construções mentais, são imprescindíveis um método estruturado e o socorro a técnicas analíticas para a verificação, por pares e superiores, do caminho que levou a determinada conclusão, o que propicia ao profissional perceber suas

1 Como exposto pelo psicólogo Kahneman, que, ao discutir sobre os sistemas de julgamento presentes nos estados mentais, cita uma experiência relatada nos *Proceedings of the National Academy of Sciences*:"Os participantes inadvertidos do estudo eram oito juízes de condicional em Israel. Eles passam dias inteiros revisando pedidos de condicional. Os casos são apresentados em ordem aleatória, e os juízes dedicam pouco tempo a cada um, numa média de seis minutos (...). (O tempo exato de cada decisão é registrado, e os períodos dos três intervalos para refeição dos juízes - a pausa da manhã, o almoço e o lanche da tarde - durante o dia também são registrados). Os autores do estudo fizeram um gráfico da proporção de pedidos aprovados em relação ao tempo desde a última pausa para refeição (...). Durante as duas horas, mais ou menos, até a refeição seguinte dos juízes, a taxa de aprovação cai regularmente, até chegar perto de zero pouco antes da refeição (...). A melhor explicação possível dos dados é uma má notícia: juízes cansados e com fome tendem a incorrer na mais fácil posição (...) de negar os pedidos de condicional. Tanto o cansaço como a fome provavelmente desempenham um papel." (KAHNEMAN, 2012, p. 58)

parcialidades e negligências. Há uma doutrina de Inteligência que preconiza fases, etapas e ampla discussão sobre o imperioso uso de técnicas de análise estruturada, especialmente para relatórios interpretativos e prospectivos (CRUZ, 2019). Mas interpretar, afirmar significado de tais fatos e situações, pode ser um momento criativo? Quão "inventivo" pode ser um servidor público? Responder a essa pergunta por meio do exercício de comparar esses dois ofícios interpretativos permite perceber e delimitar o perímetro da AI.

Marrin & Clemente (2006), ao comparar medicina e análise de Inteligência, mostraram que o exercício comparativo entre profissões auxilia a reflexão sobre as lacunas existentes para a profissionalização, à medida, por exemplo, que:

> *In contrast to the legal and medical professions, intelligence analysis does not have well-defined systemic formal knowledge, such as a coherent doctrine or theory, does not involve high levels of individual autonomy due to involvement of management in approving the dissemination of most finished intelligence analysis, and does not have standards that are formulated or enforced by other members of the occupation (ibidem., p. 647).*

Assim, neste artigo, pretende-se também refletir sobre a prática profissional do analista, sobre as pretensões de isenção que lhe atingem e sobre os deveres que o serviço público lhe impõe, contrastando com o trabalho dos juízes, como um modo de ampliar o conhecimento sobre a Atividade de Inteligência.

O intérprete na atividade jurisdicional e na Atividade de Inteligência

O ato de interpretar na atuação jurisdicional é objeto de antigo debate em que, de um lado, defende-se a total isenção do juiz ou a subsunção desse ao ordenamento jurídico, ao desconsiderar o aspecto "mundano" e humano do julgador e, de outro, convoca-se o juiz ao ativismo, ao reconhecer aspectos cognitivos e ambientais que envolvem o processo de produção de uma decisão judicial.

O ativismo judicial acontece quando uma ação do órgão jurisdicional intenciona alterar certos ambientes político-sociais, em um interesse que é, necessariamente, valorativo, e pode ser conservador ou progressista, por exemplo. É nesse cenário que Garapon conceitua: "o ativismo começa quando, entre várias soluções possíveis, a escolha do juiz é dependente do desejo de acelerar a mudança social ou, pelo contrário, de a travar" (GARAPON, 1998, p. 54).

Em uma dimensão técnica, o posicionamento de Luís Roberto Barroso (2009) assinala que o ativismo judicial representa a interpretação constitucional pelo Poder Judiciário para além da literalidade da Constituição. A postura ativista se manifestaria por meio de diferentes condutas, que incluem: (i) a aplicação direta da Constituição a situações

não expressamente contempladas em seu texto e independentemente de manifestação do legislador ordinário; (ii) a declaração de inconstitucionalidade de atos normativos emanados do legislador, com base em critérios menos rígidos que os de patente e ostensiva violação da Constituição; (iii) a imposição de condutas ou de abstenções ao Poder Público, notadamente em matéria de políticas públicas.

O fenômeno do ativismo judicial é essencialmente ideológico, vinculado às dimensões políticas do "ser" julgador e seu contexto social, político e econômico. Ao analisá-lo, surge um paradoxo: ao mesmo ponto que o ativismo pode apresentar uma dimensão de fratura institucional, ele também tem sido, em muitos casos, forma de efetivação de direitos.

Ao contrário do juiz que "toma a decisão", o analista de Inteligência "descreve cenários" para um processo decisório *a posteriori*. Mas as duas atividades, a do juiz e a do profissional de Inteligência, têm aspectos interpretativos congêneres: lidam com interpretação de fatos, leituras e, a despeito da inexistência de um sujeito neutro, mecânico, tanto na atividade jurisdicional quanto na Atividade de Inteligência, sofrem demanda por grande precisão interpretativa.

Nesse sentido, Grau (2005) afirma que, no âmbito do Direito, embora o produto da interpretação seja a norma, ela já se encontra em potência, no invólucro do texto da lei, e o intérprete apenas a desnuda, não a cria, literalmente. Igualmente, a conclusão em um conhecimento de Inteligência deve estar ali, em potência, esperando ser revelada. Embora gere algo novo, que não estava dado, não é uma conclusão inventiva, tirada da ficção ou da simples convicção pessoal (BRASIL, 2016; CRUZ, 2019).

Os relatórios de Inteligência podem ser descritivos, explicativos, mas não propositivos ou prescritivos. Eis um "julgamento" vedado ao analista: a função de assessoramento não permite que haja escolha ou sugestão sobre alternativas, já que só o usuário da AI tem legitimidade para tanto. Neste sentido, do analista de Inteligência espera-se imparcialidade profissional, sem *advocacy*, ainda que tenha suas preferências humanas; não é o profissional um "acelerador de mudanças", não lhe cabe poder executivo, e o valor da impessoalidade, da isenção analítica, do não aproveitamento dos conhecimentos a que tenha acesso em causa própria, decorrem da própria natureza do serviço e contribuem para a profissionalização da atividade (BRASIL, 2016; CEPIK e ANTUNES, 2004).

Sem ser prescritiva, a análise deve trazer um conhecimento que não estava disponível até então. Assim, ainda que eventualmente baseada em fragmentos expostos em fontes abertas, espera-se que agregue, que incorpore ao que o usuário já sabe, um

raciocínio baseado nessas pequenas peças (interpretação), que lhe traga a segurança da avaliação dessas peças e o encadeamento lógico dos eventos (CRUZ, 2019).

Em suma, a comparação entre as duas funções (analista de Inteligência e juiz) propicia perceber como o olhar humano, na ação de interpretar, pode ser direcionado a caminhos distintos nessas atribuições públicas. O analista busca interpretar um sistema social (LUHMANN, 2006) para identificar atores envolvidos, ligações externas e motivações, ou seja, realiza uma análise que é, ao fim, estratégica. Já o juiz busca primeiro esclarecer uma situação fática do sistema social a partir de contornos limitados, sem visão estratégica, para posterior encaixe dessa realidade, desse ato, no ordenamento jurídico. De todo modo, há semelhanças entre as atividades do magistrado e do analista de Inteligência, ainda que segmentadas, como veremos a seguir, pelo objetivo da descrição do sistema social.

De um lado, a Inteligência é ferramenta de assessoramento, sua interpretação não será aplicada pelo analista. De outro, o juiz interpreta e aplica o que interpreta, formula a sentença e a impõe como solução para o conflito. E se, no Direito, a interpretação não será verdadeira ou falsa, mas sim aceitável ou inaceitável (GRAU, 2005), o que se passa com os profissionais de Inteligência é diferente?

> Lembro a observação de Frosini: a decisão judicial considera e é determinada pelas palavras da lei e pelos antecedentes judiciais; pela figura delitiva que se imputa; pelas interpretações elaboradas pelas duas ou mais partes em conflito; pelas regras processuais; pelas expectativas de justiça nutridas pela consciência da sociedade; finalmente pelas convicções do próprio juiz, que pode ser influenciado, de forma decisiva, por preceitos de ética religiosa ou social, por esquemas doutrinais em voga ou por instâncias de ordem política. E mais: o juiz decide sempre dentro de uma situação histórica determinada, participando da consciência social de seu tempo, considerando o direito todo, e não apenas um determinado texto normativo (*ibidem*, p. 38).

Também há muito em jogo para o profissional de Inteligência, por exemplo: sua interpretação sobre a realidade considera os planos de Inteligência ou requerimentos do usuário; sua análise não pode ser determinada pelas expectativas do usuário, mas as compreender é fundamental para orientá-lo sobre a completude do que produz; é a situação histórica atual que lhe informa sobre atores e o papel que representam; tudo o que fizer deverá estar submetido a normativos da própria instituição, leis e objetivos constitucionais.

Em virtude de estar imerso em circunstâncias de toda ordem, trabalhar com fatos frequentemente pouco conhecidos e ser humano, o profissional de Inteligência pode falhar, obviamente, como podem os juízes. O momento da decisão judicial é, como já dito, um ato de prudência e reflexão muito íntimo, cercado de ritos, embora sem métodos muito

claros, que culmina com uma resposta entre outras possíveis, igualmente autênticas. Diferentemente, o analista, guiado pela Metodologia de Produção do Conhecimento (MPC), tem esperança da conclusão verdadeira. Se a conclusão que alcança for apenas aceitável, deverá examinar o quão aceitável ela é: se for mera possibilidade, deve descartá-la; se for probabilidade, deve exprimir isso e demonstrar que o estado de sua mente não alcançou a certeza, mas está mais próximo dela que da dúvida. É a busca pela verdade – e não pelo aceitável – que norteia a AI (BRASIL, 2016).

Na produção de Conhecimentos de Inteligência, observam-se detidamente as frações significativas para que se possa concluir algo sobre o objeto de análise, estudam-se causas, responsabilidades, consequências e desdobramentos futuros. Assim, são identificadas evidências que são relacionadas logicamente a fim de se sustentar um raciocínio. Idealmente, após o tema em estudo receber atenção ao longo do tempo, o acompanhamento realizado pelo profissional de Inteligência estará maduro a ponto de permitir o entendimento e a ponderação de seus aspectos mais importantes. (CRUZ, 2019).

É a Metodologia que ajuda o analista a reunir dados e conhecimentos com critério, a decompô-los e reuni-los novamente com crivo de pertinência e significância, de forma que o conjunto de possibilidades de interpretação colocado à disposição do profissional de Inteligência seja coerente, ordenado e dotado de credibilidade.

Comparativamente, a interpretação judicial vincula-se à lei. Eros Grau entende que "a abertura dos textos de direito, embora suficiente para permitir que o direito permaneça ao serviço da realidade, não é absoluta" (2005, p. 52), de forma que o juiz está atado à legalidade, ou, como ensina Hans Kelsen, adstrito a um *"Bild"*, um enquadramento normativo (MAGALHÃES, 1999, p. 429). O analista também está atado em sua interpretação do mundo: a Metodologia impede que a conclusão não derive de evidências listadas pelo profissional, proíbe que as evidências não tenham pertinência ou relevância para o tema que estudado (BRASIL, 2016), e exige embasamento à conclusão, similar à justificação da sentença do juiz.

Se, no Direito, é esperado que haja desacordo teórico, na AI, ele já não cabe. A objetividade dos relatórios de Inteligência centra-se em reportar e compreender fatos e eventos, selecionar os mais prováveis, e não argumentar a favor ou contra fatos e eventos ou problematizar convenções morais (BRASIL, 2016).

Por fim, se no Direito há juízos valorativos, aqueles que exprimem o "dever ser" ou o "não dever ser", e raciocínios éticos sobre algo estar "certo ou errado", na AI só cabem os juízos enunciativos (BRASIL, 2016), que informam "aquilo que é" e propiciam conclusões com base em "verdadeiro ou falso".

A imparcialidade no serviço público: servidores e atores políticos

No Brasil, a legitimidade do trabalho da AI, assim como a dos juízes[2], é burocrática e técnica, não política, isto é, os profissionais do setor público que atuam na área são, em regra, concursados e estáveis. Assim, extraem o fundamento de seu trabalho não do voto popular em eleições democráticas, mas de processos administrativos que visam a selecionar profissionais capacitados e de reputação ilibada para cumprir funções técnicas previamente definidas na legislação afim (OLIVIERI, 2011, *passim*).

Considere-se o método de seleção destas duas categorias, quais sejam, profissionais técnicos e políticos eleitos, suas semelhanças e diferenças. Em ambas, são buscados aqueles que se destacam em algum campo, conforme o princípio da distinção[3]: na política, a eleição democrática moderna (ao contrário da democracia ateniense, por exemplo) não funciona à base da lógica da escolha randômica, aleatória, mas sim da escolha de candidatos cujas virtudes – atribuíveis a critérios pessoais, partidárias, programáticas ou outras – são específicas, superiores às dos concorrentes; na seleção burocrática, que, no caso brasileiro, é feita via concursos, a lógica meritocrática também abdica da aleatoriedade e pretende escolher os mais qualificados entre os que se candidatam aos testes previstos nos editais de seleção.

Quando se discute o preenchimento de cargos em comissão e de confiança nos órgãos de governo cuja maioria dos postos é ocupada por profissionais concursados e estáveis, aponta-se a existência de uma "zona cinzenta", visto que o método de seleção dos ocupantes de tais cargos é misto. Dada tal circunstância, os profissionais que são simultaneamente concursados e ocupantes de cargos em comissão e de confiança extrairiam parte de sua legitimidade para o exercício do cargo indiretamente da política, ou seja, da autoridade investida nos eleitos democraticamente, que possuem o poder para nomear os ocupantes de tais postos (OLIVEIRI, 2011, p. 1403 e 1405).

2 Importante ressaltar que há uma diferença primordial entre os analistas de Inteligência, juízes e Ministros do Supremo Tribunal Federal (STF). Os primeiros e segundos são empossados a partir de concurso público (sem ignorar o dispositivo do quinto constitucional), enquanto os ministros do STF encontram sua gênese legitimadora em uma indicação política (indicados pelo Presidente da República e sabatinados pelo Senado Federal). É relevante essa diferenciação para compreender que há, em tese, maior abertura para incorporação de elementos principiológicos e interpretativos em Ministros do STF do que há para juízes concursados ou analistas de Inteligência, mesmo que também aos Ministros do STF seja obrigatório o limite estabelecidos pela moldura normativa.

3 O conceito é delineado por Manin conforme as seguintes citações: "O que contava não era somente o *status* social dos representantes definido em termos absolutos, mas também (e possivelmente mais importante) sua posição relativa com respeito à de seus eleitores. O governo representativo foi instituído com plena consciência de que os representantes eleitos podiam e deviam ser cidadãos eminentes, socialmente diferentes dos que os elegiam. Podemos chamar a isso o 'princípio da distinção'" (MANIN, 2010, p. 87-8) e "os representantes devem ser diferentes de seus constituintes, pois o governo republicano, como qualquer outro, requer que o poder seja confiado àqueles que possuem 'mais sabedoria' e 'mais virtude', isto é, a pessoas superiores e diferentes de seus concidadãos" (MANIN, 2010, p. 209-10).

Entretanto, tal fração da legitimidade política não se sobrepõe à legislação que define os limites para a atuação dos ocupantes de cargos comissionados e de confiança. Por exemplo, a função de assessorar o tomador de decisões, razão de ser da AI, é definida em instrumentos próprios, e suas fronteiras são demarcadas nesses regramentos. Logo, fica impossibilitado, também, um encontro indevido entre a atividade política de sugerir, indicar e desenhar políticas públicas, implícita na legitimidade política, e os vários ramos que possuam alguma similitude dentro da AI, como a descrição de políticas públicas (OLIVEIRA, 2009, p. 140). Enquanto não é admissível para os profissionais técnicos – sejam juízes ou analistas de Inteligência – fazer interpretações iluminadas por filiação partidária, esse comportamento é esperado de um ator político. O mandato dos ocupantes de postos políticos possui irredutível componente partidário no sistema político adotado no Brasil, que não admite, por exemplo, candidaturas avulsas, e concede a líderes de partido e bancada legislativa forte poder de agenda (LIMONGI e FIGUEIREDO, 1997, p. 92-5).

Nas ciências humanas, já é lugar-comum a afirmação que destaca a virtual impossibilidade da neutralidade completa, absoluta na produção do conhecimento científico. Tal afirmação pode ser aplicada em qualquer área do saber que trabalhe com métodos lógico-racionais e empíricos, como é a AI. É dificuldade constante a busca da identificação e da superação de vieses cognitivos e preferências pessoais ou grupais em documentos de Inteligência (MACHADO, 2018, p. 7-10).

Entretanto, a AI não pode correr o risco, especialmente quando há confluências com atividades cuja legitimidade é precipuamente política, de consentir com a parcialidade ao aceitar que a completa neutralidade é impossível. Caso tal fenômeno se transformasse em realidade, haveria um cenário *self-defeating* para a AI, visto que seu diferencial, o assessoramento ao processo decisório com conhecimentos oportunos e úteis (BRASIL, 2016), concederia espaço para um assessoramento paroquial, dependente da visão específica (parcial) do redator do documento de Inteligência.

A adequação da burocracia a seu papel definido nos instrumentos legais democraticamente decididos é também função do amadurecimento da cultura política. O amadurecimento institucional do Brasil explica a adesão dos funcionários públicos a esses papeis. Assim, a busca de imparcialidade coincide com a permanência dentro da legalidade. Isso tende a impossibilitar qualquer tentativa sub-reptícia de dirigismo burocrático ilegítimo: por exemplo, sugerir ou desenhar políticas, caso um órgão não possua tais competências (LYNCH, 2017, p. 13). A questão foi enunciada por Olivieri (2011):

> Na medida em que os burocratas, com a reforma meritocrática e o abandono da burocracia representativa, deixam de ser cidadãos comuns com a função de legitimamente representar grupos e interesses da sociedade dentro do Estado, surge a possibilidade de eles não serem fiéis às escolhas ou preferências do povo(...) A consequência natural do surgimento dessa "desconfiança" contra a burocracia de mérito é a necessidade de controlar os burocratas para que eles sejam fiéis aos interesses dos representantes do povo, dos únicos representantes que permaneceram no Estado: os legisladores (*ibidem,* p. 1410-11).

Assim, há a necessidade de um equilíbrio entre controle político e flexibilidade que vise a respeitar as inclinações políticas da sociedade, traduzidas pelas urnas via processo eleitoral. Entretanto, esse equilíbrio tange também as expectativas e o modelo de funcionário público que existirá na sociedade.

O modelo positivado outrora em clássicos da literatura e das ciências humanas (KAFKA, 2009, e ARENDT, 2013), do burocrata acrítico e amorfo que cumpre quaisquer ordens sem questionar ou analisar o conteúdo e os impactos de suas decisões, foi, devido à barbárie nazista, devidamente desprezado no pós-2ª Guerra Mundial. No Brasil, não foi diferente, especialmente após o retorno do regime democrático, não só por esse comportamento atentar contra a legislação que rege o funcionalismo público brasileiro e por ferir requisitos básicos de ética, mas também pela emergência de novos modelos de gestão pública.

Essas teorias objetivaram, ainda que de formas distintas, afirmar um novo papel para o funcionalismo público, ao discutir, respectivamente, sua eficiência e sua capacidade de agência (ALESSIO e AMBROZIO, 2016, p. 327). Essa questão foi debatida por Oliveira (2009), que afirma que há um equilíbrio possível e já encontrado no funcionalismo público federal:

> A livre nomeação, ou seja, a nomeação de dirigentes feita de forma arbitrária, sem qualquer requisito, é muitas vezes apresentada como uma decorrência necessária da democracia. Os políticos eleitos precisariam construir uma ligação com a burocracia que, segundo esta opinião, é resistente a mudanças e poderia obstar os programas políticos. Não observamos qualquer situação em que dirigentes se queixassem de insubordinação, quer fosse de servidores concursados, quer de outros funcionários (...) A ideia weberiana de uma burocracia ciosa de seus segredos, mais ou menos fechada em face de intervenções externas, políticas, não foi confirmada em momento algum por nossas observações cotidianas da burocracia pública brasileira (*ibidem,* p. 50).

Note-se que algumas carreiras apresentam travas legais para a indicação para determinados postos, por exemplo, por necessidade técnica especializada. Dessa forma, é possível que o legislador estabeleça critérios específicos para composição de determinadas esferas públicas, como ocorre com o Diretor da Polícia Federal, os Ministros do STF e os cargos de gestão, que são divididos em "cargos de confiança" e "funções de confiança".

Ao mesmo tempo em que se nega o

burocrata moldado em Eichmann (ARENDT, 2013), também a burocracia ativista que deseja romper seus limites democraticamente demarcados representaria um risco à democracia e à própria legitimidade de sua atuação profissional. Ao imiscuir-se nesse ativismo, essa burocracia nubla as diferenças entre o que é assessoramento e desempenho de funções técnicas e o que é atividade *self-serving* e disputa por recursos e competências para, primordialmente, avançar os interesses de um determinado grupo ou carreira pública (LYNCH, 2017, p. 13). Hipoteticamente, essa situação se verificaria, na AI, com o uso dos produtos de Inteligência para disseminar uma percepção inflada *(fearmongering)* dos riscos de atentados terroristas ou, de forma similar, a defesa entre magistrados da judicialização crescente de casos de mero dissabor do cotidiano para que, em uma ou noutra hipótese, aumentasse a importância de cada carreira.

Assim, há duas faces da parcialidade a se considerar: por um lado, a que engendra a perda do diferencial do profissional da AI; por outro, a que busca avançar seus próprios interesses ao disfarçá-los como cumprimento da função e defesa do bem público, mesmo que com desrespeito aos limites legais de sua atuação. Lindblom (1980, *apud* FERREIRA, 2015) explica que:

> (...) uma das funções dos servidores, ou burocratas, é subsidiar o processo de decisão por meio de análises técnicas; reconhece que os burocratas desempenham papel importante no processo de decisão política. O autor afirma que no senso popular se acredita que os governos precisam se valer mais da pesquisa e das análises para solução de problemas relacionados com as políticas governamentais. Entretanto, apesar de as pessoas acreditarem nesse princípio, desejam que a decisão política se mantenha sempre como um processo político, ou seja, as autoridades devem usar os serviços de analistas e técnicos sem abdicarem de suas funções políticas (*ibidem*, p.148).

Lindblom *(ibidem)* também pontua que, no entanto, ao se executar uma política pública, passo posterior a assessoramento e análise, ocorre uma inevitável politização dos servidores e burocratas, pois "a maioria dos atos administrativos fazem ou alteram *(sic)* políticas já formuladas ao implementá-las (...) São atos que formulam, reformulam e muitas vezes ampliam uma política pública já decidida no espaço legislativo" *(ibidem)*. Esse fenômeno transcorre por razões práticas, pois:

> (...) nenhum legislador tem condições de enunciar completamente uma política que cubra todas as contingências, todos os casos possíveis. Assim (...) os formuladores de políticas públicas permitem que os responsáveis pela administração daquela política determinem muitos elementos da concepção apenas esboçada. Esse é um importante espaço de atuação da burocracia. (*ibdem*, p. 149).

O profundo debate sobre os limites entre uma burocracia ativista e uma burocracia avessa a tal postura, implícito pela estrutura complexa na qual está inserida fração relevante do serviço público contemporâneo, não requer tratamento

adicional aqui. Essas considerações possuem, no entanto, um significado distinto (e mais direto) para o serviço de Inteligência brasileiro.

Dado que a AI é uma atividade cuja competência se localiza majoritariamente na esfera do assessoramento e da análise, não na execução de políticas públicas (BRASIL, 2016), não há justificativa para parcialidade do profissional (OLIVEIRA, 2009, p. 19). Assim, há um contraste dos profissionais de Inteligência em relação às carreiras do poder executivo que se veem obrigadas a percorrer este "importante espaço de atuação da burocracia" em vista de sua função de executores de políticas públicas (D'ARAÚJO e LAMEIRÃO, 2011, p. 94, e LOUREIRO e ABRUCIO, 1999, p. 70).

Considerações finais

O exercício de comparar profissionais de Inteligência e juízes pode parecer, em princípio, descabido: são vinculados a Poderes diferentes na República, têm missões próprias e reconhecimento público também desigual. Mas ambos são intérpretes de fatos e ideias, profissionais cujas tarefas, muitas vezes, são descritas como "arte" e não como "técnica", servidores públicos de quem se espera isenção científica, talento inato, conhecimento amplo, abnegação. É, assim, útil compará-los para compreender melhor cada ofício.

Aqui, foram ressaltados os limites para a interpretação aplicada por esses profissionais, seja porque estão atados a um sistema integrado de Direito (como os juízes), seja porque são guiados por uma Metodologia de Produção do Conhecimento (no caso dos analistas). Foram sinalizadas também armadilhas e críticas quando eventualmente a performance técnica extrapola para uma intervenção no mundo e confunde o ser profissional com o ator político.

Afinal, em um regime democrático, juízes, profissionais da AI e outros funcionários públicos estáveis devem permanecer dentro dos papeis constitucionais e legais determinados a eles. Constituem parte do suporte administrativo, legal e técnico da democracia e da sociedade. Se não há possibilidade legal de que façam mais do que a lei e a ética autorizam – ou seja, não podem lançar-se à busca da função de arquitetos, protagonistas ou demiurgos da sociedade – tampouco a sociedade pode depositar essas expectativas sobre esses atores.

Finalmente, trabalhos posteriores poderão comparar outros aspectos presentes no ofício dos profissionais de Inteligência e de outras espécies de servidores, à guisa de exemplo, a imparcialidade exigida de auditores, juízes e profissionais de Inteligência, a oferta de assessoramento oportuno e confiável ao processo decisório, e como a Atividade de Inteligência se

compara com o assessoramento realizado por diversos profissionais na administração direta.

Referências

ALESSIO, Maria Fernanda; AMBROZIO, Lucas. A composição da alta burocracia no Brasil e no Chile à luz das dimensões da legitimidade e do desempenho. *Revista do Serviço Público,* v. 67, nº 3, p. 319–350, 2016.

ARENDT, Hannah. *Eichmann em Jerusalém.* São Paulo: Companhia das Letras, 2013.

BARROSO, Luis Roberto. Judicialização, Ativismo Judicial e Legitimidade Democrática. *Revista Atualidades Jurídicas – Revista Eletrônica do Conselho Federal da OAB.* 4ª ed. Janeiro/Fevereiro 2009.

BONAVIDES, Paulo; ANDRADE, Paes de. *História Constitucional do Brasil.* 3ª ed. Rio de Janeiro: Paz e Terra, 1991.

BRASIL. Gabinete de Segurança Institucional. Agência Brasileira de Inteligência. *Portaria nº 244, de 23 de agosto de 2016.* Doutrina Nacional da Atividade de Inteligência: fundamentos doutrinários. 2016.

CEPIK, Marco; ANTUNES, Priscila Profissionalização da Atividade de Inteligência no Brasil: critérios, evidências e desafios restantes. *In:* SWENSON, Russell G.; LEMOZY, Susana C. [org.]. *Intelligence Professionalism in the Americas.* Washington, DC: Center for Strategic Intelligence Research, p. 109-154, nov. 2004.

CORRÊA, Andrey L.M. *et al.*. Un balance de los sistemas de control de constitucionalidad como instrumento de garantía de las constituciones material y formal. *Journal of Institutional Studies,* v. 3. p. 525-561, 2017.

CORRÊA, Andrey L. M. *et al.*. A Suprema Corte Norte-Americana e a Genealogia Decisional a partir do Perfil dos Julgadores: Uma Análise Fundada na Obra Born to Rebel de Frank Sulloway. *In:* Patrícia Alves Cardoso; Moacir Henrique Júnior; (Org.). *Interdisciplinaridade no Campo das Ciências Sociais Aplicadas:* O Universo Jurídico e Suas Interlocuções. Ituiutaba: Barlavento, 2017, v. 1, p. 158-186.

CRUZ, Anna. *Aprimoramento da Capacidade Analítica e Avanço na profissionalização da Atividade de Inteligência.* 2019 (Monografia de fim de Curso de Aperfeiçoamento em Inteligência). ESINT/ABIN, Brasília 2019.

D'ARAÚJO, Maria Celina; LAMEIRÃO, Camila . Dirigentes públicos federais de alto escalão no governo Lula. In: José Celso Cardoso Jr. (Org.). *Burocracia e ocupação no*

setor público brasileiro (Diálogos para o Desenvolvimento). Rio de Janeiro: IPEA, v. 5, p. 91-131, 2011.

FERREIRA, Maria Aparecida Chagas. *Burocracia de Estado e Políticas de Promoção da Igualdade Racial.* 2014 Tese de Doutorado (Doutorado em Sociologia), Instituto de Ciências Sociais da Universidade de Brasília, Brasília, 2014.

GARAPON, Antoine. *O guardador de promessas:* justiça e democracia. Lisboa: Edições Piaget, 1998.

GRAU, Eros. *Ensaio e discurso sobre a interpretação/aplicação do Direito.* Malheiros: 2005.

LAJUS DOS SANTOS, Bernardo. *O princípio da confiança no juiz da causa e a fundamentação das decisões penais.* Dissertação de Mestrado do Programa de Pós-Graduação em Direito da Universidade Federal de Santa Catarina, 2021.

LIMONGI, Fernando; FIGUEIREDO, Argelina. *Bases institucionais do presidencialismo de coalizão.* Lua Nova, São Paulo, n. 44, p. 81-106, 1998.

LINDBLOM, Charles E. *O processo de decisão política.* Brasília: Universidade de Brasília, 1980.

LOUREIRO, Maria Rita; ABRUCIO, Fernando Luiz. Política e Burocracia no Presidencialismo Brasileiro: o papel do Ministério da Fazenda no primeiro governo Fernando Henrique Cardoso. *Revista Brasileira de Ciências Sociais.* São Paulo, v. 11, nº 41, p. 69-89, out. 1999.

LUHMANN, Niklas. *La sociedad de la sociedad.* Mexico: Editorial Herder, 2006.

LYNCH, Christian Edward Cyril. Cultura política brasileira. *Revista da Faculdade de Direito da UFRGS.* Porto Alegre, n. 36, p. 4-19, ago. 2017.

KAFKA, Franz. *The Trial.* Oxford: Oxford University Press, 2009.

KAHNEMAN, Daniel. *Rápido e Devagar:* Duas formas de pensar. Trad. Cássio de Arantes Leite. Rio de Janeiro: Objetiva, 2012.

MACHADO, André Mendonça. O impacto de vieses cognitivos sobre a imparcialidade do conteúdo de Inteligência. *Revista Brasileira de Inteligência.* Brasília, v. 13, p. 9-24, dez. 2018.

MANIN, Bernard. O princípio da distinção. *Revista Brasileira de Ciência Política,* nº 4, p. 187-226, 2010.

MARRIN, Stephen; CLEMENTE, Jonathan. Modeling an Intelligence Analysis Profession on Medicine. *International Journal of Intelligence and CounterIntelligence,* 19, 2006. p. 642-665.

NEUENSCHWANDER MAGALHÃES, Juliana. Sobre a Interpretação Jurídica. *Revista de Direito Comparado.* Vol. 3. Belo Horizonte: Faculdade de Direito da UFMG, 1999.

OLIVEIRA, Nelson do Vale. *O Amadorismo como Traço Distintivo da Burocracia Federal Brasileira.* 2009 Tese de Doutorado (Doutorado em Sociologia). Instituto de Ciências Sociais da Universidade de Brasília, Brasília, 2009.

OLIVIERI, Cecília. 201. *Revista de Administração Pública (RAP).* Rio de Janeiro, v. 45, n. 5, p. 1395-1424, 2011.

SULLOWAY, Frank. *Born to rebel:* Birth order, family dynamics, and creative lives. New York: Pantheon, 1996.

Artigo

6

ANÁLISE DO ASSESSORAMENTO DA ATIVIDADE DE INTELIGÊNCIA: sob a ótica das lentes analíticas *Policy Cycle e Policy Argumentation*

DOI: https://doi.org/10.58960/rbi.2023.18.230

Monique Simões Brasil Batista *

Resumo

Uma das atribuições da Atividade de Inteligência no Brasil é auxiliar a formulação e o desenvolvimento de políticas públicas estratégicas. Para tal, o Sistema Brasileiro de Inteligência e a Agência Brasileira de Inteligência produzem conhecimentos com a finalidade de apontar oportunidades e ameaças à consecução dos objetivos nacionais. Assim, este artigo tem por finalidade aprofundar os estudos sobre lentes analíticas disponíveis no campo de estudo das Políticas Públicas capazes de auxiliar o profissional de Inteligência a refletir sobre as políticas analisadas e a aperfeiçoar o seu assessoramento de acordo com o objeto estudado. Para tanto, dedicou-se à análise das lentes explicativas *Policy Cycle e Policy Argumentation*. Por meio de pesquisa qualitativa e exploratória, os estudos apontam para o uso do modelo de Interpretação Adaptativa, proveniente do campo de estudo Teoria de Inteligência, como possível resposta analítica para buscar lacunas informacionais contemporâneas e, assim, melhorar o assessoramento realizado pela Inteligência brasileira aos decisores governamentais responsáveis por formular e implementar políticas públicas.

Palavras-chave: políticas públicas; Inteligência, *Policy Cycle; Policy Argumentation*; interpretação adaptativa.

ANALYSIS OF INTELLIGENCE ACTIVITY ADVISORY: from the perspective of the Policy Cycle and Policy Argumentation analytical lenses.

Abstract

One of the functions of the Intelligence Activity in Brazil is to help formulate and develop strategic public policies. To this end, the Brazilian Intelligence System and the Brazilian Intelligence Agency produce knowledge in order to point out opportunities and threats to the achievement of national objectives. Thus, this article aims to improve the studies on analytical lenses available in the field of study of Public Policy capable of helping the Intelligence professional to reflect on the analyzed policies and to improve their advice according to the studied object. To this end, this article is dedicated to the analysis of the Policy Cycle and Policy Argumentation explanatory lenses. Through qualitative and exploratory research, the studies point to the use of the Adaptive Interpretation model, from the field of study Theory of Intelligence, as a possible analytical answer to search for contemporary informational gaps and, thus, improve the advice provided by Brazilian Intelligence to decision-makers governments responsible for formulating and implementing public policies.

Keywords: *public policy; Intelligence; Policy Cycle; Policy Argumentation; adaptive interpretation.*

* Mestre em Governança e Desenvolvimento pela Escola Nacional de Administração Pública (Enap). Oficial de Inteligência da Agência Brasileira de Inteligência (Abin).

ANÁLISIS DEL ASESORAMIENTO DE LA ACTIVIDAD DE INTELIGENCIA: desde la perspectiva de los lentes analíticos el Ciclo de la Política y la Política Argumentativa.

Resumen

Una de las atribuciones de la Actividad de Inteligencia en Brasil es ayudar a formular y desarrollar políticas públicas estratégicas. Para ello, el Sistema Brasileño de Inteligencia y la Agencia Brasileña de Inteligencia producen conocimiento con el fin de señalar oportunidades y amenazas para la consecución de los objetivos nacionales. Así, este artículo tiene como objetivo profundizar los estudios sobre lentes analíticos disponibles en el campo de estudio de las Políticas Públicas capaces de ayudar al profesional de Inteligencia a reflexionar sobre las políticas analizadas y a mejorar su asesoramiento de acuerdo con el objeto de estudio. Para ello, se dedicó al análisis de los lentes explicativos: el Ciclo de la Política y la Política Argumentativa. A través de una investigación cualitativa y exploratoria, los estudios apuntan al uso del modelo de Interpretación Adaptativa, del campo de estudio Teoría de la Inteligencia, como una posible respuesta analítica para buscar vacíos informativos contemporáneos y, así, mejorar el asesoramiento que brinda la Inteligencia brasileña a los tomadores de decisiones gubernamentales responsables de formular e implementar políticas públicas.

Palabras clave: *políticas públicas; Inteligencia; Ciclo de la Política; Política Argumentativa; interpretación adaptativa.*

Introdução

A Atividade de Inteligência brasileira é caracterizada pela produção de conhecimentos com a finalidade de apontar oportunidades e ameaças à consecução dos objetivos nacionais (BRASIL, 2016). Uma das atribuições legais da Inteligência brasileira é auxiliar a formulação e o desenvolvimento de políticas públicas por meio do assessoramento dos decisores políticos.

O presente artigo tem o objetivo de analisar a atividade de assessoramento do serviço de Inteligência, realizado pela Agência Brasileira de Inteligência (Abin) e pelo Sistema Brasileiro de Inteligência (Sisbin), a gestores de políticas públicas ministeriais, sob duas lentes analíticas de políticas públicas: *Policy Cycle* de Harold Lasswell (1951), que servirá como modelo inicial de análise, e *Policy Argumentation* de Frank Fischer (2012), que permitirá pensar as novas configurações que o atual contexto exige da Atividade de Inteligência.

Com base nos pressupostos de que o Estado governa por políticas públicas e de que a elaboração e a implementação dessas políticas ocorrem em contexto de incerteza, defende-se que a Atividade de Inteligência, por ter vocação antecipatória, é capaz de revelar, em suas análises, elementos ainda não-disponíveis ao decisor político e, assim, reduzir as incertezas decorrentes de tomadas de decisão relacionadas a situações complexas com elevado fluxo de dados.

Para além desta introdução, o artigo, em um primeiro momento, apresenta os fundamentos do assessoramento de Inteligência no campo de políticas públicas e detalha as atribuições da Abin e o funcionamento do Sisbin. Em seguida, fornece explanações sobre o nascimento e o desenvolvimento do campo de estudos de políticas públicas *(Policy Studies)* e diferencia suas principais lentes explicativas. Depois, apresenta, com maior profundidade, as lentes analíticas *Policy Cycle e Policy Argumentation* e dialoga com as particularidades do trabalho de Inteligência. Na penúltima parte, faz questionamentos sobre os modelos mentais tradicionais predominantes na Inteligência brasileira e sugere a utilização do modelo de Interpretação Adaptativa de Lahneman (2010) como possível resposta analítica aos problemas atuais. Por fim, conclui-se ao retomar os principais pontos abordados na pesquisa e apresenta as contribuições trazidas de cada lente estudada ao aprimoramento do assessoramento de Inteligência.

A pesquisa realizada tem as seguintes características: é básica (não-aplicada), por explicar a relação entre Inteligência e política pública e propor modelo de atuação; qualitativa, por aprofundar questões subjetivas do fenômeno estudado; e exploratória, por buscar maior familiaridade com as abordagens propostas. Como procedimentos técnicos, executou-se uma pesquisa explicativa, bibliográfica e

documental (GIL, 2008).

Assessoramento da Inteligência no campo das políticas públicas

No Brasil, a Atividade de Inteligência é exercida por meio do Sisbin e, principalmente, por seu órgão central, a Abin. Ambos foram instituídos, no contexto de redemocratização nacional, com a publicação em 1999 da Lei nº 9.883.

Diferentemente do anterior Sistema Nacional de Informações (Sisni), em que os demais membros eram subordinados ao Serviço Nacional de Informações (SNI), o Sisbin foi desenhado para funcionar em rede, de modo horizontal, não-hierarquizado e com órgão central coordenador e facilitador do funcionamento do sistema[1]. A Abin foi escolhida como órgão central por se tratar da única instituição do Estado brasileiro que tem a função precípua de atuar com a Atividade de Inteligência. Todos os demais integrantes do sistema têm a Inteligência como atividade acessória.

O Sisbin tem por objetivo integrar as ações de planejamento e execução da Atividade de Inteligência do país, com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional (Decreto nº 11.693/2023). Apesar de o Presidente da República ser o usuário maior dos conhecimentos produzidos pelo Sisbin, ele não é o único. A principal usuária do sistema de Inteligência é a estrutura da Presidência da República, aí incluído o Gabinete de Segurança Institucional (GSI) – instância à qual a Abin tradicionalmente se subordinava – e a Casa Civil – atual instância superior da agência[2] –, por seu importante papel de articuladora de políticas públicas. Ressalta-se que os ministérios também são usuários habituais do sistema e recebem documentos individuais, produzidos pelos órgãos partícipes, ou documentos colegiados, produzidos pelo próprio Sisbin.

Com o intuito de entender as características do assessoramento realizado pelo profissional de Inteligência no campo das políticas públicas, optou-se por, inicialmente, explicar o nascimento, o desenvolvimento e a atual configuração

1 Para entender o funcionamento em rede deste sistema, além da Lei nº 9.883/1999, que criou o Sisbin e a própria Abin, e do Decreto nº 11.693/2023, que dispõe sobre a organização e o funcionamento do Sisbin, deve-se utilizar os corpos normativos que regulamentam essa atuação. O primeiro e mais abstrato deles é a Política Nacional de Inteligência (PNI), aprovada pelo Decreto nº 8.793/2016, seguido da Estratégia Nacional de Inteligência (Enint), que tem uma característica mais tático-estratégica, aprovada por Decreto de 15 de dezembro de 2017. Por fim, há o Plano Nacional de Inteligência (Planint), que rege a operacionalização do sistema e foi publicado em portaria sigilosa com acesso somente aos membros do Sisbin. De forma geral, o Planint estabelece os eixos estratégicos de atuação conjunta e reitera o papel da Abin como coordenadora e operacionalizadora dessa ação coletiva, inclusive ao capacitar e facilitar a intermediação entre os órgãos membros do sistema.

2 Com a publicação no Diário Oficial da União do Decreto nº 11.426, de 1º de março de 2023, a ABIN passou a fazer parte da estrutura da Casa Civil. Entre o breve período de 2015 e 2016, a Agência também teve uma subordinação civil, integrando a Secretaria de Governo. Nos demais anos, era parte integrante da estrutura do GSI (de 1999 a 2015 e depois de 2016 a fevereiro de 2023).

do campo de estudo em questão, para, a posteriori, analisar a interação entre o profissional de Inteligência e o gestor de políticas públicas sob a ótica das referidas lentes analíticas de *Policy Science: Policy Cycle*, de tradição positivista, e *Policy Argumentation*, de tradição pós-positivista.

Desenvolvimento do campo de estudos políticas públicas

O estudo das Políticas Públicas, *Policy Studies*, como um campo de estudo próprio, desvinculado da Ciência Política, é razoavelmente novo. O campo surgiu a partir da obra de Harold Lasswell *The Policy Sciences*, organizado com Daniel Lerner (1951). No primeiro capítulo, apresenta sua proposta de *Policy Orientation* e defende o reconhecimento da existência deste novo campo de estudos: as Políticas Públicas.

Fundamentado na tradição positivista, o campo nasce amparado nas noções de racionalidade instrumental, valoração do conhecimento especializado e resolução analítica dos problemas públicos, e consagra a teoria explicativa do ciclo de políticas públicas *(Policy Cycle)*, que, até hoje, continua a mais conhecida pelo público geral.

> Em linhas gerais, a abordagem de Lasswell, ainda que tenha mudado um pouco de configuração ao longo das décadas seguintes, apresentava-se desde o começo como uma ciência social aplicada à democracia, de filiação declaradamente pragmática, de natureza normativo-prescritiva, voltada para a resolução racional-instrumental de problemas públicos, de composição multidisciplinar e amparada pelo conhecimento especializado (BOULLOSA, 2019, p. 91).

Na academia, surgiram três principais reações à proposta de Lasswell:

> (i) a ampla maioria concordou com suas ideias;
>
> (ii) uma minoria concordou com as premissas gerais do modelo, mas questionou a racionalidade linear-sequencial e apresentou outros modelos de racionalidade; e
>
> (iii) uma minoria menos expressiva discordava da construção de um novo campo de estudos a partir de uma única abordagem e do modelo de racionalidade proposto.

Os dois primeiros grupos se aproximaram e, atualmente, são considerados o *mainstream* no campo de políticas públicas. O último, mais destoante, passou a ser conhecido como estudos críticos em políticas públicas, por questionar o excesso de racionalidade linear e, assim, propor novos modelos de racionalidade para estudar as políticas públicas[3].

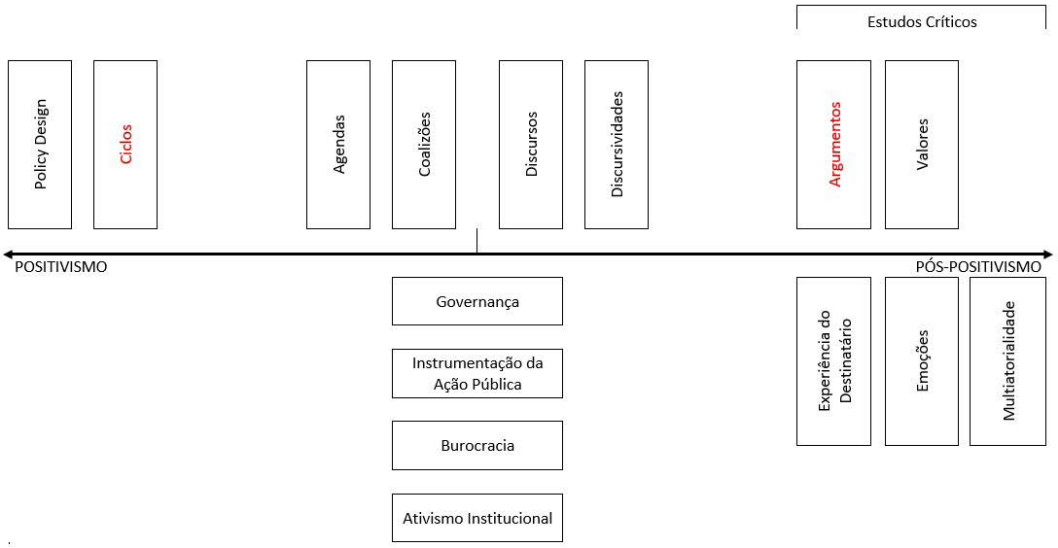
Amparados na chamada virada linguístico-argumentativa, movimento interdisciplinar

3 A saber: a racionalidade comunicativa, a racionalidade discursiva, a racionalidade argumentativa, a racionalidade no contexto, a racionalidade prática e, até, a racionalidade afetiva.

que agregou a possibilidade de compreender as políticas públicas do ponto de vista do significado, e sob a influência da racionalidade comunicativa de Habermas (1986), acadêmicos que compunham o terceiro grupo passaram a pensar as relações sociais e de poder presentes nas políticas públicas a partir de textos, ou análogos de textos, narrativas, argumentos, valores e quadros valorativos (BOULLOSA, 2019).

Assim, atualmente, no campo de estudo de políticas públicas, existem múltiplas possibilidades interpretativas[4] que ainda estão em pleno processo de desenvolvimento. A figura 1 apresenta o panorama geral das lentes analíticas e as situa nas tradições positivistas e pós-positivistas do campo de estudo de política pública.

Figura 1 - Lentes Analíticas Políticas Públicas



Fonte: elaborada pela autora

4 As principais lentes analíticas de tradição positivistas são as abordagens por policy design e por ciclos, mais ao extremo, e as abordagens por agendas e por coalizões, menos ao extremo. Com relação à tradição pós-positivista, destacam-se as abordagens por discursos e discursividades, menos ao extremo, e as abordagens por argumentos e valores, mais ao extremo. Ainda existem as lentes analíticas que buscam fazer pontes entre as tradições (abordagens por governança, pela instrumentação da ação pública, por burocracia e pelo ativismo institucional) e as novas lentes (abordagens pelas experiências do destinatário, por emoções e multifatorialidade).

As distintas lentes analíticas condensam conjuntos de argumentos, ideias e modelos que definem os modos como os envolvidos nos processos de políticas públicas interpretam, problematizam e propõem alternativas. Ao se considerar que a atuação em processos de políticas públicas depende da interpretação dos analistas e que estas interpretações são feitas a partir de lentes analíticas próprias, e que os conteúdos e redes de significado que estruturam as lentes individuais também se articulam em redes mais profundas de valores e identidades profissionais, faz-se necessário buscar uma análise reflexiva sobre os conteúdos e significados que estruturam as lentes interpretativas dos analistas que trabalham com políticas públicas.

Assim, com o intuito de analisar a influência do pensamento positivista e pós-positivista na Atividade de Inteligência, decidiu-se por analisar o papel do assessoramento de Inteligência a partir das lentes interpretativas Policy Cycle de Harold Lasswell (1951) e a Policy Argumentation de Frank Fischer (2012).

Lente analítica *Policy Cycle*

A *Policy Cycle*, desenvolvida pelo sociólogo e cientista político Harold Lasswell, foi a primeira lente analítica apresentada no campo de estudos de políticas públicas e, por isso, é considerada basilar para o desenvolvimento posterior do campo e das análises subsequentes de políticas públicas.

> A ideia de modelar o processo de construção de política pública em termos de fases foi apresentada pela primeira vez por Lasswell. Como parte de sua tentativa de estabelecer uma multidisciplinar e prescritiva ciência da política pública, Lasswell introduziu (em 1956) um modelo de construção de política pública composto de sete fases: inteligência, promoção, prescrição, invocação, aplicação, término e avaliação (...). Hoje, a diferenciação entre definição de agenda, elaboração de políticas, tomada de decisão, implementação e avaliação (que, eventualmente, leva ao término) tornou-se a maneira convencional de se descrever a cronologia de um processo de construção de política pública (JANN; WEGRICH, 2007, p. 43, tradução nossa).

De acordo com o modelo, a política pública possui um ciclo de vida baseado em uma dinâmica temporal e fases determinadas. O ciclo apresentado no presente artigo encontra-se sintetizado em seis fases. Primeiramente, há a fase de Recepção de Demandas, período em que o governo recebe, de diversos atores da sociedade, problemas a serem resolvidos e oportunidades que precisam ser aproveitadas. Depois ocorreria a fase de Formação da Agenda, entendida como o processo de seleção do que entra ou não na lista de prioridades. A próxima fase seria a Formação de Alternativas, em que são apresentados as ações e instrumentos que podem resolver o problema. A quarta fase seria a Seleção de Opções, ou seja, a escolha da melhor alternativa. A quinta seria a fase da Implementação, momento em que a ação política se transforma em algo concreto. Por fim, ocorreria a Avaliação, isto é, a análise do benefício

e do custo da implantação da política pública, momento em que os resultados da intervenção governamental na sociedade são mensurados e informações úteis são geradas para novas políticas públicas.

Ancorada na tradição positivista, a lente *Policy Cycle* defende a existência de uma racionalidade instrumental, voltada à resolução analítica de problemas considerados de relevância pública e alicerçada no saber especializado. Nesta abordagem, a tomada de decisão é considerada o principal instrumento de política pública e, portanto, toda a produção de informações deveria alimentar ou diminuir os riscos envolvidos dessa decisão.

Portanto, a abordagem da *Policy Cycle* favorece a compreensão da função informacional da Atividade de Inteligência, que, como já foi mencionado anteriormente, tem por atribuição auxiliar a formulação e o desenvolvimento de políticas públicas por meio do assessoramento dos decisores políticos, ao participar do processo como um vetor de conhecimento especializado que reduz as incertezas, organiza as complexidades e contribui para o sucesso dessas políticas estratégicas.

Outra característica que aproxima a forma como foi estruturada a Atividade de Inteligência da lente interpretativa em questão é o modelo de produção do conhecimento de Inteligência, que também segue a tradição positivista. Foi desenvolvido sob a perspectiva de estágios projetados para atuar em função do processo decisório e tem como pontos inicial e final a política, ou seja, o assessoramento do decisor público.

O ciclo de Inteligência, como ensinado nos fundamentos doutrinários da Atividade de Inteligência, possui cinco fases distintas: Política, Planejamento, Reunião, Processamento e Difusão. Na instância Política do ciclo, são estabelecidos os objetivos de governo e formuladas as políticas públicas. Na fase do Planejamento, a política é assimilada pelo órgão de Inteligência e se torna orientação de trabalho. Nas fases de Reunião e Processamento, o profissional de Inteligência realiza a obtenção de dados, processa-os a partir de metodologia analítica própria da Atividade de Inteligência (Metodologia de Produção do Conhecimento – MPC) e, por fim, na fase de Difusão, o conhecimento é entregue ao decisor político.

O ciclo de Inteligência organiza-se a partir de uma perspectiva hierarquizada *(top-down)* de formulação de políticas públicas e de demanda por informação. Tal perspectiva, por simplificar a realidade e separar as fases de formulação e implementação das políticas ou as fases de produção de conhecimento de Inteligência, acaba por desconsiderar o papel do conhecimento, das ideias e da aprendizagem

como variáveis independentes que afetam o caráter informacional de todas as etapas do processo de formulação e implementação de políticas públicas.

> (...) os estudos de implementação revelaram que uma separação clara entre a formulação de políticas públicas e sua implementação dificilmente reflete como se faz políticas públicas no mundo real, nem em termos de qualquer sequência hierárquica ou cronológica (primeiro formação, depois implementação), nem em termos dos atores envolvidos (JANN; WEGRICH, 2007, p. 55, tradução nossa).

Além disso, os processos contemporâneos de políticas públicas, caracterizados pela complexidade crescente em diferentes níveis, bem como pela incerteza, apontam para a falência de um modelo positivista de intervenção baseada na racionalidade instrumental e aplicada ao tratamento isolado dos problemas públicos (FISCHER, 2016).

> Ainda que este projeto inspire grande parte do *mainstream* dentro do campo de estudos em políticas públicas, seus limites empiricistas acabam por demandar uma redução cognitiva forte para que seus analistas possam isolar analiticamente as partes dos problemas que desejam tratar. A força projetual é tamanha que frequentemente parte dos seus problemas de implementação acabam *(sic)* por ser atribuídos prematuramente às idiossincrasias do contexto de implementação, reforçando o fetiche pelo processo racional linear de projetação de soluções para problemas públicos, bem como a supremacia do conhecimento especializado, insistindo na separação infértil entre política e políticas públicas (BOULLOSA, 2019, p. 93-94).

Essas limitações analíticas da lente *Policy Cycle* também existem no modelo tradicional de pensar o assessoramento da Atividade de Inteligência, pois a complexidade dos problemas públicos contemporâneos, agravados em tempos de crise, exige novas formas de olhar e novos modelos normativos de pensar que deem conta de suas incertezas e magnitudes.

Lente analítica *Policy Argumentation*

Por considerar ser importante o debate sobre o assessoramento promovido pela Atividade de Inteligência em uma lente analítica de tradição pós-positivista, decidiu-se analisar como se dá este relacionamento sob a ótica do campo de estudos chamado *Policy Argumentation*. Para a lente em questão, a linguagem é o elemento central para todas as etapas do processo político. Frank Fischer, John Forester e Herbert Gottweis (1993; 2012), principais responsáveis pelo desenvolvimento da escola de estudos críticos em políticas públicas, afirmam que a política pública é produto da argumentação, cujo simbolismo deve ser estudado.

Além disso, os autores defendem que os argumentos de política e planejamento estão intimamente envolvidos com as relações de poder (em disputa): incluem as preocupações de alguns e excluem as de outros, distribuem responsabilidades e causalidades e empregam estratégias políticas particulares de enquadramento

de problemas. Todas essas dinâmicas alterariam o desenho, a escolha e a avaliação das políticas públicas implementadas.

A virada linguístico-argumentativa defende que o desafio dos planejadores e analistas de políticas está além da definição do problema ou da apresentação da solução. Para trabalhar bem e em tempo real, estes profissionais devem apresentar argumentos práticos que sejam coerentes e convincentes a seu público-alvo (FISCHER; FORESTER, 1993).

Este desafio é compartilhado pelo profissional de Inteligência que necessita adaptar seu produto de assessoramento à linguagem do decisor-cliente, sem esquecer de adotar a metodologia de produção da Inteligência. O analista de Inteligência está, cada vez mais, sendo cobrado a identificar, elaborar e produzir conteúdo assertivo e dinâmico, que, além de ser relevante e oportuno, deve ser interessante para a autoridade que tomará alguma decisão.

A lente *Policy Argumentation* considera que os seres humanos são culturalmente moldados, baseados em comunicação, socialmente motivados e emocionalmente fundamentados (FISCHER; GOTTWEIS, 2012). A lente destaca que não há argumentos neutros, todos estão ancorados em bases de valores (o que se compreende por Estado, seu papel, sua relação com a sociedade, onde está o poder legitimado, o que deve ser promovido, o que deve ser evitado, etc.).

Essa premissa vale tanto para o assessorado (o decisor político), quanto para o assessor (o profissional de Inteligência) que fornece conhecimento, sinaliza probabilidades ou emite conclusões baseadas em suas interpretações. Esta preocupação com o viés ideológico do analista de Inteligência já vem sendo discutida no âmbito da doutrina de produção de conhecimento.

> Ao percorrer as fases da MPC (planejamento, reunião, análise e síntese, interpretação, formalização e difusão), há uma série de tarefas das quais o analista deve se ocupar (...). Mais delicada é a fase de análise e síntese. Para esse momento, embora haja orientações e discussões pormenorizadas sobre como determinar valor de uma fração e como integrá-la, há também ampla margem para avaliações subjetivas. O julgamento da veracidade do conteúdo (quanto a coerência interna, compatibilidade com a situação e semelhança com outros dados) e da idoneidade da fonte (quanto a autenticidade, confiança e competência) dos dados que chegam ao analista não escapam de vereditos pessoais e, em alguma medida, de assunção de riscos. Ainda mais difícil é, após a síntese, expressar a interpretação do que foi agregado no texto e a atribuição de um significado final, seja conclusão baseada em raciocínios elaborados ou tendência (CRUZ, 2020, p. 29).

Assim, a lente interpretativa *Policy Argumentation* representa avanços práticos e teóricos no campo de análise, por permitir examinar as estratégias comunicativas e retóricas que os planejadores e analistas de políticas públicas e de Inteligência usam para direcionar a atenção para os problemas e opções que estão sendo avaliadas.

Além disso, sua utilização permite revelar tanto a micropolítica da definição da

agenda desses planejadores e analistas, quanto a macropolítica da participação de analistas em discursos mais amplos, sejam eles articulados em coalizões discursivas organizadas ou mais difusas (FISCHER; FORESTER; 1993). Subtrai-se desse entendimento que os gestores públicos, usuários finais dos produtos de Inteligência, são partícipes de coalizões de interesses da mesma forma que os profissionais de Inteligência, os assessores, também o são.

Ainda sob a ótica da lente em questão, torna-se perceptível que o profissional da Inteligência, ao difundir conhecimento, está, na realidade, produzindo argumentos (válidos) para o processo de tomada de decisão. A efetividade de seu assessoramento depende da compreensão de que os decisores, planejadores e analistas de políticas públicas tomam decisões baseadas em argumentos que expressam ou resistem a relações mais amplas de poder e crença. Assim, entender o dia a dia do gestor público e a forma como este se comunica torna-se fundamental para o bom assessoramento promovido por este profissional.

Para além do fator subjetividade, que afeta especialmente a forma como o produto de Inteligência será produzido, apresentado e difundido a seu cliente, este assessoramento também possui outro desafio: o de analisar as incertezas, ambiguidades e imprevisibilidades dos problemas contemporâneos, por exemplo, o renascimento de nacionalismos, conflitos étnicos, ondas desestabilizadoras de migração, novas formas de terrorismo e ameaças aceleradas de mudanças climáticas.

O mundo atual está submetido a crises cada vez mais agudas e frequentes em que as perdas e prejuízos são crescentes. A Inteligência nesse contexto de complexidade assume papel imprescindível na construção e no estabelecimento de modos de organizar ações para prevenir crises e responder a elas. O que se espera da Inteligência é que a Atividade forneça conhecimentos para antecipar, de forma confiável, problemas e situações estratégicas, e gere conhecimento que não estava disponível para o gestor tomador de decisão (CRUZ, 2020).

Assim, a compreensão e a análise dos chamados *wicked problems*[5] são favorecidas quando analisadas pela lente Policy Argumentation, por demonstrar compreender melhor a complexidade desses tipos de problemas do que os modelos mais simplificados de explicação.

> (...) a análise de políticas públicas não pode mais se limitar aos modelos acadêmicos simplificados de explicação. Esses métodos falham em abordar a natureza não-linear dos confusos problemas de políticas públicas de hoje. Eles não conseguem capturar o caráter tipicamente heterogêneo, interconectado,

5 Compreende-se por *wicked problem* as questões que apresentam altos níveis de complexidade, incerteza e divergência, com as quais vários *stakeholders* – com diferentes papéis institucionais, níveis de conhecimento, expectativas, interesses pessoais, valores e ideologias – estão engajados, resultando em conflitos e gerando soluções apenas "boas o suficiente", não abrangentes e duradouras (HEAD, 2022).

> muitas vezes contraditório e cada vez mais globalizado dessas questões. Muitos desses problemas são, como tal, adequadamente descritos como *wicked problems*. Nestas situações, não só o problema necessita de solução, a própria natureza e a conceitualização do problema não são bem compreendidos. Soluções eficazes para esses problemas exigem deliberação contínua e informada que envolva perspectivas conflitantes por parte de funcionários do governo e cidadãos (FISCHER; GOTTWEIS; 2012, p. 6, tradução nossa).

Com a virada argumentativa, os significados contidos nos textos, narrativas, argumentos e quadros de valor ativos assumem uma função singular na produção de conhecimento e contribuem para a reflexão do papel crítico do discurso e da argumentação, tanto para as práticas de análise de políticas públicas *(policy)*, quanto para uma compreensão da atual dinâmica de formulação de políticas *(politics)*. Os estudos da Atividade de Inteligência devem se aproximar do mundo acadêmico e se apropriar dessas contribuições para, assim, ampliar suas possibilidades de refletir sua prática de análise e a dinâmica de seu assessoramento.

> Ao ver o fluxo de políticas públicas como um fluxo de produção de conhecimento, o sujeito em ação pode problematizar o seu próprio processo de produção de conhecimento como um processo *in progress* de produção de conhecimento aplicado. Contudo, esta produção de conhecimento se dá em um processo coletivo. Ninguém produz conhecimento sozinho, como tantas vezes problematizou John Dewey, a partir do conceito de público. A produção de conhecimento é um processo de investigação situada e, de certa forma, aplicada (BOULLOSA, 2019, p. 99).

A qualidade do assessoramento da Inteligência brasileira em políticas públicas depende tanto da compreensão por parte dos analistas de Inteligência das principais lentes explicativas que disputam o campo de estudos de políticas públicas, quanto da atualização da metodologia de produção de conhecimento para permitir o acompanhamento sistemático de determinadas políticas públicas (as entendidas como estratégicas) a partir de instrumentos capazes de auxiliar na obtenção de dados diversos, na compreensão de contextos complexos, na interpretação de discursos e na identificação de quadros valorativos dos partícipes na formulação e na implementação de políticas públicas.

O presente artigo, com o intuito de buscar uma resposta analítica para as lacunas informacionais contemporâneas, propõe o estudo do modelo de Interpretação Adaptativa de Lahneman (2010) como alternativa metodológica para a Inteligência brasileira lidar com o excesso de dados e assuntos cada vez mais difusos e complexos.

Modelo de interpretação adaptativa

No campo da Teoria da Inteligência, Lahneman (2010) propôs a adoção do modelo denominado Interpretação Adaptativa, cuja produção do conhecimento de Inteligência teria por objetivo montar *puzzles* muito complexos,

nos quais praticamente todas as peças (informações) estão disponíveis, porém requerem alta capacidade de processamento de grande volume de informações obtidas pelo compartilhamento de informações não apenas entre serviços de Inteligência.

O paradigma tradicional da Inteligência classifica as informações a serem obtidas como sigilosas ou abertas. O novo paradigma proposto por Lahneman (2010) adiciona o conceito de informações confiáveis *(trusted information):* informações processadas por atores fora do sistema de Inteligência de um país, que fazem parte de uma rede de confiança, incluindo entes privados.

> É necessário um novo conceito de informação, que incluirá uma nova forma de informação conhecida como "informação confiável", além de informação secreta e aberta. As informações confiáveis circulam dentro de "redes confiáveis", nas quais espera-se que todos os membros insiram apenas informações validadas e usem as informações da rede com responsabilidade. Dentro dessas restrições, a rede pode ser integrada por qualquer organização que possa fornecer as informações necessárias. Isso inclui agências governamentais, empresas privadas, organizações intergovernamentais (OIGs), organizações não governamentais (ONGs) e até mesmo indivíduos em várias comunidades informais de interesse. Como seu objetivo é abordar questões e ameaças transnacionais, as redes confiáveis devem ter escopo global (LAHNEMAN, 2015, p. 216-217, tradução nossa).

O modelo de Interpretação Adaptativa permite que o profissional de Inteligência lide melhor com situações mais dinâmicas, comparado com o paradigma do modelo tradicional de pensar a Atividade. A quantidade de informações e a atual velocidade de propagação fazem com que frações significativas de informações mudem de valor em curtos períodos de tempo. O mesmo ocorre para as relações entre as informações, dados que não estavam correlacionados em um primeiro momento podem se relacionar a posteriori e vice-versa. Além disso, a maioria das análises que exigem interpretações adaptativas não terá grandes peças do *puzzle*, apenas um grande número de pequenas peças. Isso significa que analistas precisam encontrar novas maneiras de atribuir valor a cada pequena informação coletada e reavaliar continuamente esse valor (LAHNEMAN, 2010).

Assim, do mesmo modo que, para o campo de estudos de políticas públicas, a análise dos *wicked problems* é considerada mais adequada pelas lentes explicativas pós-positivistas, como a *Policy Argumentation*, a interpretação dos mesmos problemas pelos estudos para a Inteligência é favorecida se for realizada a partir da ótica do modelo de Interpretação Adaptativa, que possibilita tratar tais problemas sob a lacuna da complexidade.

Lahneman (2010) também sugere uma definição mais restritiva de Inteligência, voltada apenas para as atividades de coleta secreta e de ação secreta *(covert action)*. As informações confiáveis sairiam do

escopo exclusivo da Inteligência e seriam classificadas como informações estratégicas a serem coletadas e processadas por uma estrutura estabelecida especificamente para este fim.

> O *Office of Strategic Information* (OSI) integraria e analisaria as informações da rede para identificar e analisar anomalias que possam sinalizar o início de uma epidemia, um desastre iminente ou um ataque terrorista planejado. Encaminharia essas informações para as agências de inteligência e de segurança pública, que poderiam agregar valor por meio de suas atividades de coleta secreta (LAHNEMAN, 2015, p. 223, tradução nossa).

A adoção do modelo proposto pelo serviço de Inteligência brasileiro requereria algumas medidas, p. ex.: a ampliação do atual escopo do Sisbin (para permitir a participação de instituições e entes privados); o fortalecimento do papel da Abin como órgão central (responsável por integrar dados e conhecimentos advindos do sistema); a implantação de modelos de compartilhamento de informações de interesse; e a atualização de instrumentos normativos para possibilitar a promoção das novas parcerias. Destaca-se que todo trabalho de assessoramento da Inteligência, em especial o relacionado a políticas públicas estratégicas, beneficiar-se-ia com o aumento do fluxo de informações provenientes da incorporação de novos entes ao sistema de Inteligência.

Considerações finais

Uma das missões da Atividade de Inteligência, conforme determinado por lei, é o assessoramento estratégico brasileiro de alto nível. A Inteligência de Estado deve antecipar fatos e situações de interesse nacional, e apresentar, de forma clara, ágil e dinâmica, as informações necessárias para a tomada de decisão do cliente-usuário do relatório de Inteligência.

Em seu papel de assessoramento a decisores governamentais, a Inteligência brasileira produz e difunde conhecimentos capazes de explicar desdobramentos e reduzir as incertezas inerentes à elaboração e à implementação de políticas públicas. Como exemplos, cita-se os documentos produzidos pela Abin e pelo Sisbin e difundidos para a Casa Civil e os distintos decisores ministeriais.

O campo de estudos em políticas públicas é bastante vasto e plural, com diferentes tradições, escolas, matrizes, abordagens ou lentes que conformam os muitos caminhos que os envolvidos nos processos de políticas públicas podem tomar para produzir percursos de análise. A compreensão dos principais componentes de cada lente, o que ela permite ver melhor, para quais caminhos de interpretação ela leva e, especialmente, o que ela impede de observar ou fazer, são essenciais para os analistas que trabalham com políticas públicas ou as estudam.

No presente artigo, verificou-se que o ciclo de Inteligência, como ensinado na doutrina da Atividade, possui raiz positivista, similar ao modelo trazido pela lente analítica *Policy Cycle*, que favorece a compreensão da função informacional da Atividade de Inteligência; e que a lente *Policy Argumentation*, ao priorizar o papel do argumento e de sua recepção na tomada de decisão, amplia as discussões sobre os instrumentos utilizados pelo profissional de Inteligência para atingir um assessoramento mais efetivo e oportuno.

Ao analisar o papel da Inteligência no assessoramento a gestores públicos ministeriais, concluiu-se que as duas abordagens de políticas públicas estudadas trazem contribuições para pensar e discutir o papel do assessoramento de Inteligência na formulação e na implementação dessas políticas. A primeira, *Policy Cycle*, apesar das limitações analíticas, possibilita o uso de explicações simplificadas e *briefings* rápidos ao decisor político. Já a segunda, *Policy Argumentation*, mais apta a analises de estruturas complexas, auxilia na apresentação de argumentos práticos capazes de persuadir o assessorado a considerar o conhecimento produzido pela Inteligência na tomada de decisão.

O principal desafio da Inteligência de Estado em seu papel de assessoria a gestores ministeriais é compreender as redes de política e os modos negociados de coordenação entre os atores públicos e privados, nacionais e internacionais, na formulação de políticas contemporâneas e na construção de governança. O modelo de Interpretação Adaptativa proposto por Lahneman apresenta-se como uma possível resposta analítica por parte da Inteligência para buscar lacunas informacionais contemporâneas e, assim, melhorar o assessoramento aos decisores governamentais responsáveis por formular e implementar políticas públicas complexas.

Assim, espera-se que a Atividade de Inteligência brasileira acompanhe os avanços trazidos tanto pelos estudos de políticas públicas – que seguem cada vez menos o modelo tradicional de estágios, considerado ultrapassado para a complexidade dos problemas atuais –, quanto pelos estudos recentes da Teoria de Inteligência, que abordam tais complexidades como lacunas informacionais a serem buscadas de forma cooperativa e ampliada.

Referências

BRASIL. Gabinete de Segurança Institucional. Agência Brasileira de Inteligência. *Portaria 926/2023*, de 6 de setembro de 2023, que estabelece o rol de órgão e de entidades que integram o Sistema Brasileiro de Inteligência – Sisbin. *Diário Oficial da União*, seção 1, Brasília, DF, 13 set. 2023.

BRASIL. Decreto nº 11.693, de 6 de setembro de 2023. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência. *Diário Oficial da União:* seção 1 edição extra, Brasília, DF, 6 set. 2023.

BRASIL. 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. *Diário Oficial da União*, seção 1, Brasília, DF, 02 fev. 2023.

BRASIL. Gabinete de Segurança Institucional. *Portaria nº 40/GSI/PR*, de 3 de maio de 2018. Aprova o Plano Nacional de Inteligência (PLANINT). Brasília, 2018.

BRASIL. Decreto s/n, de 15 de dezembro de 2017. Aprova a Estratégia Nacional de Inteligência. *Diário Oficial da União*, seção 1, Brasília, DF, 18 dez. 2017.

BRASIL. Decreto nº 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência. *Diário Oficial da União*: seção 1, Brasília, DF, 30 jun. 2016.

BRASIL. Gabinete de Segurança Institucional. Agência Brasileira de Inteligência. *Doutrina Nacional da Atividade de Inteligência*: fundamentos doutrinários. Brasília: Abin, 2016.

BRASIL. Lei nº 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência, e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, 08 dez. 1999.

BOULLOSA, Rosana. Mirando ao Revés as políticas públicas: os desenvolvimentos de uma abordagem crítica e reflexiva para o estudo das políticas públicas. *Publicações da Escola da AGU*, p. 89-105, 2019.

CRUZ, Anna. Aprimoramento da Capacidade Analítica e Avanço na Atividade de Inteligência. *Revista Brasileira de Inteligência*, Brasília, n. 15, p. 25-40, dezembro 2020.

DURNOVA, Anna; FISCHER, Frank; ZITTOUN, Philippe. Discursive approaches to public policy: politics, argumentation, and deliberation. *Contemporary Approaches to Public Policy*. International Series on Public Policy. London: Palgrave Macmillan, p. 35-56, 2016.

FISCHER, F., FORESTER, J. *The Argumentative Turn in Policy Analysis and Planning*. London: Duke University Press, 1993.

FISCHER, F.; GOTTWEIS, H. *The Argumentative Turn Revisited:* public policy as communicative practice. Durham & London: Duke University Press, 2012.

FISCHER, Frank. Para além do empirismo: policy inquiry na perspectiva pós-positivista. *Revista NAU Social,* v. 7, n. 12, p.163-180, maio/nov. 2016.

GIL, A. C. *Métodos e Técnicas de Pesquisa Social.* 6. ed. São Paulo: Atlas, 2008.

HABERMAS, Jurgen. *The theory of communicative action:* the critique of functionalist reason. Cambridge: Policy Press, 1986. v. 2.

HEAD, Brian. *Wicked problems in public policy:* understanding and responding to complex challenges. Queensland, Australia: Palgrave Macmillan/The University of Queensland, 2022.

JANN, Werner; WEGRICH, Kai. Theories of the Policy Cicle. *In:* FISCHER, Frank; MILLER, Gerald J.; SIDNEY, Mara S (ed). *Handbook of public policy analysis:* theory, politics, and methods. [S. l.]: CRC Press, 2007.

LAHNEMAN, William. The need for a new Intelligence paradigm. *International Journal of Intelligence and Counterintelligence*, vol. 23, n. 1, p. 201-225, 2010.

LASSWELL, Harold. The Policy Orientation. *In:* LERNER, Daniel; LASSWELL, H. D. (ed). *The Policy Sciences:* recent developments in scope and method. Stanford, CA: Stanford University Press. p. 3-15.

Artigo

7

É DEVER DE TODO PROFISSIONAL DE INTELIGÊNCIA ALERTAR?
Características e potencialidades de aplicação da Inteligência de Alerta

DOI: https://doi.org/10.58960/rbi.2023.18.231

Iêda Maria Toledo Silveira *

Resumo

Originalmente, a alteridade da Inteligência de Alerta (IA) ou da Inteligência Indiciária é o inimigo, o país inimigo, o exército inimigo. Como a proposta deste estudo é apoiar a tese de utilização da IA para além do universo militar, sugere-se que o inimigo seja substituído por adversário, elemento hostil, ameaça, fator adverso ou antagônico. Para a aplicação da Inteligência de Alerta, em uma dada situação, atores antagônicos, suas intenções, motivações e meios devem ser mapeados e permanentemente monitorados para, a partir de determinados indícios, integrarem a emissão de um alerta a fim de antecipar-se uma ameaça ou uma oportunidade. A IA é distinta da Inteligência Corrente, da Inteligência de Base ou da Inteligência Prospectiva e tem como principal aspecto doutrinário uma metodologia específica, traduzida neste trabalho como metodologia indiciária (*"Indications and Warning"* – I&W). Entendida em suas características distintivas e aplicada adequadamente, a IA tem potencial de ampliar e aprimorar a qualidade do assessoramento realizado pela Inteligência no Brasil.

Palavras-chave: inteligência de alerta; inteligência indiciária; metodologia indiciária.

IS IT THE DUTY OF EVERY INTELLIGENCE PROFESSIONAL TO WARN?
Characteristics and possible applications of warning intelligence

Abstract

The otherness in Warning Intelligence (WI) or in Indications Intelligence (II) is originally the enemy, the enemy country, the enemy Army. As the purpose of this study is to support the thesis that WI should not be confined to the military universe, the concept of enemy will be replaced with adversary, hostile actor, threat, antagonistic or adversarial factor. In a given situation, the WI must identify and monitor antagonistic actors, their intentions, motivations and means in order to determine indications that will be part of a warning, anticipating a threat or an opportunity. The II is different from Current Intelligence, from Basic Intelligence or from Estimative Intelligence; the II has a specific methodology known as "Indications and Warning" (I&W) as main doctrinal aspect. If the WI is understood in all its distinctive characteristics and properly applied, it has the potential to expand and enhance the quality of Intelligence in Brazil.

Keywords: *warning intelligence; indications intelligence; indications and warning (I&W) methodology.*

* Bacharel e Licenciada em Geografia pela Universidade de São Paulo (USP). Bacharel em História pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Mestre em História Social pela USP. Oficial de Inteligência da Agência Brasileira de Inteligência (Abin).

¿ES DEBER DE TODO PROFESIONAL DE INTELIGENCIA ALERTAR? Características y potenciales de aplicación de la Inteligencia de Alerta

Resumen

Originalmente, la alteridad de la Inteligencia de Alerta (IA) o de la Inteligencia Indiciaria (II) es el enemigo, el país enemigo, el ejército enemigo. Como la propuesta aquí es defender la tesis de utilización de la IA no solamente para el universo militar, se sugiere que el enemigo sea sustituido por adversario, elemento hostil, factor adverso o antagónico. Para la aplicación de la Inteligencia de Alerta en una dada situación, actores antagónicos, sus intenciones, motivaciones y medios deben ser mapeados y permanentemente monitoreados para, a partir de determinados indicios, hacer parte de la emisión de una alerta con el objetivo de anticipar amenazas u oportunidades. La IA es distinta de la Inteligencia Actual, de la Inteligencia Básica o de la Inteligencia Prospectiva, y la primera tiene como principal aspecto doctrinario una metodología específica que ha sido traducida aquí como metodología indiciaria ("Indications and Warning" – I&W). Entendida en sus características distintivas y aplicada de manera adecuada, la IA tiene el potencial de ampliar y mejorar la calidad del asesoramiento de Inteligencia en Brasil.

Palabras clave: *inteligencia de alerta; inteligencia indiciaria; metodología indiciaria.*

Introdução

"You did not tell me this was going to happen. We were not led to expect this and were surprised". Cynthia Grabo, sobre a crítica mais comum dos tomadores de decisão em relação à Inteligência (2015, p. 42).

O objetivo desse estudo é interpretar a vertente analítica descrita pela Comunidade de Inteligência dos Estados Unidos da América (EUA) como *Warning Intelligence* ou *Indications Intelligence*, traduzidas como Inteligência de Alerta (IA) ou Inteligência Indiciária, e analisar como a IA pode contribuir para as atribuições de assessoramento do Sistema Brasileiro de Inteligência (Sisbin). Avaliar a IA obriga a tratar de seus tangenciamentos com a Inteligência Corrente (IC) e a Inteligência Prospectiva (IP[1]), ou mesmo com a Inteligência de Base (IB – *"Basic Intelligence"*). Desse modo, complementarmente, a ótica comparativa fará parte deste trabalho, sobretudo pela necessidade de diferenciação entre IA e IC. A hipótese inicial é que a distinção entre essas tipologias da Inteligência e a própria caracterização da IA podem se dar à luz de uma perspectiva temporal: do passado aos futuros possíveis. Como será demonstrado, a hipótese pôde ser comprovada.

Além desse recorte cronológico para separar os ramos da Inteligência, foram abordados mais dois enfoques temporais: os fatos históricos que marcam o nascimento e a trajetória da Inteligência de Alerta; e a linha do tempo utilizada pelo profissional de Inteligência para a coleta, a análise da trajetória e o assessoramento.

Toda a fundamentação da IA está nas clássicas balizas historiográficas das obras de Cynthia Grabo, que convergiram para o Handbook of Warning Intelligence, periodicamente atualizadas desde seu ofício como analista nos anos 1940 a 1970, até 2015, quando seus manuscritos foram totalmente desclassificados pelo governo estadunidense. Como contraponto e, ao mesmo tempo, continuidade da interpretação da IA, está o livro de John A. Gentry e Joseph S. Gordon, Strategic Warning Intelligence (2019), que amplia o espectro metodológico e temático da Inteligência de Alerta, com ênfase no nível estratégico e não mais centrado em assuntos militares. Gentry e Gordon, acadêmicos e, respectivamente, ex-analistas da CIA e da Agência de Inteligência de Defesa (Defense Intelligence Agency -DIA), utilizam ampla bibliografia sobre Inteligência e IA, esta última bastante atualizada desde o livro de Grabo, datado do início dos anos 1970.

Adicionalmente, alguns artigos serviram como referência dialógica para a explicação do método indiciário, sobretudo em referência aos aprimoramentos necessários

1 Ao compararem a Inteligência de Alerta com outras tipologias da Inteligência, como a IC *("Current Intelligence")* ou a IB *("Basic Intelligence")*, os principais autores analisados também diferenciam a IA da Estimativa *("Estimative Intelligence")*. No entanto, como, para a Doutrina de Inteligência no Brasil, estimativa é um tipo documental, e não um ramo da Inteligência, optou-se por traduzir *"Estimative Intelligence"* como Inteligência Prospectiva.

para o assessoramento de natureza antecipatória.

Além da introdução e do encerramento, o artigo está dividido em quatro seções: uma primeira aborda a IA sob as perspectivas histórica e historiográfica; na segunda, explica-se o método indiciário e as características e atributos que fazem um bom analista de IA e, na sequência, analisa-se a Inteligência Indiciária em seu papel de assessoramento. Por fim, há um mapa com os principais conceitos e características que integram o Ciclo de Produção e Difusão da Inteligência de Alerta, conforme proposto neste estudo.

A Inteligência de Alerta em perspectiva histórica e historiográfica

A concepção de Inteligência de Alerta ou Indiciária, concernente àquilo que o adversário está prestes a realizar, foi sendo construída por imposição dos acontecimentos e das necessidades dos usuários. Nascida formalmente após a 2ª. Guerra Mundial, a IA torna-se estratégica durante a Guerra Fria, como instrumento de antecipação e monitoramento dos movimentos dos países integrantes do bloco soviético e permanece atual no contexto das guerras assimétricas.

Na linha do tempo que delimita a trajetória de países e indivíduos, o ataque do Japão a Pearl Harbor, em 1941, significou um múltiplo ponto de inflexão: determinou não apenas o ingresso dos EUA na 2ª. Guerra Mundial, mas também a gestação do que ficaria conhecida, na Comunidade de Inteligência dos Estados Unidos, como IA ou Inteligência Indiciária. Era também o começo das atividades de Cynthia Grabo como profissional de Inteligência, que duraram de 1942 a 1980. Ela fora recrutada pela Inteligência do Exército depois do ataque japonês; tornou-se especialista em IA a partir de 1949 e, entre 1950 e 1975, atuou como pesquisadora sênior no *National Indications Center*, uma unidade entre agências, e, em sua organização sucessora, o *Strategic Warning Staff*, que não existe mais. A vida da autora estadunidense é indissociada da história e da metodologia da Inteligência de Alerta.

A experiência e o conhecimento adquiridos por Grabo foram reunidos na publicação da DIA *Handbook of Warning Intelligence,* três volumes escritos de 1972 a 1974 (433 páginas), mas que permaneceram por décadas indisponíveis ao público. Apenas em 2002, Grabo viu parte de sua obra ser desclassificada pelo *Joint Military Intelligence College's Center for Strategic Intelligence Research*, sob o nome de *Anticipating Surprise: Analysis for Strategic Warning* (com apenas 175 páginas). Até então, a obra, escrita para ensinar novos analistas a como ler, escrever e analisar IA, era classificada como secreta e permanecera como propriedade do governo estadunidense.

Essa decisão pela desclassificação parcial, em 2002, não foi coincidência. Tanto o ataque a Pearl Harbor, em 1941, quanto às Torres Gêmeas em Nova Iorque e ao Pentágono, 60 anos depois, são considerados problemas de alerta *("warning problems")*: representaram falhas de antecipação em todas as dimensões da ameaça inimiga, ainda que tenham sido de naturezas distintas. No primeiro caso, o clássico exemplo de antagonismo interestatal, ainda que sem declaração formal de guerra; no segundo, o conflito entre atores estatais e atores não estatais: dois ataques-surpresa.

Apesar do reconhecimento do valor dessa perspectiva metodológica para o assessoramento de Inteligência, dos vários artigos sobre IA escritos a partir dos anos 2000, e da persistência da autora em ver sua obra publicada na íntegra, apenas em 2015, surgiria a versão completa e desclassificada do *Handbook of Warning Intelligence*, utilizada aqui como substrato para a caracterização do tema. Conforme a referência bibliográfica, a obra foi publicada com Jan Goldman, professor de Inteligência e Segurança Nacional nos EUA, pois Grabo falecera em 2014, aos 98 anos.

Aspectos axiológicos da Inteligência de Alerta

Após os atentados de 11 de setembro de 2001, o mundo parecia ter alterado a natureza do problema de alerta: primeiro, com o colapso do comunismo na URSS e nos países do leste europeu; depois, com a emergência da ameaça terrorista em solo estadunidense. A despeito disso, os problemas analíticos afetos à IA, bem como a natureza de suas falhas, permaneciam os mesmos: percepção equivocada das ameaças emergentes; coleta inadequada de informações sobre essas mesmas ameaças; colapso da comunicação entre agentes de campo, analistas e agências de Inteligência; desconsideração de pontos de vista divergentes (dissenso); vulnerabilidade ao engano e à dissimulação (*"denial and deception"* – D&D – GRABO, 2002).

Apesar da permanência desses mesmos desafios, a definição da Inteligência de Alerta não permaneceria a mesma ao longo da história e viria a ser ampliada para além da antecipação de uma ameaça externa iminente pelas mãos do analista sênior da CIA Jack Davis, após os ataques de 11 de setembro. Primeiro, o autor define a Inteligência de Alerta, principalmente, em linha com dois aspectos consoantes à tradição de Grabo: a) a IA só se efetiva na comunicação com o cliente; sem a expressa ciência do decisor, ou a IA não existe ou fracassa; b) o objetivo do alerta é "prevenir a surpresa estratégica" (DAVIS, 2002 A, p. 3).

Em seguida, em um aprofundamento do conceito, Davis (2002 A) destaca o elemento inédito que seria, décadas

depois, reconhecido como mérito seu em outras interpretações sobre a IA. Para o autor estadunidense, mais do que avisar o cliente sobre algo que ocorrerá, é preciso alertá-lo para que tome todas as medidas cabíveis e possíveis caso a ameaça de fato se concretize, ou seja, a surpresa pode ser inevitável (DAVIS, 2002 A).

Essa ênfase na prontidão (*"readiness", "preparedness"*) para afastar ou minimizar prováveis danos se tornaria central no conceito lapidado pelo mesmo autor em artigos subsequentes. Davis (2003) conclui que análises críticas sobre a missão da IA devem reconhecer a prioridade em se evitar ou limitar o dano previsto, e não, de forma talvez pouco realista, buscar evitar a surpresa, como estava em sua primeira definição. Posteriormente, repete que a história comprova a tese da dificuldade em se evitar surpresas, sobretudo as táticas (DAVIS, 2007).

Na década seguinte, outras interpretações mantiveram essa conceituação do autor sobre a Inteligência de Alerta. Kimmelman (2017) inspirou-se na referência conceitual e nos objetivos da IA definidos por Davis para adaptar a metodologia aos desafios da segurança doméstica. Já Gentry e Gordon (2019), na obra que é o outro substrato basilar desse artigo, citaram Davis ao enfatizar a natureza do assessoramento de alerta, ou seja, assistir os decisores na adoção "de medidas defensivas e preemptivas contra ameaças futuras, e de ações de defesa contra ameaças iminentes" (GENTRY & GORDON, 2019, p. 11).

Observa-se, assim, como a antecipação da ameaça, a comunicação com o usuário e a prontidão de resposta complementam o princípio da oportunidade, tal como entendido pela Doutrina Nacional de Inteligência (BRASIL, 2016).

Alertas estratégicos e alertas táticos

A Inteligência de Alerta estratégico é diferenciada da Inteligência de Alerta tático em termos de espectro temporal, objeto e forma de assessoramento. Para alguns autores, apenas o alerta estratégico está no campo da Inteligência de Estado.

Em Grabo (2015), não aparece o termo "estratégico" no título, talvez porque, para ela, o alerta tático não seria Inteligência de fato. Diferenciados em termos do alcance temporal, a autora afirma que o alerta estratégico é relativamente de longo prazo, emitido com antecedência de semanas ou meses: "Na prática, não é o reconhecimento da iminência da ação, mas o reconhecimento da probabilidade de ocorrência da ação" (GRABO, 2015, p. 11-12). Ademais, a função própria da IA seria estratégica, no sentido já descrito: ou o alerta é emitido com antecedência suficiente para o decisor agir – independentemente do adjetivo que o acompanhe – ou terá falhado.

Em Gentry & Gordon (2019), o qualificador "estratégico" está no título, e a diferenciação clarifica-se quando analisam os atentados de 11 de setembro. Em sua avaliação, os ataques surpresa ocorreram por uma falha de Inteligência de Alerta tático, pois, em termos estratégicos, há muito o governo estadunidense estava avisado de que seus interesses eram alvo da al-Qaeda. Assim como Grabo, distinguem o alerta estratégico pela natureza do assessoramento: apoia políticos sêniores e chefes militares em nível decisório nacional, e é distinto, portanto, do nível operacional ou tático. Por isso, quando mencionam alertas, afirmam sempre referir-se aos estratégicos, pois os táticos dizem respeito à notificação de uma ameaça militar iminente.

Os dois autores, mesmo em reconhecimento à crescente dedicação dos serviços de Inteligência ao contraterrorismo (CT) depois do 11 de setembro, mantêm a instância tática fora do âmbito da Inteligência. Admitem que muitas agências criaram o papel do *"targeting analyst"*, em apoio às operações de CT, mas "essas funções se sobrepõem e às vezes causam fricção dentro das organizações analíticas" (GENTRY & GORDON, 2019, p. 12).

Por sua vez, Davis (2003) diferencia os níveis tático e estratégico, mas os vê como complementares e típicos da Inteligência. Por um lado, coloca CT e crime organizado no nível dos alertas táticos, ao lado de ataques militares, ameaças relativas a armas de destruição em massa e crises políticas externas. Segundo o autor, a IA tática envolve diagnósticos sobre incidentes específicos, perpetradores, alvos, modalidades e *timing*, pois responde previamente às questões "quando, onde e como" um potencial adversário atacará. O autor não questiona, portanto, sua natureza de Inteligência e destaca a interligação entre ambos: "um bom alerta estratégico tem o potencial de aprimorar tanto o alerta tático quanto a prontidão". E vai além: "um alerta estratégico robusto serve como suplemento analítico indispensável ao alerta tático" (DAVIS, 2003, p. 3-4). Ele insistiria nessa mesma correlação anos mais tarde (DAVIS, 2007).

Além do fator cronológico (curto e longo prazos) e do tipo de assessoramento, outro binômio que caracteriza alertas táticos e estratégicos refere-se a seus objetos. Alertas táticos referem-se a aspectos tangíveis, a quebra-cabeças, como os que explicam o trabalho dos profissionais de CT. Já "o alerta estratégico é sobre adivinhar o significado de importantes mistérios da arena internacional (...), que são questões analíticas para as quais ainda não há respostas objetivas" (GENTRY & GORDON, 2019, p. 21-22).

O ciclo de Inteligência de Alerta

Em maior ou menor grau, os autores

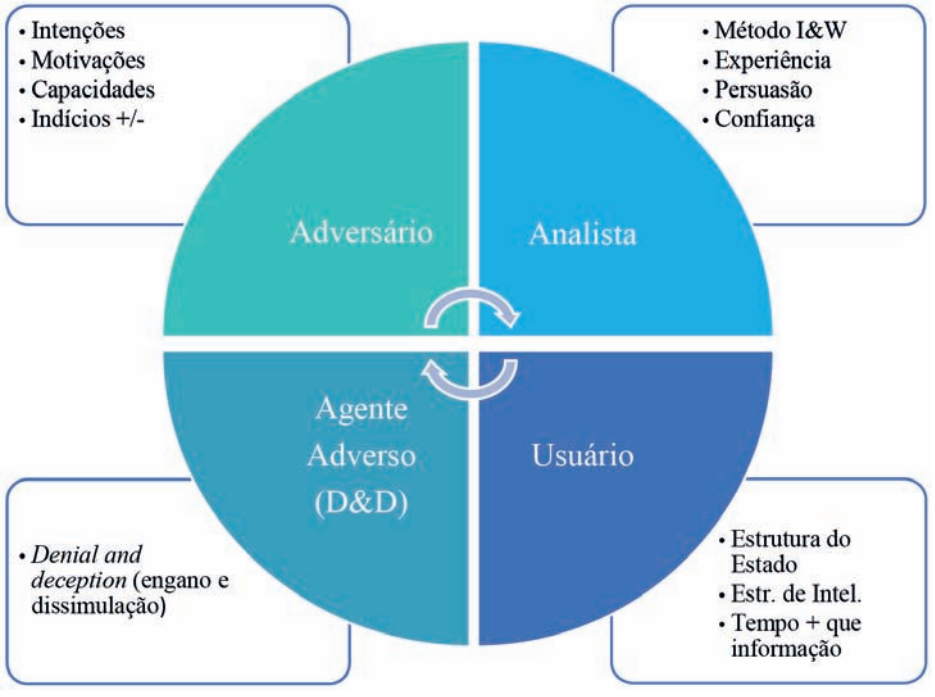
que se dedicaram à IA reconhecem que uma das peculiaridades complexas dessa corrente analítica reside na articulação entre todos os atores envolvidos no que será aqui definido como Ciclo de Produção e Difusão da Inteligência de Alerta.

Davis (2003) defende uma ampla atuação dos usuários no processo do alerta: alocação de recursos; definição de temas e parâmetros analíticos; indicação de técnicas indiciárias; e seleção e monitoramento de indicadores de mudanças na probabilidade, no impacto, no *timing* e na descrição das ameaças. Para "a desconexão entre produtores e consumidores de alertas estratégicos ser superada", esses deveriam ser "responsabilidade" de todo o governo, e não apenas da Inteligência (DAVIS, 2003, p. 13-15).

Por sua vez, Wirtz (2013), autor de inúmeros livros sobre Inteligência e controle de armamentos, também salienta a mesma importância da integração entre os atores quando menciona um dos desafios da metodologia indiciária: ser implementada ao longo de todo o ciclo de Inteligência – coleta, análise e resposta – para ser efetiva.

Nesse sentido, propõe-se aqui a seguinte configuração para o Ciclo de Produção e Difusão da Inteligência de Indiciária, com foco nos atores: analista e usuário, de um lado, e adversário e agente adverso, de outro (Figura 1):

Figura 1 – Ciclo de Inteligência de alerta (foco nos atores)



Fonte: elaborado pela autora.

A tarefa do analista de IA, com base no método indiciário, é desvendar as intenções, motivações e capacidades do adversário. Os indícios levantados durante o trabalho analítico podem ser positivos ou negativos, no sentido de confirmar ou não as inferências realizadas. Segundo Grabo (2015), ao buscar-se desvendar o inimigo, deve-se fazer o cruzamento entre indícios positivos e negativos, ou seja, analisar o que ele fez e o que nunca fez. Em linha com a autora, algumas perguntas podem ser feitas para se chegar à mente (intenções e motivações) do adversário: ele está comprometido com os objetivos declarados?; sua meta pode ser atingida ou o problema solucionado pela via negociadora?; todas as outras opções foram eliminadas, antes de uma suposta ameaça militar ou retaliação?; o fator de risco é baixo ou pelo menos tolerável?

Por sua vez, o produto da Inteligência Indiciária tem de ser persuasivo o suficiente para chamar a atenção do usuário, ganhar sua confiança e mobilizá-lo para a ação (Figura 1). O desafio é justamente chegar ao cliente, para quem o tempo pode ser mais importante que o próprio acesso à informação. Nesse sentido, para Wirtz (2013), os decisores não devem ser prevenidos sobre um único evento, mas assessorados em toda uma análise de risco sobre a ameaça crescente *("risk assessment")*, de modo que o aparato do Estado possa agir, ou seja, "desviar, deter ou atrapalhar" a ameaça (DAVIS, 2003, p. 12).

Esse contato direto da Inteligência Indiciária com o cliente dependerá de como essa corrente analítica está inserida nas organizações de Inteligência e na própria estrutura do Estado (Figura 1). Muitas vezes, uma das limitações do analista é "desconhecer o que outras áreas do governo estão pensando ou fazendo a respeito do problema de alerta", caso esse já tenha sido identificado (GENTRY & GORDON, 2019, p. 157).

As duas obras angulares aqui utilizadas abordam o papel que o adversário (às vezes, aliado) exerce na negação da informação, na dissimulação, na desinformação, ou nos "sinais da mentira" (D&D – Figura 1), com o intuito de criar o elemento surpresa. Grabo (2015) destaca a importância da contrainteligência e de outras estratégias de negação à informação pelos países inimigos, como o controle da mídia. Acerca da coleta de dados sobre espionagem, afirma: "sua relevância deriva do fato de que os serviços de segurança e suas ações funcionam como um espelho que reflete os objetivos e interesses do líder do país inimigo sobre importantes assuntos internacionais" (GRABO, 2015, p. 223).

Finalmente, Gentry & Gordon (2019) lamentaram que, ao menos no momento em que escreviam, IA e contrainteligência *("counter-deception")* permaneciam em estruturas organizacionais separadas nos EUA. "(...) Porque alerta, e engano e dissimulação estão intimamente

relacionados, é importante os profissionais indiciários conhecerem técnicas de D&D e métodos de contrainteligência" (GENTRY & GORDON, 2019, p. 4). Também atribuíram às redes sociais papel fundamental de desinformação nos dias atuais.

O método indiciário

Já se observou que a metodologia indiciária (*"Indications and Warning"* – I&W) foi tecida durante a Guerra Fria, para buscar-se antecipar um ataque militar surpresa por parte da URSS e dos seus aliados. Ou seja, a metodologia nasceu durante a guerra, sobretudo para períodos de guerra, baseada no antagonismo entre países aliados e inimigos. No entanto, a continuidade do uso das técnicas de I&W e a análise atual sobre o tema demonstram que esses mesmos princípios metodológicos podem ser aplicados a conflitos assimétricos ou a temáticas não-militares, por vezes com adaptações, mas não sem polêmica.

Com o fim da Guerra Fria, muitos fizeram e ainda fazem objeção à capacidade de antecipação da metodologia indiciária, em particular, em relação a dois aspectos. Por um lado, pelo fato de os desafios contemporâneos, como os impostos por atores não estatais, gerarem indícios fracos ou pouco significativos para serem submetidos às técnicas tradicionais de I&W. Células terroristas, por exemplo, emitem sinais tíbios ou muito dissimulados de antecipação da ameaça comparados, por exemplo, a unidades militares inteiras; porém, ainda assim, emitem-nos, e a comunidade de Inteligência pode identificá-los. Por outro lado, ameaças vindas de atores não estatais são "distintas, imprevisíveis, diabólicas e inovadoras" (WIRTZ, 2013, p. 555-556 e 561) em relação àquelas provenientes de autores estatais; portanto, identificar com antecedência locais, métodos e alvos de ataques seria mais difícil. Gentry & Gordon (2019) seguem essa mesma linha de incredulidade acerca da eficácia da tradicional metodologia da Inteligência de Alerta para temas de segurança doméstica *("homeland security")*, como CT.

Defende-se aqui, porém, inclusive para o caso de ameaças terroristas, que a metodologia é aplicável, porque o "quesito imaginação" não falta a analistas de Inteligência para antecipar ameaças prováveis (WIRTZ, 2013, p. 556). Kimmelman (2017) explora, adapta e atualiza sua funcionalidade para temas de segurança doméstica, o que demonstra que as técnicas de I&W podem ser mais um instrumento de natureza preventiva em CT, em complemento ao estudo de Ribeiro (2019).

Por sua vez, Grabo (2015) insiste no caráter didático de "análises *post-mortem*" (GRABO, 2015, p. 6-8, 70 e 84), para se aprender com fatos que representaram grandes fracassos de alerta (o mesmo o

faria Davis mais tarde – 2002 A). O ataque da Coreia do Norte à Coreia do Sul, e a intervenção chinesa na Coreia, em 1950, a revolta da Hungria e a crise do canal de Suez, em 1956, a crise dos mísseis de Cuba, em 1962, e a invasão da Tchecoslováquia pela URSS, em 1968, envolveram tropas estadunidenses e foram marcadas por preparações e movimentações militares, ainda que secretas, algumas ações de D&D, grande variedade de indícios políticos e, com exceção ao caso cubano, chegaram a ser conflitos militares de fato. Portanto, arquivos de alertas de longa duração – fracassados ou não –, ao contrário daqueles de IC, que logo se tornam desatualizados, melhoram com o tempo. Manter arquivos com essas crises é uma das coisas mais úteis que uma unidade de Inteligência de Alerta pode fazer (GRABO, 2015).

Assim como os estadunidenses, os britânicos analisam seus fracassos e sucessos na detecção de crises e ameaças. Ao contrário dos profissionais estadunidenses, os britânicos anteciparam as crises do canal de Suez e dos mísseis em Cuba. No entanto, também falharam ao não prever a Guerra da Coreia, a invasão da Tchecoslováquia, a Guerra do Yom Kippur (1973) e a invasão das Malvinas (1982). Por sua vez, o sistema de Inteligência japonês foi totalmente reestruturado e fortalecido pelo então primeiro-ministro Shinzo Abe, depois da falha da antecipação do lançamento de mísseis norte-coreanos sobre o Japão, em 2008 (GENTRY & GORDON, 2019).

E quando a Inteligência Indiciária antecipa uma crise, e o decisor a evita ou a debela, inclusive pela dissuasão do inimigo? Não é difícil imaginar que não há tantos registros sobre o que é denominado "paradoxo do alerta" ou "dilema do alerta". Afinal, a complexidade da IA vem também da dificuldade da caracterização ou até da identificação do que seria seu sucesso, pois sempre pode alegar-se que o inimigo não teria agido de nenhuma forma (atacado ou ameaçado), independentemente do alerta. Será que os soviéticos não invadiram a Polônia em 1980, como fizeram com a Hungria e a Tchecoslováquia, porque a CIA alertou os presidentes Jimmy Carter e Ronald Reagan, e esses, por sua vez, ameaçaram a URSS com sanções, ou Leonid Brezhnev estava blefando desde o início? A análise histórica dos desempenhos da IA não apresenta, portanto, um simples resultado dicotômico entre acertos e erros (GENTRY & GORDON, 2019).

Em contrapartida, ao citarem Mark Lowenthal, eminente autor sobre Inteligência e segurança nacional, os autores estadunidenses destacam dois sucessos inequívocos da IA, pela pronta e assertiva resposta dos usuários: os assessoramentos que levaram o Presidente George H. Bush a enviar um representante de segurança nacional para evitar a guerra entre Índia e Paquistão, em 1990; e o Presidente George W. Bush, em 2003, a negociar com o líder líbio Muammar el-Qaddafi para que esse pusesse fim a seu programa de armas de

destruição em massa (LOWENTHAL *apud* GENTRY & GORDON, 2019).

A metodologia I&W: fundamentos conceituais e diferenciais

A metodologia de *Indications and Warning* (I&W) ou, como foi traduzida aqui, metodologia indiciária ou de alerta, parte do conceito central de indício. Para Grabo (2015), essa definição é acompanhada de outras igualmente fundamentais, sintetizadas e explicadas neste estudo a partir da ilustração (Figura 2):

Figura 2 - Níveis de apreensão da realidade pelo analista de IA

Fonte: elaborado pela autora.

O real, representado pela clássica imagem do iceberg, percebido inicialmente apenas em sua pequena porção superficial, permite caracterizar o indício, do verbo indicar, que significa indicação, sinal, sugestão, grau de inferência (GRABO, 2015). Como traduzido aqui, o indício passa justamente a ideia de que se trata de um nível inferior à certeza e, portanto, à evidência, como está representada na Figura 2.

Já indicador é diferente de indício e tem um sentido aproximado do que se utiliza em vários ramos do conhecimento, inclusive na Inteligência. Seleciona-se um indicador para monitorar a expectativa de que certa ameaça tem potencial de ocorrer. Grabo (2015) defende a distinção criteriosa entre os dois conceitos: "Um indicador é um passo conhecido ou hipotético que o inimigo pode ou deve tomar em preparação para as hostilidades" (GRABO, 2015, p.10 e 59). Em seguida, indicadores devem ser compilados em listas, que funcionarão como um conjunto de expectativas. Além de "monitoráveis", os indicadores devem

ser "preditivos, descritíveis, inequívocos e coletáveis" (GENTRY & GORDON, 2019, p. 133).

Grabo (2015) enfatizou, ainda, que, para se chegar a uma interpretação de Inteligência de Alerta, o analista terá utilizado quase sempre inferências. Por isso, a metodologia indiciária é indutiva: o profissional de IA chegará a suas conclusões a partir de fatos, ou melhor, com base no que ele pensa sobre os fatos: as conclusões resultantes de juízos e raciocínios[2] não serão alcançadas diretamente dos fatos, pois todo "processo é altamente subjetivo." Como o analista tem acesso apenas a indícios ("fragmentos ou migalhas" da realidade), ele pode ter de chegar a conclusões mais abrangentes (inferências) sobre as pretensões do inimigo. Para ela, "a subjetividade será ainda mais necessária no exame de questões de natureza política e de propaganda, do que em assuntos militares" (GRABO, 2015, p. 91 e 93).

Gentry & Gordon (2019) afirmam que a metodologia indiciária, entendida como "técnica ou viés de análise", evoluiu ao longo do tempo e assumiu "armadilhas de doutrina de Inteligência" (GENTRY e GORDON, 2019, p. 130-131), que podem ser entendidas como aquelas enfrentadas pelo analista de IA ao buscar desvendar a realidade.

Ainda assim, em Grabo já é possível identificar a formalidade do método e a busca por sua sistematização, representadas por etapas que o profissional de IA deve seguir no que é proposto aqui como Ciclo de Produção e Difusão da Inteligência Alerta (Figura 3): (1) reunião de dados e informações → (2) isolamento dos indícios mais relevantes e identificação de quais podem ser as intenções do adversário (aqui também poderia entrar o início da seleção de indicadores) → (3) avaliação da validade, do significado e da significância dos indícios, e análise de como podem estar relacionados com os fatos mais relevantes para caracterizar a ameaça → (4) interpretação de evidências que podem indicar as intenções do adversário → (5) preparação de *briefing* oral ou escrito para o decisor. Em resumo, o método permite a formação de juízos e raciocínios sobre indícios e evidências, para se chegar a juízos e raciocínios sobre os possíveis cursos de ação dos adversários e agentes adversos.

2 O termo utilizado por Grabo (2015) é *"judgement"*. Como, às vezes, ela separa *analyses* e *judgements*, aqui se optou por traduzir *"judgement"* como juízo e raciocínio, em referência à diferenciação feita pela Doutrina Nacional de Inteligência, na descrição das formas racionais e dos tipos de conhecimento (GRABO, 2015, p. 53 e 58).

Figura 3 – Ciclo de Inteligência de Alerta (foco no método)

Nota: Nenhum dos autores utiliza o conceito de Ciclo de IA. A proposta é da autora (vide p. 5 a 7).
Fonte: Esquema elaborado pela autora com base em Grabo (2015, p. 77) e Gentry & Gordon (2019, p. 130-133).

Antes, para uso exclusivamente militar, o analista aplicava o método da seguinte maneira: identificava uma "situação ruim" que já tinha evoluído ou poderia evoluir para hostilidades contra o país ou contra os interesses nacionais e monitorava a ameaça com indicadores. Hoje, uma "situação ruim" é denominada pelo Departamento de Defesa dos EUA ou pela Organização do Tratado do Atlântico Norte (Otan) como *"end-state"*. São definidos, a partir da probabilidade de ataque do País A sobre o País B, uma série de cenários mais plausíveis sobre como a hostilidade pode se materializar (Figura 3). Em geral, são construídos de três a cinco cenários, entre os mais e menos prováveis. Gentry & Gordon (2019, p. 131-132) não recomendam que se utilize o *"worst case scenario"* (pior cenário), pois acreditam que ele antecipa possibilidades antes do efetivo trabalho de análise estar completo.

Para cada cenário, os analistas indicam um caminho que pode levar ao *"end-state"*. Na medida do possível, os diferentes cenários devem ter um conjunto distinto de indicadores, entre militares, políticos, econômicos, sociais, tecnológicos etc. A etapa da reunião (Figura 3-1) deve ser constante para possibilitar a atualização oportuna dos cenários. "Quando os eventos [evidências] associados a um indicador mudam, o analista tem o indício de um possível movimento em direção (ou contrário) ao *'end-state'*" (GENTRY & GORDON, 2019, p. 133. Os grifos são dos autores) – Figura 3-2 e 3-4.

Por sua vez, interpretou-se neste estudo que os indícios, por sua natureza menos concreta, devem ser interpretados em toda sua expressão: na essência, como substantivo (significado) e, na qualidade, como adjetivo ou elementos descritores (significância). Assim estariam completam a validação e a qualificação do indício – Figura 3-3.

Gentry & Gordon (2019) defendem que há uma habilidade essencial ao profissional que aplica o método indiciário e que tem relação direta com a análise da trajetória (inflexões na linha do tempo): perceber mudanças e integrar novas informações, mesmo não-confirmadas, à interpretação em andamento. Por isso, explicam, consoante com Grabo (2015), que especialistas temáticos não seriam os melhores para identificar mudanças, porque ficam apegados a seus pontos de vista. Assim, não seria o analista de Bolívia, ao menos não sozinho, o mais indicado a ter observado a necessidade de alerta.

O exame do passado é essencial para a projeção do futuro. A analogia com os esportes olímpicos de arremesso de pesos ou dardos mostra que, quanto maior o posicionamento da mão para trás, maior o impulso para se atingir longas distâncias, mas só até certo limite. O desafio do analista, portanto, é compreender o quanto é preciso voltar ao passado para interpretar um indício no presente que se mostra com potencial de ameaça no futuro. Sem dúvida essa é uma forma de se reduzir as incertezas (Figura 2).

Boa parte da bibliografia caracteriza a metodologia indiciária como a detecção de anomalias dentro de padrões de normalidade: "uma cronologia é uma detectora de anomalias – e enquanto nem todas as anomalias levam a crises, todas as crises são feitas de anomalias" (GRABO, 2015, p. 69). Wirtz explica: "... a detecção de anomalias requer um estudo sustentado, de forma que os padrões de atividade que refletem a normalidade possam ser identificados" (WIRTZ, 2013, p. 558-559). Já Gentry & Gordon (2019) avaliam que a anomalia pode vir a ser um indício no futuro (Figura 3-3 e 3-4) e valorizam, igualmente, a construção de cronologias.

Tempos da Inteligência e vertentes de análise

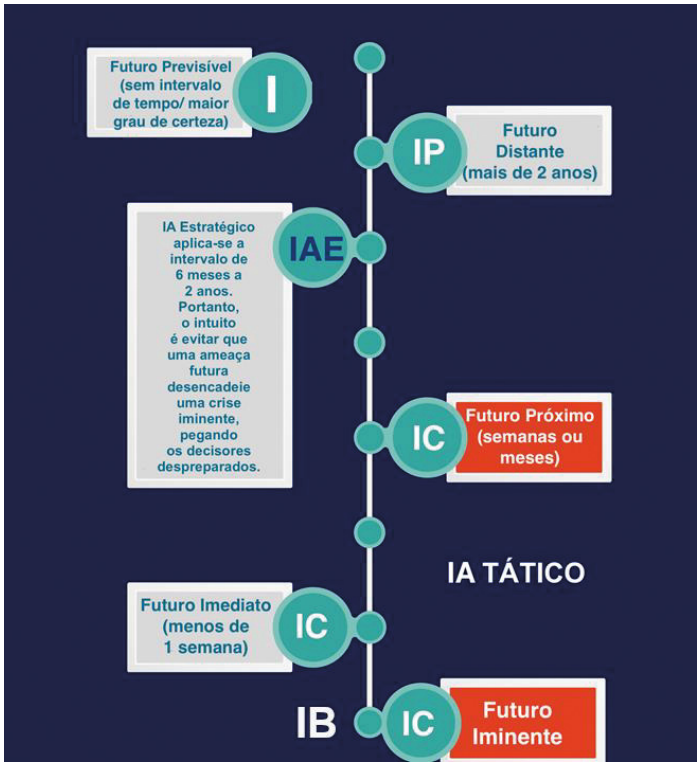
James Williams, antigo diretor da AID, no prefácio da obra de Grabo (2002), destacou que a Inteligência de Alerta difere da Inteligência Corrente e da Inteligência Prospectiva, porque "...aceita a presunção da surpresa e da Inteligência incompleta, e requer pesquisa exaustiva...". Afirmou que o desafio da Inteligência de Alerta é sua incompletude: relação não evidente entre eventos, sinais iniciais baseados em evidências fragmentadas ou relatórios contraditórios. Nessa diferenciação, Williams reforça a intangibilidade da IA, que não "é uma compilação de fatos. É uma

abstração, o intangível, uma percepção ou uma crença". Uma intuição.

São a intensidade e a complexidade que diferenciam a IA (GRABO, 2015). Ademais, o analista indiciário está atento à possibilidade – por mais remota que seja – de o adversário iniciar preparativos para uma ação hostil. Assim, o profissional de IA estará à frente dos demais do sistema de Inteligência, funcionando como o *"advogado do diabo"* (GRABO, 2015, p. 82).

A partir da autora estadunidense, pôde-se propor recortes temporais específicos para cada uma das tipologias da Inteligência (Figura 4), em complemento à análise de Faria (2017) sobre estudos de futuro e seu papel na melhoria da qualidade do assessoramento.

Figura 4 – tempos da Inteligência



Nota 1: As siglas representam:
IB (Inteligência de Base);
IC (Inteligência Corrente – nas três referências);
IAT (Inteligência de Alerta Tático);
IAE (Inteligência de Alerta Estratégico);
IP (Inteligência Prospectiva) e
I (Inteligência).
Nota 2: A diferenciação entre os tempos é de Grabo, mas a correlação com as vertentes da Inteligência é da autora.
Nota 3: A identificação e a delimitação temporal da IAE são de Gentry & Gordon.
Nota 4: A identificação e a caracterização de Futuro Distante para a Inteligência Prospectiva (IP) é da autora.
Fonte: Elaborado pela autora, com base em Grabo (2015) e Gentry & Gordon (2019).

Os ramos da Inteligência distribuem-se ao longo da trajetória que vai do mais próximo do presente ao futuro distante. A Inteligência Corrente foca no que está prestes a ocorrer, até cerca de uma semana adiante, ou mesmo poucas semanas. A principal característica da IC revela ainda a necessidade de consideração do passado recente. Hulnick (2008), também analista da CIA, ao tratar de todas as vertentes da Inteligência no assessoramento, comparou a IC à atividade jornalística: "...envolve reportes diários sobre o que aconteceu ontem, sobre o que está ocorrendo hoje, e sobre o que sucederá amanhã" (HULNICK, 2008, p. 224-225). Conclui que, apesar de ser demandada pelos clientes ao iniciar o dia, contraditoriamente, a IC é objeto de crítica por sua natureza menos analítica e mais descritiva ou narrativa. Já a Inteligência de Base, consolidação de temas basilares, ("uma compilação enciclopédica" – HULNICK, 2008, p. 225), trata de assuntos encerrados ou com desdobramentos de curto prazo.

A Inteligência de Alerta, por sua vez, aparece relacionada a praticamente todos os espectros de tempo da Figura 4. A partir do futuro iminente até o futuro próximo (de semanas ou meses), podem ser emitidos alertas táticos, e o futuro próximo também pode ser objeto de alertas estratégicos. Grabo (2015) define, ainda, o futuro previsível, não a partir de um limite cronológico, mas do grau de certeza do analista (por essa razão, aparece solto na linha do tempo).

Depois de apresentar propostas de vários autores para intervalos temporais de IA, Gentry & Gordon (2019) sugerem que o alerta estratégico se aplique a um período de seis meses a dois anos. A proposta permanece focada na antecipação de crises iminentes, como inúmeras vezes destacou Grabo (2015), no sentido de que cabe ao analista indiciário apresentar os fundamentos para se evitar ou minimizar uma crise que se apresenta, no momento ou em algum ponto futuro, como inevitável. Como a autora diferencia os alertas táticos e estratégicos também pelo tempo, pois esses últimos seriam de longo prazo, entende-se que sua insistência em se referir a alertas de crises iminentes (*"impending crisis"* – GRABO, 2015, p. 25, 53, 68 e 85) seja mais para dar um sentido de urgência e inevitabilidade, do que de proximidade temporal com o presente. Certamente, a iminência também pode se aplicar ao intervalo de poucas semanas ou meses. De todo modo, segundo ela, se a IA não escolher suas crises, não se diferencia da IC.

Davis (2003, p. 3) enfatiza os "perigos iminentes e potenciais"; Gentry & Gordon (2019, p. 12, 18, 94, 133 e 136) também mencionam "eventos e crises iminentes", mas parecem preferir "problemas de alerta emergentes". Outras técnicas complementam a I&A e deixam o profissional de Inteligência atento e imaginativo para identificar o mais

longe, em distância e tempo, "tendências emergentes de relevância" (GENTRY & GORDON, 2019, p. 149). Segundo os autores, porém, o ambiente de muita incerteza torna esse recorte analítico o mais desafiador de todos.

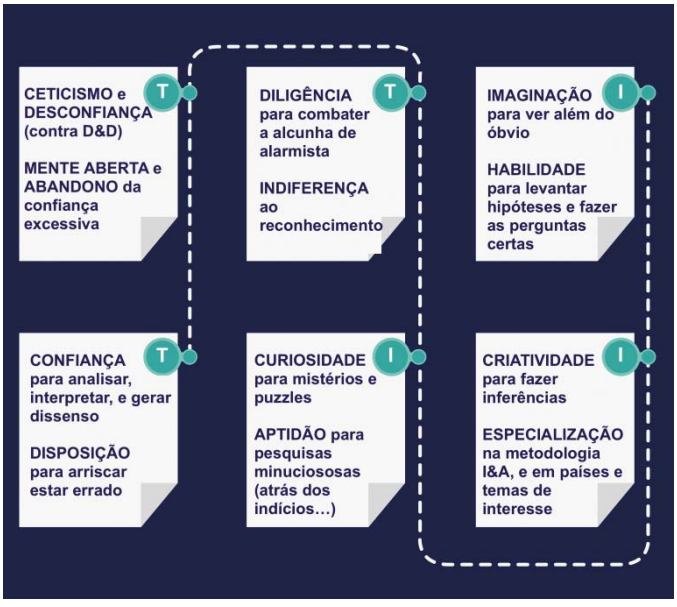
Por fim, a Inteligência Prospectiva é considerada por Hulnick (2008, p. 227) a categoria mais "...controversa e que envolve juízos e raciocínios simultâneos sobre o futuro e sobre a análise de Inteligência gerada para apoiar a Política". Aqui, reconhece-se que é sobretudo a metodologia a distinguir a IA da Inteligência Prospectiva, mas a proposta também é, para efeitos didáticos e metodológicos próprios, delimitar a IP para um período superior a dois anos (Figura 4), evitar sobreposições temporais indesejáveis e facilitar delimitações procedimentais.

Como é o bom analista de IA?

As duas obras principais utilizadas nesse estudo têm capítulos específicos e várias outras seções dedicadas a analisar as características cognitivas, intelectuais e de temperamento e caráter que fazem um bom profissional do método indiciário. Gentry & Gordon (2019) admitem que o que Grabo (2015) descrevera décadas atrás permanece válido até hoje.

Nesse estudo, foram selecionados (Figura 5) os atributos comportamentais e intelectuais considerados mais relevantes para a aplicação eficiente da metodologia de I&A:

Figura 5 – Bons analistas indiciários demonstram...



Legenda: T – diz respeito aos atributos de temperamento e comportamento. I – refere-se às características intelectuais e cognitivas desejáveis.
Fonte: esquema elaborado pela autora, com base em Grabo (2015) e em Gentry & Gordon (2019).

Gentry & Gordon (2019) resumem o diferencial do analista indiciário pela necessidade de apresentarem um "pensamento excepcional" (GENTRY & GORDON, 2019, p. 148 e 218). Acompanham Davis (2003) quando este afirma que o ofício do profissional de alerta é conseguir desenvolver uma "análise alternativa", ao avaliar ameaças que, para a maioria, são improváveis ou indeterminadas (DAVIS, 2003, p. 9; e DAVIS, 2007, p. 181-182).

Outro aspecto fundamental para todos é a preferência por analistas mais antigos na carreira, mais experientes e com alguma especialização antes de se dedicarem à Inteligência de Alerta.

Os demais traços de caráter levantados por Grabo (2015), Gentry & Gordon (2019) foram considerados neste estudo igualmente necessários para todos os profissionais de Inteligência: ser confiável e perspicaz; demostrar interesse e motivação; ter senso de responsabilidade, disposição para o trabalho duro e iniciativa.

Sobre características e habilidades intelectuais, os três autores apontaram, igualmente, a necessidade de objetividade, sofisticação analítica, capacidade para reconhecer o que é importante, competência criativa, perspectiva intelectual heterodoxa e questionadora, e capacidade de fazer apresentações lógicas e convincentes.

A Inteligência Indiciária e seu papel no assessoramento

Alertar é mais que informar. Esta distinção, nada simples, talvez seja o grande diferencial da IA nas organizações. O produto resultante da metodologia I&W implica ação para o ciclo da IA fechar-se (Figuras 1 e 3.5). A depender da circunstância e da natureza da ameaça ou da oportunidade, espera-se do decisor iniciativa, e não apenas reação à ação adversária. Mesmo que o usuário resolva não agir, tal decisão precisa ser consciente, o que difere da inação ou do desconhecimento da iminência das hostilidades.

Volta-se, assim, diversamente, ao imperativo do tempo: o sentido de oportunidade da IA é, de fato, peculiar. Não basta informar antes de o evento ocorrer; é preciso alertar para permitir a decisão. Essa análise oportuna é denominada *"action"* ou *"implementation analysis"* (GENTRY & GORDON, 2019, p. 212; e DAVIS, 2003, p. 12), cuja complexidade decorre do fato de que o tempo da Política não é o tempo da Inteligência.

A complexa relação entre Inteligência de Alerta e instância decisória

Com a perspectiva do cliente, completa-se o outro problema que o analista indiciário encara: "Os profissionais enfrentam dois desafios especiais no que diz respeito ao

alerta estratégico: superar seu próprio *mindset* e o dos usuários" (DAVIS, 2002 A, p. 3).

As falhas da Inteligência de Alerta podem resultar de limitações do método e das capacidades dos analistas, mas também das experiências, habilidades, preferências e dos interesses dos clientes. Quando Hulnick (2005) centrou seu estudo em IA e CT, e analisou fracassos e sucessos dessa corrente analítica nos EUA, abordou, na realidade, as falhas de percepção da relevância do alerta pelo usuário. Mais tarde, concluiu: no que diz respeito a alertas, as conexões entre Inteligência e Política têm um aspecto distintivo que vai além de saber do que os decisores precisam; é necessário garantir que eles estejam entendendo o que estão vendo, ou seja, que uma crise se avizinha (HULNICK, 2008).

A bibliografia é farta ao explorar formas de superação dos entraves postos pelos usuários: conhecer suas idiossincrasias; conquistar sua confiança e criar formas de persuadi-los (Figura 1); mostrar a relevância e a qualidade da Inteligência frente a outros produtos de assessoramento, em especial aqueles da instância política; ajudá-lo a superar o viés da falta de objetividade. Segundo Davis (2002 A e 2003), o próprio cliente pode sentir-se confiante em contribuir para a seleção dos problemas de alerta, juntamente com os órgãos de Inteligência. Assim, facilita-se a abertura de canais diretos de comunicação, e os alertas estratégicos tornam-se assunto governamental mais do que responsabilidade exclusiva da Inteligência, o que tanto Davis (2003) quanto Gentry & Gordon (2019) identificaram no modelo inglês do *Joint Intelligence Committee* (JIC – Tabela 1).

O desafio, no entanto, é que essa aproximação não leve à "politização da Inteligência" (DAVIS, 2002 B e 2003, p. 15; GENTRY & GORDON, 2019, p. 204). Os três autores admitem que essa preocupação é herança de Sherman Kent, mas defendem ser necessário aos profissionais de Inteligência conhecerem o governo estadunidense e seus representantes tanto quanto conhecem governos de países inimigos ou aliados. "Quanto mais os analistas souberem sobre o processo decisório norte-americano, e quanto mais compreenderem os desafios enfrentados pelos decisores, melhor posicionada estará a Inteligência em sua atribuição de prover alertas estratégicos" (DAVIS, 2002 A, p. 9).

Em linha com Kent, na divisão de trabalho entre analistas e decisores, "o papel do oficial de Inteligência na *'action analysis'* é identificar e analisar; já os formuladores de política têm a responsabilidade profissional de recomendar e escolher" (DAVIS, 2003, p. 12). O contato direto deve permanecer para melhor guiar os planos de contingência e evitar as atitudes do "*wait and see*" ou "*so-what*?" (WIRTZ, 2013, p. 557).

Davis (2003) destaca que a reticência

ou a demora dos usuários em levar em consideração alertas, mesmo bem fundamentados, decorre de distrações com temas politicamente mais prementes, e da lembrança de "falsos positivos" e dos altos custos pagos ao se adotar medidas contra hostilidades que não se realizaram (DAVIS, 2003, p. 4).

Por sua vez, a aplicação adequada do método não é menos relevante. Davis (2003, p. 8) conclui: "(...) É o balanço favorável entre evidência e inferência que galvaniza os clientes para a ação". Seguir um método ajuda o cliente a ser melhor assessorado, pois ele mesmo pode: estimular posições divergentes; fazer perguntas certas; explicar a necessidade da informação; compartilhar o que não precisa ser negado ou compartimentado (GRABO, 2015); e estar aberto a novos assuntos ou temas inesperados (WIRTZ, 2013), para além de suas preferências políticas ou pessoais.

Arranjos institucionais para o assessoramento da Inteligência Indiciária

Há décadas, Grabo apontara o desafio, atual, das organizações de competir com os assessorados que "...se valem de sua própria Inteligência" (GRABO, 2015, p. 27), o que recoloca a questão muito bem trabalhada por Gentry & Gordon (2019) sobre como os Estados podem integrar de forma mais eficiente a Inteligência de Alerta em seus arranjos institucionais.

O quadro comparativo a seguir abrange variações históricas e geográficas, ou seja, sintetiza como diferentes países, ao longo do tempo, deram maior ou menor espaço à Inteligência Indiciária, experiência que nos ensina um conjunto de vantagens e desvantagens resultantes da adoção de cada um dos modelos: 1) cada especialista temático tem a tarefa adicional de aplicar a Inteligência de Alerta; 2) há uma organização especializada em IA; 3) existem estruturas híbridas entre os tipos 1 e 2; 4) os alertas são responsabilidade de todo o aparelho de Estado.

Percebe-se, além disso, pelo quadro-síntese, que alguns países concentram a Inteligência de Alerta em temas mais típicos de segurança doméstica, como contraterrorismo. Gentry & Gordon (2019) são entusiastas, por exemplo, da aplicação da metodologia indiciária que o serviço holandês faz para a emissão de alertas táticos e estratégicos voltados a CT.

Quadro 1 – Estruturas governamentais de Inteligência de Alerta

	CARACTERÍSTICAS	VANTAGENS	DESVANTAGENS
1 – Cada analista tem a tarefa adicional de IA.	Adotado em países com múltiplas agências, como os EUA, ou em Estados menores, com serviços de Inteligência modestos. Há um modelo "moderado ou híbrido" (CIA), que aceita o papel separado de alerta de outras organizações. E existe uma versão "rígida", em que todos os analistas devem reportar, pelos canais tradicionais, ameaças e oportunidades durante seus trabalhos de coleta, IC ou IP. A ideia é que todo profissional deve realizar "Inteligência antecipatória", algo muito ironizado e criticado pelos autores.	Todos os assuntos considerados importantes pela Inteligência são monitorados. Todo o serviço e seus analistas estão, em princípio, disponíveis para tratar de temas de alerta. A relação de confiança entre serviço e usuário está estabelecida para todo tipo de assessoramento, inclusive para os problemas de alerta. Muitos profissionais de reconhecida capacidade acreditam nesse modelo.	Analistas são consumidos pela rotina e não têm tempo para IA; O caminho regular de revisão aumenta o tempo de difusão; O caminho regular, em documentos tradicionais, deixa os assuntos de alerta soltos; Pode faltar credibilidade ao produto; Temas de alerta são raros *vis-à-vis* à IC; Faltam os atributos necessários ao analista de IA; Visões tradicionais e conservadoras dos analistas temáticos preponderam sobre a IA.
2 – Organizações especializadas em IA	Atribui a uma organização a responsabilidade pelos alertas: EUA (anos 1950 e 1960), ou Austrália (Sistema de Defesa de Alerta). Na Bélgica e na Holanda, os alertas dedicam-se a CT. Na União Europeia, há um Centro de Análise de Inteligência também com responsabilidades de *"early warning"*.	Uma estrutura exclusiva voltada a alertas permite dedicação, especialização, prioridade na coleta e no treinamento, com foco em usuários que, provavelmente, conhecem e aguardam esse produto específico de Inteligência.	Não é fácil atrair profissionais que queiram se dedicar apenas a IA; Analistas não podem contar com as unidades temáticas, a não ser que haja troca efetiva entre agências. Casos de alerta tendem a ser escassos, o que pode parecer aos demais que é uma unidade improdutiva.
3 – Estruturas híbridas (2 e 3)	Combina o que há de melhor da versão "moderada" do 1º modelo com o 2º: unidades dedicadas a alertas que funcionam como ponto focal, de articulação e coordenação com áreas temáticas especializadas. Seguido pelo Japão atualmente.	Uma unidade voltada a IA e que trabalha de forma articulada com unidades temáticas ou especializadas em outras metodologias (IC, IB, IP e D&D) tende a aproveitar a qualificação de cada uma e a minimizar as respectivas fragilidades.	Como mostra a história estadunidense *(National Intelligence Office for Warning* – NIO/W – 1979-2011), esse modelo fica muito dependente das peculiaridades da personalidade do coordenador da unidade de IA.

	CARACTERÍSTICAS	VANTAGENS	DESVANTAGENS
4 – Alertas são de todo governo	Vários órgãos de governo, e não apenas a Inteligência, respondem por situações de alerta, como ocorre no Reino Unido (JIC) e em Cingapura.	Maior capacidade de coleta e várias *expertises* para a identificação de temas de alerta. Reduz a distinção entre "produtores" e "clientes" da Inteligência de Alerta.	Muito dependente de relações próximas entre agências governamentais muitas vezes bem distintas. Essa integração precisa funcionar para o modelo dar certo.

Fonte: elaborada pela autora, com base em Gentry & Gordon (2019, p. 54 a 108, e 215 a 240).

Os autores revelam sua preferência pelo modelo 3, mas admitem que não há um tipo ideal de inserção da Inteligência Indiciária. O problema é que, a depender de seu baixo grau de integração ou de seu elevado isolamento em relação ao restante das instituições ou estruturas do Estado, a eficiência do alerta é negativamente afetada. As razões para essas variações nos tipos organizacionais certamente não estão relacionadas apenas a preocupações com a qualidade do trabalho, mas são também de natureza burocrática, política, pessoal (do gestor ou dirigente) e, talvez, acima de tudo, resultam dos fatores confiança e preferência: confiança, ou não, na capacidade da IA em, de fato, preparar o Estado para lidar com situações inesperadas e ameaçadoras; preferência por assuntos mais prementes, de curto prazo, ou seja, crença na maior necessidade da Inteligência Corrente.

A extinção do *National Intelligence Office for Warning* (NIO/W), em 2011, revela que os próprios EUA acabaram por mostrar certo descrédito em relação à IA, ao apoiar, na última década, sobretudo o modelo 2 "rígido" (Tabela 1). Depois de tantas reestruturações da Inteligência estadunidense após 11 de setembro, o que se verificou foi o escrutínio constante da IA – refletido em seus reposicionamentos na estrutura governamental – e o crescimento exponencial do espaço da Inteligência Corrente, inclusive com a perda da *expertise* dos analistas de pensarem a partir de uma linha do tempo ampliada e avaliarem diversos futuros possíveis (Figura 4).

Gentry & Gordon (2019) valem-se de dois colegas sêniores da CIA para enfatizar sua crítica ácida à tirania da IC entre estadunidenses, australianos e britânicos: Douglas MacEachin (2002) refere-se à "armadilha da Inteligência Corrente" (MACEACHIN *apud* GENTRY & GORDON, 2019, p. 218), coloquialmente explicada com a metáfora da *"fábula do sapo fervente"*: o sapo e os que o cercam ignoram que a água está aquecendo lentamente, até ser tarde demais e a crise estar instaurada. Por sua vez, Carl Ford (2006) confessa: "Se eu tiver de apontar um problema específico

que explica porque estamos fazendo um trabalho tão ruim em Inteligência, é o foco obstinado em relatórios de Inteligência Corrente" (FORD, *apud* GENTRY & GORDON, 2019, p. 217). E esse foco seria decorrência justamente do imediatismo e das preferências dos usuários.

Seguindo a tradição de Grabo (2015), para Gentry & Gordon (2019), o ideal seria haver um equilíbrio entre as tipologias e uma integração das especialidades em prol da qualidade da produção e do assessoramento de Inteligência, o que fica nítido na Tabela 1, com seu entusiasmo pelo modelo 3. Para ambos, pode tranquilamente ocorrer que temas de Inteligência Corrente se convertam em problemas de alerta; no entanto, o que não pode absolutamente acontecer é a Inteligência Indiciária acabar se transformando em IC, e os analistas de IA não perceberem que o tema de alerta não é mais pertinente.

Considerações finais

É dever de todo profissional de Inteligência alertar? Sim e não!

Não, porque, primeiro, o ofício indiciário é particular no universo da Inteligência e é caracterizado por objetivos definidos, metodologia própria, recortes temporais claros e uma aproximação bastante peculiar entre os atores envolvidos: produtor da informação, adversário, agente adverso e usuário.

Em segundo lugar, idealmente, o profissional de Inteligência deve apresentar um perfil muito específico, com experiência, comportamentos e habilidades desenvolvidas especialmente para conseguir superar as armadilhas colocadas pelo trabalho com indícios e inferências, ou seja, com uma perspectiva analítica, por definição, menos tangível que outras tipologias e cujo objeto são preferencialmente os mistérios. Por fim, a Inteligência de Alerta pode ser atribuição apenas de uma organização ou unidade especializada no serviço de Inteligência, dedicada, exclusivamente, à aplicação das técnicas de I&A.

Ao mesmo tempo, sim, pode vir a ser dever de todo profissional de Inteligência alertar, caso essa seja a decisão do órgão finalístico, ou seja, dividir a responsabilidade de identificação e acompanhamento de problemas de alerta entre todos os analistas, com ou sem articulação com uma unidade de Inteligência de Alerta específica. O diferencial continuará sendo a necessidade de capacitação dos profissionais para a aplicação do método indiciário.

O Brasil, com suas agências especializadas ou em conjunto, como Sisbin, tem maturidade para selecionar e monitorar temas de alertas táticos e estratégicos, e definir assuntos emergentes entre aqueles mais tradicionais, relativos a ameaças e oportunidades para o país. O amadurecimento do sistema brasileiro

permite que sejam testados distintos arranjos institucionais para a inserção da IA à estrutura do Estado. A integração entre os órgãos também possibilita a troca de experiências entre profissionais que apliquem metodologias típicas das diferentes vertentes da Inteligência: Inteligência Indiciária, Inteligência Corrente, Inteligência de Base e Inteligência Prospectiva, sem necessidade ou risco de predominância de um ramo, em detrimento de outro.

Dessa forma, saem beneficiados profissionais e órgãos de Inteligência, com a preservação da autenticidade de seu ofício, e clientes, com a qualidade do assessoramento, fruto da capacidade de antecipação, da comunicação eficaz, da prontidão e de produtos oportunos e diversificados.

Figura 6 – Ciclo de Inteligência de Alerta: universo conceitual e características

Fonte: elaborado pela autora

Referências

BRASIL. Gabinete de Segurança Institucional. Agência Brasileira de Inteligência. *Doutrina Nacional da Atividade de Inteligência*: fundamentos doutrinários. Aprovada pela Portaria nº 244 - ABIN/GSI/PR, de 23 de agosto de 2016. Brasília: Abin, 2016.

DAVIS, Jack. Strategic Warning: If Surprise is Inevitable, What Role for Analysis? *The Sherman Kent Center for Intelligence Analysis Occasional Papers: Volume 2, no. 1*, 2003. Disponível em https://www.hsdl.org/?abstract&did=442470. Acesso em: 11 jul. 2022.

DAVIS, Jack. Sherman Kent and the Profession of Intelligence Analysis. *The Sherman Kent Center for Intelligence Analysis Occasional Papers: Volume 1, no. 5*. Sherman Kent Center, 2002. Disponível em https://www.hsdl.org/?view&did=442468. Acesso em: 12 ago. 2022.

DAVIS, Jack. Improving CIA Analytic Performance: Strategic Warning. *The Sherman Kent Center for Intelligence Analysis. Occasional Papers: Volume 1, no. 1*. Sherman Kent Center, 2002. Disponível em https://www.hsdl.org/?abstract&did=449505. Acesso em: 11 jul. 2022.

DAVIS, Jack. Strategic Warning: Intelligence support in a world of uncertainty and surprise in *Handbook of Intelligence Studies*. Lock K. Johnson. Disponível em https://www.routledgehandbooks.com/doi/10.4324/9780203089323.ch13. Acesso em: 11 ago. 2022.

FARIA, Bruno. *Estudos de futuro aplicados à Atividade de Inteligência:* possibilidades. Conclusão de Curso (Aperfeiçoamento em Inteligência). ABIN/ ESINT, 2017.

GENTRY, John A. & GORDON, Joseph S. *Strategic Warning Intelligence:* History, Challenges, and Prospects. Georgetown University Press, 2019.

GRABO, Cynthia with Jan Goldman. *Handbook of Warning Intelligence*. Complete and Declassified Edition. Rowman & Littlefield, 2015.

GRABO, Cynthia. *Anticipating Surprise:* Analysis for Strategic Warning. Joint Military Intelligence College's Center for Strategic Intelligence Research. Defense Intelligence Agency, 2002.

HULNICK, Arthur S. The intelligence producer – policy consumer linkage: A theoretical approach. *Intelligence and National Security*, 1:2, 2008. Disponível em https://pt.booksc.

org/book/39636362/4cd38b. Acesso em: 26 ago. 2022.

HULNICK, Arthur S. Indications and Warning for Homeland Security: Seeking a New Paradigm. *International Journal of Intelligence and Counterintelligence, 18, 2005*. Disponível em https://pt.booksc.org/book/29907550/7be597. Acesso em: 11 jul. 2022.

KIMMELMAN, Susann. *Indications and Warning Methodology for Strategic Intelligence*. Naval Postgraduate School (U.S.). Monterey, Califórnia, 2017. Disponível em https://www.hsdl.org/?abstract&did=808274. Acesso em: 11 jul. 2022.

MAISONNAVE, Fabiano. Morales invade Petrobras e nacionaliza gás. *Folha de São Paulo*, 2 maio 2006. Disponível em https://www1.folha.uol.com.br/fsp/dinheiro/fi0205200602.htm. Acesso em: 30 jul. 2002.

RIBEIRO, Alexandre Carreira. *Uso de Ferramentas de Análise de Risco na Prevenção ao Terrorismo no Brasil*. Conclusão de Curso (Aperfeiçoamento em Inteligência). ABIN/ESINT, 2019.

WIRTZ, James J. Indications and Warning in an Age of Uncertainty, *International Journal of Intelligence and CounterIntelligence,* 26, no. 3, 2013. Disponível em https://core.ac.uk/download/pdf/36739628.pdf. Acesso em: 27 jul. 2022.

Artigo

8

TÉCNICA DE AVALIAÇÃO DE DADOS (TAD) E FONTE EM INTELIGÊNCIA

DOI: https://doi.org/10.58960/rbi.2023.18.232

Irene Calaça *

Resumo

O objetivo do presente trabalho é apresentar a profissionais de Inteligência em formação o julgamento de fonte (conforme a Técnica de Avaliação de Dados - TAD), as dificuldades em estabelecer esse julgamento e possíveis formas de minimizá-las. Sabe-se que o conhecimento produzido pela Atividade de Inteligência é utilizado para reduzir incertezas dos usuários, e que deve ser elaborado a partir de metodologia. Uma das etapas é a checagem da fonte e do dado por ela produzido, que auxilia a qualificar o conhecimento de Inteligência e atestar sua veracidade. Dados em Inteligência são oriundos de fontes abertas, meios tecnológicos e fontes humanas. A idoneidade dessas fontes é julgada por três aspectos: autenticidade, confiança e competência; já a credibilidade do conteúdo, por coerência, compatibilidade e semelhança dos dados. Podem interferir na análise de idoneidade da fonte questões como: diferenças taxonômicas entre órgãos; interpretações diversas de dados obtidos por meios técnicos ou órgãos parceiros; existência de rumor; interferência de vieses cognitivos na percepção da fonte; necessidade de adaptação da TAD tanto para fontes humanas, como fontes tecnológicas; necessidade de checagem de imagens, gravações de voz, vídeo e outras quanto a inconsistências temporais, geográficas ou de metadados. Essa é uma área basilar para a Inteligência, que exige do analista pensamento crítico e capacidade de trabalho em equipes horizontais, com revisão pelos pares; e exige da instituição oferta de meios tecnológicos para aprimoramento de análises, além de melhoria do sistema de armazenamento e recuperação de dados, de forma a permitir a reavaliação desses com certo distanciamento histórico.

Palavras-chave: Técnica de Avaliação de Dados; fonte; idoneidade da fonte.

DATA EVALUATION TECHNIQUE AND INTELLIGENCE SOURCE

Abstract

The aim of this study is presenting to Intelligence intern the judgment of the source (according to the Data Evaluation Technique, TAD, in Portuguese), the difficulties in establishing this judgment and possible ways to minimize them. It is known that the Intelligence knowledge is used to reduce the uncertainties of users, and that it has a methodological basis. One of the stages of the process is the verification of both the source and the produced data, which helps to qualify the Intelligence's knowledge and attest to its veracity. Intelligence data comes from open sources, technological means and human sources. The adequacy of these sources is judged from three aspects: authenticity, reliability, and competence. The credibility of the content is evaluated through the coherence, compatibility and similarity of the data. Issues that may affect the analysis are: taxonomic differences between organizations; different interpretations of technical mean data or partner data; existence of rumor;

* Especialista em Bioética pela Universidade de Brasília (UnB). Mestre em Letras e Linguística pela Universidade Federal de Goiás (UFG). Oficial de Inteligência da Agência Brasileira de Inteligência.

interference of cognitive biases in the perception of the source; adapting the TAD to both human and technological sources; checking images, voice recordings, video and the like for temporal, geographical or metadata inconsistencies. This is a key area for Intelligence, which requires from the analyst critical thinking and ability to work in horizontal teams, with peer review. It also demands from the organization technological means to improve the analysis, as well as improve the data storage and retrieval system, in order to allow the reassessment of these with a certain historical impartiality.

Keywords: *Data Evaluation Technique; source; source reliability.*

TÉCNICA DE EVALUACIÓN DE DATOS Y FUENTES DE INTELIGENCIA

Resumen

El objetivo de este estudio es presentar a los internos de Inteligencia el juicio de la fuente (según la Técnica de Evaluación de Datos, TAD, en portugués), las dificultades para establecer este juicio y las posibles formas de minimizarlas. Se sabe que el conocimiento producido por la Actividad de Inteligencia se utiliza para reducir las incertidumbres de los usuarios, y que debe ser elaborado a partir de la metodología. Uno de los pasos es la verificación de la fuente y los datos producidos por ella, lo que ayuda a calificar el conocimiento de la Inteligencia y atestiguar su veracidad. Los datos de Inteligencia provienen de fuentes abiertas, medios tecnológicos y fuentes humanas. La idoneidad de estas fuentes se juzga desde tres aspectos: autenticidad, fiabilidad y competencia. La credibilidad del contenido se examina a través de la coherencia, compatibilidad y similitud de los datos. Pueden perjudicar el análisis cuestiones como diferencias taxonómicas entre órganos; diversas interpretaciones de los datos obtenidos por medios técnicos u organismos asociados; existencia de rumores; interferencia de sesgos cognitivos en la percepción de la fuente; la necesidad de adaptar la TAD a las fuentes humanas y tecnológicas; la necesidad de verificar imágenes, grabaciones de voz, vídeo y otros para detectar inconsistencias temporales, geográficas o de metadatos. Esta es un área clave para la Inteligencia, que requiere que el analista piense críticamente y trabaje en equipos horizontales, con revisión por pares; y requiere que la institución ofrezca medios tecnológicos para mejorar el análisis, así como mejorar el sistema de almacenamiento y recuperación de datos, a fin de permitir la re-evaluación de estos con cierta imparcialidad histórica.

Palabras clave: Técnica de Evaluación de Datos; fuente; confiabilidad de la fuente.

Introdução

Com base em pesquisa bibliográfica aberta, o presente artigo apresenta e discute a Técnica de Avaliação de Dados (TAD) na Atividade de Inteligência, aponta áreas nebulosas que envolvem a checagem da idoneidade da fonte e traz alguns meios para sobrepujá-las. O material se divide em quatro tópicos. Nos dois primeiros, breve exposição teórica ("Sobre Fontes e Dados" e "A Técnica de Avaliação de Dados -TAD"). Indagações levantadas pela prática encontram-se reunidas em "Nublando a fonte", e ajustes são propostos em "Clareando a fonte". O material se destina, principalmente, a profissionais de Inteligência em formação.

Sobre fontes e dados

No Brasil, "dados" são "qualquer representação de coisa ou evento não produzida pelo profissional de Inteligência" (DNAI, BRASIL, 2016).

Fonte de dados na Inteligência são documentos, meios técnicos e fontes humanas (parceiros, recrutados e colaboradores) que estejam ligados a eventos e sejam aptos a repassar aos profissionais de Inteligência dados que armazenam, conhecem, acompanham ou testemunham. Essas fontes são espécie de lente, a qual deve ser ajustada para permitir a visualização mais fidedigna[1] possível de fatos, estados ou eventos.

O dado[2] fornecido pela fonte deve ser analisado de acordo com a Técnica de Avaliação de Dados (TAD) e, a depender de sua qualidade, receber respaldo para ser ou não usado em conhecimento de Inteligência.

Nesse processo, vale lembrar que:

> o conhecimento é formado por juízos mentais, raciocínios complexos e representações conceituais, os quais descrevem e interpretam eventos e dados, e se manifestam através da linguagem; e
>
> existem quatro estados da mente frente à expressão da verdade – certeza, quando a mente acredita[3] na concordância integral entre imagem formada e o objeto a ser representado; opinião, quando há conformidade parcial (provável) entre

1 O conhecimento objetiva atingir a verdade, e é conceituado como "a representação de coisa ou evento real ou hipotético, de interesse para a Atividade, produzida pelo profissional de Inteligência" (DNAI, BRASIL, 2016, p. 57).

2 O termo "dado" é encontrado com, pelo menos, dois escopos diferentes: a Doutrina de Inteligência de Segurança Pública (2009) e outras, conforme descritas em Irwin e Mandel (2019), Capet e Revault D'Allonnes (2014), sugerem a organização das unidades de informação em três níveis, que se distinguiriam por seu maior ou menor processamento e qualidade, a saber: dados (brutos); informação (organização dos dados por meio de técnicas estruturadas e metodologia, que geraria novo conteúdo semântico e significado) e conhecimento de Inteligência (raciocínio elaborado a partir da Metodologia de Produção do Conhecimento). Por outro lado, a Doutrina Nacional da Atividade de Inteligência (BRASIL, 2016) teria mantido dois níveis (dado e conhecimento de Inteligência), abordagem que ora adotamos.

3 É preciso atentar que, quando em estado de certeza, o sujeito imagina ter atingido a verdade, e pode manter suas convicções mesmo diante de erros – por exemplo, quando está sob influência de vieses cognitivos e não percebe a inadequação dos argumentos que utiliza. Detalhes em Machado, 2018.

imagem e objeto; dúvida, quando há razões tanto para se aceitar, como para se refutar a imagem criada; ignorância, quando a mente não consegue visualizar nenhuma imagem do objeto.

A relação entre conhecimento, estados da mente e posicionamento do profissional em relação à verdade delineia a compreensão de certeza e incerteza na Atividade de Inteligência e se reflete na produção de conhecimento.

O conhecimento produzido pela Atividade de Inteligência é utilizado para reduzir as incertezas dos usuários, e deve ser elaborado a partir da metodologia de produção de conhecimento (MPC), para que possa representar a realidade o mais fielmente possível e com o mínimo de ambiguidades.

Importante componente das fases Reunião e Processamento na MPC é a checagem da fonte e do conteúdo, do dado por ela produzido, a fim de qualificar o conhecimento e atestar sua veracidade. Contudo, é importante lembrar que que dados são representações de coisas e eventos que, por sua adequação, são apropriadas pelo profissional de Inteligência no processo de construção do conhecimento.

Os dados podem ser compostos por observações simples sobre fatos, estados ou eventos e caracterizam-se por serem estruturáveis, quantificáveis, transferíveis e coletáveis. Eles podem ser obtidos de forma automática, por máquinas e sensores, e serem representados e transmitidos através de diversos suportes: forma textual, gráfica ou por sinais (LUZ, 2019, p. 27). O dado só recebe significância, ou seja, passa a ser conhecimento, quando processado pelo analista através da MPC.

Os dados que servem de base para a produção do conhecimento pelo analista são produzidos por fontes que podem ser pessoas, imagens, sinais, documentos e bases de dados obtidos através de coleta e análise. Kaminski (2019) lembra que proteger fontes e métodos empregados na produção de conhecimento faz parte da segurança nacional de cada país.

As fontes de dados em Inteligência, por sua vez, são originárias de fontes abertas, meios tecnológicos e fontes humanas. A Inteligência de fontes abertas (OSINT) surge da coleta dados de fontes disponíveis para o público geral, como periódicos técnicos, internet, meios de comunicação, redes sociais e dados estatísticos. OSINT também pode incluir informações que, embora não-classificadas, são consideradas sensíveis, como dados pessoais, econômicos e de produção (KAMINSKI, 2019, p. 98).

A Inteligência oriunda de sensores e meios tecnológicos é bastante diversificada. A Inteligência de imagens (IMINT) deriva da análise de imagens fixas e vídeos; a Inteligência geográfica (GEOINT) utiliza imagens enriquecidas com dados geoespaciais; a Inteligência de sinais (SIGINT) capta dados oriundos do espectro

eletromagnético (Inteligência eletrônica e de comunicações); a Inteligência de medidas e assinaturas (MASINT) registra medidas de eventos como explosões atômicas; e, finalmente, a Inteligência cibernética (CYBINT) emprega dados obtidos no espaço cibernético (BRASIL, IMT, 2015, p. 19-23)[4].

A Inteligência de fontes humanas (HUMINT), por outro lado, envolve a coleta de informações por seres humanos, seja aberta ou secretamente. O uso de fontes humanas implica risco (inclusive legal) e requer cuidado no gerenciamento dessas, para que se possa separar a opinião pessoal da fonte humana daqueles dados que ela dispõe, a fim de se chegar à verdade. O gerenciamento também acontece por necessidade de acompanhamento psicológico durante todo o processo, principalmente por ocasião do desligamento da Atividade, para evitar saídas não-amigáveis e danos à imagem da instituição (KAMINSKY, 2019; BURKETT, 2013; RONIN, 2002).

De acordo com Kaminski *(ibidem)*, a Atividade de Inteligência adquire maior valor quando consegue conciliar dados de diferentes fontes, na denominada *All-source Intelligence* (Inteligência de todas as fontes). É uma empreitada difícil, pois a compilação de dados costuma ser efetuada por diferentes órgãos do governo, que possuem objetivos próprios e buscam se destacar perante a administração pública e a sociedade para obtenção de recursos, o que dificulta a manutenção do sigilo[5] e gera relutância para cooperação[6] e compartilhamento de dados.

A Técnica de Avaliação de Dados (TAD)

Como avaliar se a fonte e o dado por ela produzido são corretos e confiáveis, ou seja, se detêm a qualidade necessária para compor conhecimento de Inteligência? Pela aplicação de Técnica de Avaliação de Dados (TAD), que julga a idoneidade de fonte (do produtor do dado) e a credibilidade dos dados, no intuito de garantir maior aproximação com a verdade. A Doutrina de Inteligência de Segurança Pública (DNISP, 2009), por exemplo, propõe que se confira a idoneidade da fonte por três aspectos: autenticidade, confiança e competência.

(i) Autenticidade, verifica-se se o

4 Atualmente existem sites, programas e aplicativos que auxiliam os interessados a checarem adulteração de imagens e vídeos, o que facilita a avaliação dos dados, como TinEye, Google Earth, SunCalc, Cybermap Kaspersky e outros, a depender da necessidade.

5 Lahneman (2010) trabalha a questão do sigilo e do repasse de dados nos Estados Unidos da América (EUA). O autor esclarece que a concepção tradicional da corrente de informação divide os dados entre os já conhecidos e os a conhecer, os dados secretos e os abertos. Atualmente, a comunidade de Inteligência estaria inserida em novo perfil, de acordo com o qual todos participariam do preenchimento de quebra-cabeças único ao elaborar o conhecimento de Inteligência. Assim, além de dados abertos e secretos, far-se-ia necessária outra categoria de dados – os dados "confiáveis", advindos de parceiros do governo. O rótulo "confiável" contornaria o "sigiloso" e facilitaria a intermediação de dados e conhecimentos entre parceiros.

6 Exemplo de relacionamento conflituoso numa mesma comunidade de Inteligência tem lugar entre a Agência Central de Inteligência (CIA) e a Direção Nacional de Inteligência (DNI), nos EUA (ROSE, 2017).

dado ou conhecimento provém realmente da fonte presumida (originou o dado), ou de intermediários. (...)

(ii) Confiança (...), verifica-se, sobre a fonte, antecedentes e comportamento social, colaboração anterior procedente e motivação de ordem ética ou profissional. Pode-se considerar, ainda, instrução, valores, convicções, maturidade.

(iii) Competência, verifica-se se a fonte é habilitada (técnica, intelectual e fisicamente), e detinha (... condições ambientais adequadas) para obter aquele dado específico.

Em relação ao conteúdo do dado, a DNISP (2009) sugere a verificação da credibilidade por três aspectos:

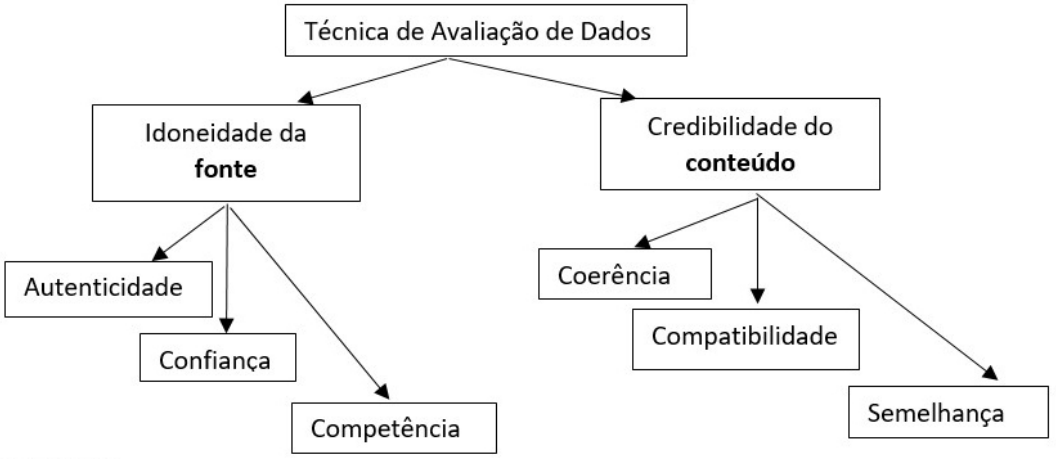
(i) Coerência, verifica-se se o dado apresenta contradições em seu conteúdo, no encadeamento lógico (cronologia) e na harmonia interna (sequência lógica); (também pode ser empregado para definir a autenticidade da fonte).

(ii) Compatibilidade, verifica-se o grau de harmonia com que o dado se relaciona com outros dados conhecidos (se é factível).

(iii)Semelhança, verifica-se se há outro dado, oriundo de fonte diversa, que venha reforçar, por semelhança, os elementos do dado sob observação.

A TAD pode ser visualizada no seguinte esquema:

Figura 1 - Esquema da TAD



Fonte: elaborado pela autora

A TAD se realiza por série de questionamentos aos quais o profissional de inteligência busca responder: existe a certeza de que o dado foi realmente proferido por fonte qualificada no contexto descrito? O conteúdo representa a realidade em sua totalidade? Teria sido adulterado? Há dúvidas ou inconsistências, ainda que parciais, que não permitam plena aceitação do conteúdo? Adiante listamos questionamentos a serem esclarecidos durante julgamento de fonte e conteúdo. Note que alguns quesitos de um e outro elemento se inter-relacionam.

Quadro 1 - Questionamentos sobre fonte e conteúdo

ANÁLISE DA FONTE:	ANÁLISE DO CONTEÚDO:
Quem é a real fonte do conteúdo?	De onde provém o conteúdo? Dados de autoria.
É possível estabelecer autenticidade da fonte?	Quando foi proferida a mensagem? Checar datas.
É fonte qualificada (possui autoridade) para proferir o enunciado?	Em que contexto foi proferida a mensagem?
É fonte primária ou secundária?	O conteúdo é coerente ou existem incongruências (temporais, geográficas, técnicas, linguísticas)?
E fonte ou canal de difusão da mensagem?	Os *metadados* (informações incorporadas ao arquivo) encontram-se alterados? Podem ser checados por sites e programas?
É patrocinadora? Intenções/agenda da fonte.	
Assina abertamente o conteúdo?	Há evidências que confirmem o enunciado?
Há indicação de contato, credenciais?	O conteúdo é original?
A URL revela algo sobre a fonte? (por exemplo:.com; .edu; .gov; .org);	O conteúdo é embasado ou opinativo?
Já forneceu dados verídicos anteriormente?	O conteúdo foi confirmado por outras fontes? Há frações de conteúdo que se correlacionam com as de outros meios de coleta?
Em qual contexto emitiu o enunciado? Quando?	O conteúdo foi confirmando por fontes amigas, hostis ou independentes?
Informações involuntárias na mensagem (opiniões, registros...)	Conexões em redes sociais (contatos, análise de sentimentos)
A fonte é vulnerável a manipulações?	
O que a fonte esperava observar?	

Fonte: Dados compilados pela autora a partir de: DNAI (2016); DNISP (2009); LAHNEMAN (2010); IRWIN e MANDEL (2019).

A partir das respostas obtidas, formaliza-se, com recursos linguísticos, o estado de certeza do analista em relação ao dado ou fração de dado examinada, conforme o "estado da mente" visto anteriormente. A fonte seria considerada idônea, parcialmente idônea ou inidônea. O conteúdo seria confirmado por outras fontes, provavelmente verdadeiro, possivelmente verdadeiro, duvidoso ou improvável – os termos e a forma de expressão dependeriam da taxonomia empregada por cada órgão de Inteligência.

Após essas considerações, o profissional de Inteligência encontra-se apto a descartar o dado (ou sua fração) ou a utilizá-lo parcial ou integralmente nas demais etapas da MPC.

A qualidade dos dados utilizados impacta diretamente a qualidade do conhecimento de Inteligência e sua aceitação (utilização) ou não pelo usuário (tomador de decisão). Por um lado, faz-se necessário o uso da TAD, a fim de que o conhecimento não se contamine, não se torne impreciso ou de credibilidade duvidosa, nem seja processado erroneamente. Por outro lado, o valor desse conhecimento precisa atingir o usuário, que nele reconheceria pertinência, precisão, consistência, confiabilidade e atualidade – entre outras qualidades (LUZ, 2019, p. 31-33).

A TAD foi desenvolvida para avaliar fontes humanas e foi estendida para aplicação em dados obtidos por mediação tecnológica (LEMERCIER, 2014). Os aspectos de avaliação da fonte (autenticidade, confiança e competência) e do conteúdo (coerência, compatibilidade e semelhança) são bastante amplos e acolhem detalhes pertinentes a diferentes tipos de fontes, contudo demandam ser adaptados às diferentes características de fontes humanas e tecnológicas. A aplicação da TAD depende sobremaneira do profissional que a utiliza.

Em um primeiro momento, o profissional deve se inquirir se está lidando com a fonte produtora do dado (meio tecnológico ou fonte humana primária) ou seu canal (retransmissor), isto é, se o dado provém de indivíduo ou equipamento que efetivamente o produziu, ou se o dado foi retransmitido a partir de algum meio. Adiante, precisa considerar que os dados oriundos de meios tecnológicos (imagens, gravações de voz, vídeo e outras) devem ser checados quanto a inconsistências temporais, geográficas ou de metadados.

Ao avaliar fontes humanas, o profissional também deve lembrar que o ser humano possui desejo inerente de influenciar seu ouvinte de modo a lhe atrair a atenção ou obter alguma regalia; ou então se esquece de detalhes; possui antecedentes que o comprometem; confirma dados em que acredita. Assim, é bom considerar aspectos como a existência de vieses cognitivos, características psicológicas, objetividade do relato, proximidade do evento, restrições e motivações de todas as fontes envolvidas –

e mesmo do canal – durante a avaliação.

Muito interessante o exemplo de análise de fonte/conteúdo em relação ao *Twitter*, uma rede social caracterizada pela relativa anonimidade, concisão e agilidade, proposta por Pichon *et alii* (2014). Os autores levantam atributos diferenciados (multi critérios) que, quando usados de forma agregada, facilitam o julgamento de idoneidade de fonte, tais como: enriquecimento que o dado divulgado trouxe ao usuário; exame do nome de usuário e foto de perfil utilizados na conta; reputação perante outros usuários (obtida através de análise de conteúdo ou análise relacional); função agregadora exercida pela fonte (diversidade de fontes comprovadas que cita; explicação metodológica de como coletar os dados; centralidade e precedência ao divulgar os dados, entre outras); envolvimento pessoal da fonte na produção do dado, legitimidade (proximidade geográfica, testemunho); e riqueza de expressão.

Com frequência, quem atua em operações de Inteligência, ao mencionar "fonte", tem em mente o agente "recrutado", *i. e.*, colaborador externo que possui acessos no campo operacional, enquanto quem trabalha com análise de Inteligência associa o termo a "produtor" da mensagem ou mesmo OSINT. Essa polissemia é uma das anomalias com as quais os serviços de informação precisam lidar. Como evitá-la? Talvez, identificar o tipo de fonte na primeira vez em que for mencionada no documento, elucidar contextos, propiciar treinamento e reciclagem dos profissionais.

Não há parâmetros unificados para aplicação da TAD nos órgãos de Inteligência. O *"Admiralty Code"*, utilizado por países integrantes ou próximos da Organização do Tratado do Atlântico Norte (OTAN), apresenta gradação de critérios de avaliação, em que as letras de A até F representam a idoneidade da fonte, e os números de 1 a 6, a credibilidade do conteúdo do dado (IRWIN; MANDEL,2019, p. 2-3; HANSON, 2015). A Inteligência militar brasileira utiliza código semelhante, conforme apresentado no Quadro 2.

Quadro 2 - Avaliação do dado

JULGAMENTO DA FONTE	JULGAMENTO DO CONTEÚDO
A- Inteiramente idônea	1- Confirmado por outras fontes
B- Normalmente idônea	2- Provavelmente verdadeiro
C- Regularmente idônea	3- Possivelmente verdadeiro
D- Normalmente inidônea	4- Duvidoso
E- Inidônea	5- Improvável
F- A idoneidade não pode ser avaliada	6- A veracidade não pode ser avaliada

Fonte: BRASIL. [PCI]. (2019, p. 2-19).

Nublando a fonte

Apesar da aparente objetividade da TAD e de suas gradações, registram-se áreas nebulosas que não são atendidas pela técnica.

Primeiro ponto nebuloso: cada órgão de inteligência é autônomo em relação à taxonomia que emprega. Se uma agência estipular apenas três graus para avaliar a fonte (como inteiramente idônea, parcialmente idônea ou inidônea), surgiria lacuna de interpretação entre essa e a Inteligência militar (vide Quadro 2). Da mesma forma, grande detalhamento de opções não confere, necessariamente, maior precisão à avaliação, pois depende da subjetividade do avaliador em discernir o que seria fonte "normalmente idônea" daquela "regularmente idônea", por exemplo. E até que medida o usuário final estaria preparado para distinguir essas nuanças? (LUZ, 2019: 46-48)

Segundo ponto: há que se levantar a questão da interpretação dos dados advindos de diferentes meios ou órgãos parceiros (CAPET; REVAULT D'ALLONNES, 2014). Às vezes, dados coletados por drones, sensores ou parceiros contradizem informações recebidas de outras fontes, são desconexos ou difíceis de interpretar. Sob quais condições foram obtidas gravações? Essas condições influenciariam no estudo do dado pelo analista? Como interpretar a credibilidade de frações críveis, mas contraditórias? E se o profissional de Inteligência que gerenciar a fonte humana não for o mesmo que estiver processando o conhecimento[7]? Como esse último interpretaria os dados, ao considerar as peculiaridades individuais da fonte?

Outra questão seria que a confirmação de um dado por fontes "independentes" não se traduziria, necessariamente, em confirmação da credibilidade, uma vez que pode estar acontecendo redundância ou rumor (fenômeno de amplificação de notícias durante alguma operação de desinformação ou mesmo divulgação de dado proveniente de fonte única por parceiros diferentes). E se o dado que contraria todas as demais fontes se originasse de um informante? Qual seria o peso de uma e outra fonte frente à ambiguidade? Quem escolheria a fração a ser utilizada? A experiência (subjetividade) do analista?

Quarta área cinzenta: credenciar alguma fonte, a priori, como idônea. A idoneidade é característica mutável conforme contexto, acesso, capacidade e interesses (CAPET; REVAULT D'ALLONNES, 2014). Por exemplo, houve um ato terrorista. A fonte X trabalha em hospital, teria acesso ao local do ataque e estaria capacitada a repassar informações sobre quantas pessoas

7 Por questões de segurança, o ideal é que, ao lidarem com fontes humanas, os Serviços de Informação deleguem etapas diferentes de trabalho a pessoas diferentes – por exemplo, o profissional de Inteligência que estabelece o primeiro contato com eventual fonte não é o mesmo que a abordará depois, nem aquele que gerenciará (orientará e registrará) as atividades da fonte no transcorrer dos trabalhos (RONIN, 2002).

morreram ou se encontram feridas, mas não estaria qualificada a esclarecer que tipo de bomba foi utilizada, qual *modus operandi* dos agressores. A fonte X é idônea em relação a X', não a outros tipos de informação (BLOCK, 2021).

Quinta nebulosa: há considerável variação linguística entre indivíduos que utilizam diferentes termos lexicais para se referir ao mesmo grau de incerteza, ou então, fazem uso das mesmas expressões para se referir a graus de incerteza discrepantes (DHAMI, 2018, p. 2). Além disso, ao se considerar a existência de profissional de Inteligência gerenciador de fonte, seria importante oferecer relato cru do dado recebido para a análise? Há que se manter a coloquialidade, ou forjar a credibilidade do usuário final ao se identificar pontos sensíveis? (McLachlan *apud* BLOCK, 2021).

Uma última questão seria o uso seguro de "fontes abertas". Termo historicamente relacionado a documentos, artigos científicos, dados e estatísticas governamentais (UNITED STATES, 2012), OSINT encontra-se, atualmente, ligada a reportagens veiculadas pela mídia aberta, redes sociais e *big data*, e exige mediação de Inteligência Artificial, programas e aplicativos especiais para que sejam acessados em sua plenitude e com qualidade, conforme descrição de Williams e Blum (2018).

Sob a perspectiva da Contrainteligência, é preciso levar em consideração se a utilização dos referidos programas consistiria em vulnerabilidade para a produção do conhecimento. Os indivíduos que elaboraram tais programas são orgânicos? Se forem terceirizados, teriam acesso direto a fontes ou dados pesquisados durante a execução do trabalho? Como garantir o princípio de segurança?

Clareando a fonte

A Técnica de Avaliação de Dados, aparentemente, consegue se adaptar aos avanços tecnológicos, contudo ainda depende do profissional de Inteligência para aplicá-la a contento, e dirimir eventuais dúvidas sobre dados e suas fontes e evitar vieses cognitivos e erros.

A seguir, tecemos comentários que minimizam as seis nebulosas elencadas no tópico anterior, a saber: redundância de fonte; rotulação de fonte como idônea; diferenças em taxonomias, na interpretação de dados e na forma de expressão de profissionais de Inteligência; e, ainda, questões de segurança.

Quando um evento que comporta diversas perspectivas é descrito de forma similar por várias fontes, é prudente buscar checar se não se trata de versão originada em uma única fonte e difundida como se pertencesse a fontes distintas. Nesse caso, a validação do dado por fonte antagônica (por exemplo, a Arábia Saudita confirma informação da Síria) seria de maior utilidade (IRWIN; MANDEL, 2019).

Evitar rotular fonte, a priori, como idônea. Faz-se necessário considerar contexto, acessos e motivações da fonte caso a caso. Há que se checar cada fração de dado conforme a TAD e verificar se o novo dado se ajusta a outros conhecimentos, se trouxe consequências que podem ser checadas (CAPET; REVAULT D'ALLONNES, 2014).

A dificuldade de interpretação de dados oriundos de determinado meio tecnológico, de HUMINT, de diferentes taxonomias e de variações linguísticas pode ser minimizada com aproximação e diálogo entre o profissional de Inteligência que gerencia a fonte humana (ou que acessa diretamente o dado do meio tecnológico) e aquele que processa o conhecimento de Inteligência. Assim, pontos dúbios poderiam ser esclarecidos, e haveria verdadeiro trabalho de equipe entre pares.

A segurança no uso de programas e aplicativos terceirizados pode ser assegurada pela checagem deles por pessoal especializado interno ao serviço, ou com apoio de ferramentas especiais, como TOR[8], ou mesmo pela transferência de ferramentas que sejam vulneráveis para redes paralelas, as quais não permitam acesso a dados sensíveis do órgão.

Vimos que a aplicação da TAD depende do profissional de Inteligência. Machado (2018) sugere que a neutralidade na produção de conhecimento seja assegurada pela capacitação do analista em pensamento crítico, para que este entenda o modo pelo qual concatena ideias e raciocínios e melhore a percepção de si e do mundo, de forma a adaptar a mente mais rapidamente às transformações. Outras propostas levantadas pelo autor são melhoria do sistema de armazenamento e recuperação de dados, de forma a permitir reavaliação de dados e fontes com certo distanciamento histórico; e trabalho de equipes horizontais com verificação pelos próprios pares.

De nossa parte, sugerimos a criação de fóruns de discussões para pensar quais questionamentos (Quadro 1) atenderiam mais rapidamente o julgamento de cada tipo de fonte e conteúdo, para evitar dispersões e retrabalhos, em espécie de lista de checagem, como a preenchida por pilotos antes de cada voo. Vídeos e imagens poderiam ser conferidos pelo software X; gravações sonoras, pelo Y; a agência de Inteligência do país Z se interessa pela área de agronegócio e já atuou na área geográfica Z', buscando dados sobre Z", tendo como parceiros Z'"; e assim por diante.

Bastante atual a visão de Katz e Vardi (2008, p. 316-317) sobre a dinâmica do pensamento do profissional de Inteligência na avaliação de dados. Os autores sugerem a existência de dois mundos: o externo, composto de fatos e eventos; e o interno, um mundo em que o profissional de

8 TOR *(The Onion Router ou roteador cebola)* é *software* livre e de código aberto que protege identidade e privacidade do usuário (BARBOSA, 2020).

Inteligência explica, percebe, interpreta e hierarquiza possíveis cenários do mundo externo. Somente ao criar modelos mentais, o profissional consegue avaliar e comparar o mundo real com o dos diferentes cenários e distingue o melhor caminho a seguir. Não obstante, esses modelos podem ser afetados por distorções, denominadas vieses cognitivos, e as mais recorrentes na Inteligência são: ambiguidades (variedade de opções e variantes que se sobrepõem e dificultam a tomada de decisão); parâmetros de validade (emprego de valores subjetivos, experiências pessoais, incertezas e pressuposições como parâmetros, os quais são difíceis de justificar e validar, e que exigem abordagem crítica para serem evitados); conhecimento tácito (as avaliações dos tomadores de decisão e dos avaliadores dos dados podem ser influenciadas por opções coletivas pré-definidas, as quais, muitas vezes, distorcem os dados); avaliação contextual (um mesmo dado é percebido de forma diferente conforme experiências anteriores do avaliador, o que gera diferentes percepções do contexto); e modelos de referência (parâmetros de coleta de dados desconhecidos e mesclados, oriundos de diferentes organizações ou adaptados diretamente da intuição do tomador de decisão). Assim, cada fração de dado analisado estaria sob potencial influência dessas fontes de ruído ou distorção.

Para Katz e Vardi (2008), apesar do processo de distorção, é possível identificar "estrutura constante", a "verdade", através de peças relevantes dissolvidas nos dados distorcidos. Os especialistas sugerem que o analista examine "sintomas" e "sinais" e que usem o conhecimento próprio para diagnosticar se o evento está ou não acontecendo, se é ou não verdadeiro[9]. Se não for possível chegar a resultado imediato, alternar o modo de pensar (dedutivo ou analítico), refazer diagnóstico - aqui, a importância do distanciamento histórico mencionado por Machado (2018) -, reanalisar criticamente o caminho percorrido até o momento e fazer correções. Doronin (2016, p. 65) lembra que, na prática, há casos em que a informação confiável se oriunda de fonte não-confiável e vice-versa. A sobreposição de dados obtidos de diferentes fontes acerca de um mesmo contexto, ou, então, a checagem, junto a cada fonte, de como ela obteve o dado, podem auxiliar o profissional a apreender a verdade.

Considerações finais

Ainda existem necessidades práticas e teóricas relacionadas à TAD que precisam ser atendidas? Sim. Sempre há espaço para se desenvolver estudos sobre

9 Nosso exemplo de "sintomas" e "sinais": meio de comunicação "não-confiável" afirma que golpe de Estado no país X, promovido com auxílio de países considerados "aliados" de X, foi evitado com auxílio do país Y (um inimigo), que preveniu X. Alguns países "aliados" negam o evento, outros não comentam, mas série de sinais podem ser identificados: fuga de grupo de indivíduos do país X para os países "aliados", estremecimento de relações entre X e seus aliados, aproximação de X com Y, alterações em relações comerciais. A verdade pode ser vislumbrada pelos eventos, independentemente de rótulos e afirmativas.

avaliação de capacidade e motivação de fonte, abordagem, gerenciamento de fontes (BURKETT, 2013; DORONIN, 2009). Nesse processo, os profissionais de Inteligência devem ser protagonistas, buscar e propor soluções que atendam às necessidades que surgem, uma vez que fazem parte tanto do problema, como de sua solução.

O primeiro passo para a melhoria da qualidade do produto da Inteligência inicia-se com a capacitação do profissional de Inteligência, com provimento de ferramentas computacionais, oferta de cursos e seminários a todos, para que compreendam e empreguem, efetivamente, as técnicas necessárias à produção do conhecimento. Após isso, precisam ser conduzidas discussões na comunidade de Inteligência, para que se pense o futuro e as ferramentas que queremos para a Inteligência brasileira.

Referências

BARBOSA, Daniel C. *O que é o TOR e para que serve?* 30 dez. 2020. Disponível em: https://www.welivesecurity.com . Acesso em: 18 abr. 2023.

BLOCK, Ludo (2021). *The origin of information grading systems*. 20 jan. 2021. Disponível em: https://www.blockint.nl/methods/the-origin-of-information-gradin-systems/. Acesso em: 18 abr. 2023.

BRASIL. Ministério da Defesa. Exército Brasileiro. *Produção do Conhecimento de Inteligência* [PCI]. Brasília: Comando de Operações Terrestres, 2019. Disponível em: https://bdex.eb.mil.br/jspui/handle/123456789/3270. Acesso em: 18 abr. 2023.

Ministério da Defesa. Exército Brasileiro. *Produção do Conhecimento de Inteligência* [PCI]. Brasília: Comando de Operações Terrestres, 2019. Disponível em: https://bdex.eb.mil.br/jspui/handle/123456789/3270. Acesso em: 18 abr. 2023.

BRASIL. Decreto nº 8793, de 29 de junho de 2016. *Fixa a Política Nacional de Inteligência*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm. Acesso em: 18 abr. 2023.

BRASIL. Gabinete de Segurança Institucional. Agência Brasileira de Inteligência. *Doutrina Nacional da Atividade de Inteligência [DNAI]*: fundamentos doutrinários. Brasília: Abin, 2016.

BRASIL. Ministério da Defesa. Exército Brasileiro. *Inteligência militar terrestre* [IMT]: manual de fundamentos. 2. ed. Brasília: Estado Maior do Exército, 2015. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/95/1/EB-20-MF-10.107.pdf. Acesso em: 18 abr. 2023.

BRASIL. Ministério da Justiça. Secretaria Nacional de Segurança Pública. *Doutrina Nacional de Inteligência de Segurança Pública* [DNISP]. Brasília, 2009. Disponível em: https://dspace.mj.gov.br. Acesso em: 18 abr. 2023.

BURKETT, Randy. An alternative framework for agent recruitment: from MICE to RASCLS. *Studies in Intelligence*, v. 57, n. 1, p. 7-17, Mar. 2013.

CAPET; REVAULT D'ALLONNES. Information evaluation in the military domais: doctrines, practices and shortcomings. *In:* CAPET, P; DELAVALLADE, T. (Eds.) *Information Evaluation.* London: ISTE Ltd., 2014. p. 103-127.

CEPIC, Marco. *Espionagem e democracia*. Rio de Janeiro: Editora FGV, 2003.

DORONIN, Aleksandr Ivanovich. *Biznes-razvedka* [em russo: *Espionagem industrial*]. 5. ed. Moscou: Osi-89, 2009. Disponível em: https://studfile.net/preview/5288609/page:14/. Acesso em: 18 abr. 2023.

DHAMI, M. Towards an evidence-based approach to communicating uncertainty in intelligence analysis. *Intelligence and National Security*, 30 Oct. 2018. Disponível em: http://dx.doi.org/10.1080/02684527.2017.1394252. Acesso em: 18 abr. 2023.

HANSON, J. The admiralty code: a cognitive tool for self-directed learning. *International Journal of Learning, Teaching and Educational Research*, v. 14, n. 1, p. 97-115, nov. 2015. Disponível em: https://www.ijlter.org/index.php/ijlter/article/download/494/234. Acesso em: 18 abr. 2023.

IRWIN, D.; MANDEL, D. *Improving information evaluation for intelligence production. Intelligence and National Security*. 6 feb. 2019. DOI: 10.1080/02684527.2019.1569343. Acesso em: 18 abr. 2023.

KAMINSKI, M.A. Intelligence Sources in the Process of colletion of information by the U.S. Intelligence Community. *Security Dimensions*, n. 32, p. 82-105, 2019. Disponível em: https://www.researchgate.net/publication/340647256. Acesso em: 18 abr. 2023.

KATZ, Y; VARDI, Y. Strategies for data gathering and evaluation in the intelligence community (1991). *International Journal of Intelligence and Counterintelligence,* v. 5, n. 3, p. 313-328, 2008. Disponível em: https://doi.org/10.1080/08850609108435185. Acesso em: 18 abr. 2023.

LAHNEMAN, W. The need for a new intelligence paradigma. *International Journal of Intelligence and Counterintelligence*, v. 23, n. 2, p. 201-225. Disponível em: https://doi.org/10.1080/08850600903565589. Acesso em: 18 abr. 2023.

LEMERCIER, Philippe. The fundamentals of intelligence. *In:* CAPET, P; DELAVALLADE, T. (Eds.) *Information Evaluation*. London: ISTE Ltd., 2014. p. 55-102.

LUZ, Alessandro R. *O emprego da Técnica de Avaliação de dados (TAD) na Produção do Conhecimento de Inteligência*. 2019. 72 p. Trabalho de Conclusão de Curso (TCC de Graduação e Especialização em Especialização em Inteligência de Segurança) - UNISUL, Palhoça. Disponível em https://repositorio.animaeducacao.com.br/handle/

ANIMA/12002. Acesso em: 18 abr. 2023.

MACHADO, André M. Gestão do processo de produção de conhecimentos: o impacto de vieses cognitivos sobre a imparcialidade do conteúdo de inteligência. *Revista Brasileira de Inteligência*, Brasília: Agência Brasileira de Inteligência, n. 13, p. 9-24, 2018.

PICHON, Frédéric *et alii*. Multidimensional approach to reliability evalution of information sources. CAPET, P; DELAVALLADE, T. (Eds.) *Information Evaluation*. London: ISTE Ltd., 2014. p. 129-159.

RONIN, Ronan. *Svoia razvedka*. [Em russo: *Nossa espionagem*]. [s.l.]: Ozonio, 2002. Disponível em: https://altairbook.com/books/4735699-svoya-razvedka.html. Acesso em: 18 abr. 2023.

ROSE, Robert N. *Restructuring the U.S. Intelligence Community*. The George Washington University: Center for Cyber and Homeland Security, 2017. Disponível em: https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/Rose-DNIPaper-2017.pdf. Acesso em: 2 set. 2022.

WILLIAMS, H; BLUM, I. *Defining second generation open source intelligence (OSINT) for the defense enterprise*. Santa Monica: RAND Corporation, 2018. Disponível em: https://apps.dtic.mil/sti/pdfs/AD1053555.pdf. Acesso em: 18 abr. 2023.

UNITED STATES. Department of the Army. *Open-Source Intelligence:* Producing OSINT. July 2012. Disponível em: https://irp.fas.org/doddir/army/atp2-22-9.pdf. Acesso em: 18 abr. 2023.

Artigo

9

UMA VISÃO CRÍTICA SOBRE A AUSÊNCIA DE PROTOCOLO GERAL DE INTEGRAÇÃO DE AGÊNCIAS NA INTELIGÊNCIA EM SEGURANÇA PÚBLICA

DOI: https://doi.org/10.58960/rbi.2023.18.228

Marcos Paulo Hiath da Silva *
Almir de Oliveira Júnior **
Anna Carolina Mendonça Lemos Ribeiro ***

Resumo

As políticas e os programas de segurança pública requerem aprimoramento constante das agências de Estado responsáveis pela execução de ações tanto preventivas quanto repressivas nessa área. Há um conjunto crescente e dinâmico de atividades criminosas que requerem, como resposta, um serviço especializado de identificação, coleta, análise e disseminação de informações que orientem decisões e intervenções efetivas dos órgãos de segurança. A Inteligência de segurança pública possui um papel crucial nesse sentido, e vários órgãos estão integrados por meio do Subsistema de Inteligência de Segurança Pública (Sisp), regulamentado pelo Decreto no 3.695/2000. Os objetivos envolvem identificar e avaliar ameaças e produzir informações e conhecimentos para subsidiarem medidas que neutralizem e reprimam atos criminosos. Para isso, órgãos de Inteligência ou dotados de setor de Inteligência, p. ex., a Agência Brasileira de Inteligência, a Polícia Federal, a Polícia Rodoviária Federal, o Conselho de Controle de Atividades Financeiras, a Receita Federal, o Ministério da Defesa, a Secretaria Nacional de Segurança Pública e as polícias militares e civis dos estados (estas de forma conveniada) devem, nas respectivas competências, somar esforços para a implementação e o aprimoramento da Inteligência de segurança pública no país. No entanto, a ausência de um referencial específico, apto a direcionar gestores e operadores da atividade de Inteligência à consecução dos objetivos pretendidos com a atuação dos órgãos, representa importante fator desfavorável à efetividade das ações no âmbito do Sisp.

Palavras-chave: Inteligência; agências de Inteligência; integração; segurança pública; protocolos.

A CRITICAL VIEW OVER THE ABSENCE OF A GENERAL PROTOCOL FOR THE INTEGRATION OF AGENCIES IN PUBLIC SECURITY INTELLIGENCE

Abstract

Public security policies and programs require constant improvement by the State agencies responsible for carrying out preventive and repressive actions in this area. There is a growing and dynamic set of criminal activities that require, as a response, a specialized service for identifying, collecting, analyzing

* Especialista em Gestão Integrada de Inteligência pela Agência Brasileira de Inteligência (Abin) e em Altos Estudos em Defesa pela Escola Superior de Defesa (ESD). Mestrando em Políticas Públicas e Desenvolvimento no Instituto de Pesquisa Econômica Aplicada (IPEA). Policial Rodoviário Federal.

** Doutor em Sociologia e Política pela Universidade Federal de Minas Gerais (UFMG). Pesquisador do Instituto de Pesquisa Econômica Aplicada (IPEA).

*** Doutora em Administração pela Universidade de Brasília (UnB). Técnica em desenvolvimento e administração do Instituto de Pesquisa Econômica Aplicada (IPEA).

and disseminating information that guides decisions and effective interventions by security agencies. Public security intelligence plays a crucial role in this regard, and several organizations have been integrated through the Public Security Intelligence Subsystem - SISP, regulated by Decree 3695/2000. The objectives involve identifying and assessing threats and producing information and knowledge to support measures that neutralize and repress criminal acts. For this, intelligence agencies, such as the Brazilian Intelligence Agency, the Federal Police, the Federal Highway Police, the Financial Activities Control Council, the Federal Revenue Service, the Ministry of Defense, the National Secretariat for Public Security, and the military and civil polices from the states (these in an agreed manner) must, respecting the respective competences of each member of the system, join forces for the implementation and improvement of public security intelligence in the country. However, the absence of a specific protocol for directing managers and operators of the intelligence activity to achieve the intended objectives represents an important unfavorable factor to the effectiveness of the actions within the scope of the SISP.

Keywords: *Intelligence; Intelligence agencies; integration; public security; protocols.*

UNA VISIÓN CRÍTICA SOBRE LA AUSENCIA DE UN PROTOCOLO GENERAL PARA LA INTEGRACIÓN DE AGENCIAS EN INTELIGENCIA DE SEGURIDAD PÚBLICA

Resumen

Las políticas y programas de seguridad pública requieren una mejora constante por parte de los organismos del Estado encargados de llevar a cabo acciones preventivas y represivas en esta materia. Existe un conjunto creciente y dinámico de actividades delictivas que requieren como respuesta un servicio especializado de identificación, recolección, análisis y difusión de información que oriente decisiones e intervenciones efectivas por parte de los organismos de seguridad. La inteligencia de seguridad pública juega un papel crucial en este sentido, y varios organismos se han integrado a través del Subsistema de Inteligencia de Seguridad Pública - SISP, reglamentado por el Decreto 3695/2000. Los objetivos implican identificar y evaluar amenazas y producir información y conocimiento para apoyar medidas que neutralicen y repriman actos delictivos. Para ello, organismos de inteligencia, como la Agencia Brasileña de Inteligencia, la Policía Federal, la Policía Federal de Carreteras, el Consejo de Control de Actividades Financieras, el Servicio de Ingresos Federales, el Ministerio de Defensa, la Secretaría Nacional de Seguridad Pública y las policías militares y civiles de los estados (estos de manera consensuada) deben, respetando las respectivas competencias de cada miembro del sistema, aunar esfuerzos para la implementación y el perfeccionamiento de la inteligencia de seguridad pública en el país. Sin embargo, la ausencia de un protocolo específico para orientar a los administradores y operadores de la actividad de inteligencia para el logro de los objetivos previstos representa un importante factor desfavorable a la efectividad de las acciones en el ámbito del SISP.

Palabras clave: *Inteligencia; agencias de Inteligencia; integración; seguridad pública; protocolos.*

Introdução

Em sua formulação já clássica e amplamente difundida, Sherman Kent (1949) descreve a Inteligência a partir de seu triplo significado: é considerada como uma atividade (o processo de produção de Inteligência), também como o produto dessa atividade (a informação que já foi analisada para assessorar o processo de decisão) e, ainda, como a unidade organizada para realizar essa mesma atividade, onde o pessoal especializado atua.

O principal objetivo da Inteligência é auxiliar o processo decisório ao antecipar os movimentos de atores do macroambiente e no ambiente organizacional e, assim, evitar que os decisores sejam surpreendidos, especialmente por atores-chave (MARCIAL, 2011). Portanto, é atribuição da atividade de Inteligência oferecer o necessário respaldo informacional para se implementar ações que correspondam aos anseios da sociedade (FERNANDES, 2012). Está ligada, portanto, à ação eficiente, isto é, à tomada da melhor decisão para otimizar recursos (RIBEIRO; SANTOS, 2020).

O processo de Inteligência é formado por um ciclo que envolve essencialmente as fases de planejamento, coleta, análise e difusão das informações (BATTAGLIA, 1999; CAPUANO *et alii*, 2009; KAHANER, 1996). O planejamento consiste em estabelecer as necessidades de Inteligência e definir os recursos necessários para os objetivos propostos. É importante observar que, nessa fase, define-se a finalidade dos resultados a serem alcançados, ou seja, qual uso será feito das informações produzidas. Na etapa da coleta, estabelece-se a seleção das fontes de informação e a organização do material a ser analisado. Já a análise corresponde ao estudo minucioso dos dados coletados, com o exame sistemático de dados e conhecimentos relevantes de modo a transformar os fragmentos de informação em conhecimento acionável. Fragmentos de informação que não podem ser utilizados de forma decisiva para guiar a ação, que não passaram por esse tratamento e ainda não são úteis, não são, pelo menos ainda, o produto final da Inteligência. Só depois da significação da informação, portanto, é que se fecha o ciclo, com a difusão do conhecimento construído, que deve chegar aos decisores legitimamente instituídos de forma oportuna, em tempo hábil para resolução mais adequada diante de determinada situação, adversidade ou crise que esteja sendo enfrentada.

Esse ciclo é básico do processo de Inteligência e pode ser aplicado em qualquer subcategoria da Inteligência, cuja diferenciação se encontra em seu foco de atuação. A Inteligência Militar, por exemplo, trata dos assuntos próprios da dinâmica militar e do fenômeno bélico. Deu origem a todas as outras e é chamada de "mãe" dos serviços de Inteligência (GUEDES, 2006). Já a Inteligência de

Estado almeja produzir conhecimentos para o assessoramento na formulação de políticas adequadas em vários campos da atuação governamental (FERNANDES, 2012). Refere-se à capacidade de coleta, análise e utilização tempestiva de informações estratégicas, acumulada pelos órgãos públicos sobre assuntos de relevância estratégica em suas respectivas esferas legítimas de atuação. A atividade de Inteligência de segurança pública, por sua vez, é erigida no enfrentamento às ameaças de corrupção, ao crime organizado, aos ilícitos transnacionais e ao terrorismo.

A Inteligência de segurança pública é um componente significativo de poder e recurso de ação dos órgãos envolvidos na detecção e na prevenção de delitos, imprescindível ao aparato de controle de ameaças internas, ao Estado e aos cidadãos. De acordo com a Estratégia Nacional de Inteligência (Enint), aprovada no Decreto no 8.793, de 15 de dezembro de 2017, a Inteligência de segurança pública representa uma subcategoria da Inteligência de Estado e desempenha um importante papel no assessoramento dos gestores públicos com vistas à elaboração de políticas públicas voltadas à prevenção e à neutralização de ações criminosas de grupos organizados.

Há princípios legais e normativos que precisam orientar a implementação dos procedimentos em todos os setores em que agentes públicos atuam na busca de cumprimento de sua missão. Isso é válido no contexto de atividades de Inteligência típicas de Estado, em qualquer área de políticas públicas em que venham a ser aplicadas (saúde, educação, defesa nacional, segurança pública, etc.). Mesmo que alguns setores pareçam ser mais abertos ao debate e à participação social, enquanto outros pareçam tratar de assuntos mais técnicos e, portanto, no domínio fechado de um determinado conjunto de "especialistas", as mesmas diretrizes associadas a transparência, eficiência e efetividade devem guiar as iniciativas no âmbito da ação governamental.

O caráter sigiloso das informações e dos conhecimentos utilizados pelos agentes que lidam com Inteligência de Estado não pode ser justificativa para uma discricionariedade radical, capaz de anular a possibilidade de qualquer tipo de *accountability* ou prestação de contas. Pelo contrário, não há campo de atuação do Estado em que o desempenho de suas instituições não deva ser escrutinado, de modo a alargar o entendimento a respeito do funcionamento das burocracias profissionais e sua capacidade de promover, de forma democrática, condições favoráveis à superação das condições que sejam adversas ao desenvolvimento do país em sua acepção mais ampla; ou seja, que englobe garantia de direitos individuais e a promoção da justiça entre os cidadãos. Isso se aplica às organizações públicas em geral, sem exceção àquelas que se dedicam à atividade de Inteligência levada a cabo em qualquer esfera do Estado.

Ao contrário do que muitas vezes se pensa no senso comum, as atividades de Inteligência não se confundem com a espionagem. No contexto anárquico dos antagonismos e disputas entre as nações, a espionagem emerge como ferramenta para obtenção de informações sensíveis, muitas vezes segredos de Estado, para minimizar ameaças ou obstáculos estrangeiros frente aos interesses do país. Para isso, a espionagem lança mão de vários meios, até mesmo na clandestinidade, que poderiam ser classificados como ilícitos ao colher informações de maneira clandestina (CONDEIXA, 2015). O mesmo se aplica à espionagem industrial, em que ocorre a ação para se obter informações privilegiadas de concorrentes para auferir vantagens comerciais de forma antiética ou mesmo criminosa (CRANE, 2005). Já a Inteligência, entendida como atividade de Estado promovida por órgãos públicos, deve trabalhar com as restrições constitucionais relativas a coleta, armazenamento de dados e uso da informação.

A Inteligência trabalha com fontes abertas e também, em larga medida, com informação classificada, de acesso restrito. Ainda assim, toda essa informação deve ser vista como um ativo de valor coletivo, a ser utilizado estritamente dentro de um mandato legal. Segundo Brandão (2013), a atividade de Inteligência no Brasil deve se ajustar às normas constitucionais e legais, que são claras, específicas e capazes de suprimir seu alto grau de discricionariedade como meio de ação. No entanto, não há um arcabouço que oriente, de forma sistemática e prática, a execução das atividades de Inteligência de forma integrada entre diferentes instituições.

O Brasil, ao acompanhar o exemplo da comunidade internacional de Inteligência, tem realizado a atualização do sistema de Inteligência e do arcabouço legislativo que envolve a matéria, e tem promovido profundas transformações estruturais, com os objetivos de integrar as estruturas, modernizar o aparelho estatal e dar efetividade às políticas públicas. Porém, apesar da constante evolução legislativa da área, ainda existem lacunas acerca da integração das ações das agências de Inteligência, a qual pressupõe certo grau de cooperação entre os órgãos, o que não é um processo espontâneo.

Órgãos de Inteligência ou dotados de setor de Inteligência, p. ex., a Agência Brasileira de Inteligência (Abin), a Polícia Federal (PF), a Polícia Rodoviária Federal (PRF), o Conselho de Controle de Atividades Financeiras (Coaf), a Receita Federal, o Ministério da Defesa, a Secretaria Nacional de Segurança Pública (Senasp) e as polícias militares e civis dos estados, trabalham em suas próprias culturas organizacionais e constroem seu capital de informação estratégica a partir de *modus operandi* próprios, mas não-integrados.

Não é por acaso que a Estratégia Nacional de Inteligência de Segurança Pública (Enisp),

aprovada no Decreto nº 10.778/2021, tem como um de seus objetivos estratégicos a criação de protocolos específicos para atuação integrada no âmbito do Subsistema de Inteligência de Segurança Pública (Sisp), que participa do Sistema Brasileiro de Inteligência (Sisbin). Entretanto, esses protocolos não foram devidamente regulamentados, o que dificulta o processo integrativo entre as agências de Inteligência. Diante da típica complexidade das Atividades de Inteligência de segurança pública, faz-se necessária a elaboração desses protocolos para a neutralização de ações e ameaças adversas à segurança pública. Isso posto, este artigo visa a apresentar uma contribuição teórica sobre a importância dos protocolos de ação integrada, especialmente na segurança pública.

A importância dos protocolos

O termo protocolo pode ser entendido, de maneira concisa, como um conjunto de normas ou regras voltadas à padronização das atividades desenvolvidas pelo órgão estatal. A necessidade de padronizar determinadas atividades decorre, principalmente, da busca pela boa administração – ou seja, auferir os melhores resultados ao otimizar os recursos públicos disponíveis, evitar desperdícios, garantir uma maior rentabilidade social – e, ainda, da necessidade de definição de marcos regulatórios de atuação que impeçam o transbordamento de competências.

O estabelecimento de um modelo protocolar de atuação integrada visa a implementar um referencial específico para as ações integradas no âmbito da Atividade de Inteligência. Dessa forma, a padronização dedica-se a disciplinar, naquilo que lhe couber, as minúcias que permeiam o processo de integração, para garantir aos gestores e operadores a segurança jurídica no desempenho de sua função. Na estruturação de um protocolo, alguns aspectos devem ser observados, tais como: finalidade, público-alvo, linhas de cuidado prioritárias, evidências científicas e princípios éticos e legais.

O uso de protocolos apresenta várias vantagens, como a promoção de maior segurança aos usuários e profissionais, estabelecimento de limites de ação e cooperação entre os envolvidos, redução da variabilidade do cuidado, norteamento ao profissional para a tomada de decisão em relação às condutas, incorporação de novas tecnologias, respaldo legal das ações, maior transparência e controle dos custos, entre outras (PIMENTA, 2015).

Na área médica, por exemplo, o estabelecimento de protocolos com vistas a disciplinar uma atuação específica já está consolidado. Pode-se destacar o Protocolo de Manchester, que consiste em um conjunto de regras norteadoras da atividade dos agentes de saúde para a triagem de pacientes. Assim que chega à unidade

hospitalar, o paciente é enviado para a triagem, onde o agente de saúde, após entrevista e exame preliminar, correlaciona a gravidade do estado geral do paciente a cores. Esse protocolo impõe a padronização no atendimento das emergências ao estabelecer a prioridade de atendimento de acordo com a indicação clínica, para minimizar os problemas encontrados, com base em critérios de gravidade sistemáticos (TEIXEIRA; OSELAME; NEVES, 2014).

A implementação de protocolos de atuação, de um modo geral, tende a contribuir para que os objetivos da boa administração dos recursos públicos sejam atingidos e proporcionem melhores serviços à sociedade. Na área de Inteligência, a criação e a implementação de um protocolo apto a nortear a atuação integrada entre agências teria o condão de organizar e padronizar o exercício da Atividade de Inteligência em um contexto específico. Seria um instrumento destinado a direcionar a estruturação e o desenvolvimento da atuação integrada pelos órgãos, disciplinar, na medida em que lhe cabe, questões legais e administrativas, e reduzir as incertezas e tensões entre os envolvidos, principalmente quanto à falta de consenso decisório, definição de matriz de responsabilidade e disponibilização de recursos.

Dessa forma, em linhas gerais, as principais vantagens trazidas pelo estabelecimento de um protocolo de atuação integrada na área de Inteligência seriam a uniformização dos processos que envolvem ações integradas, a dinamização na prestação de serviços públicos de qualidade aos cidadãos e segurança jurídica aos gestores e operadores de Inteligência.

Por um protocolo de atuação integrada na área de segurança pública

A segurança pública é um direito ligado à distribuição da justiça como um bem coletivo e individual, que envolve a resolução de uma série de problemas e situações que vão além do campo de ação das agências estatais que atuam diretamente com a criminalidade e a violência. Há um grande conjunto de questões associadas ao desenvolvimento econômico, à desigualdade social, à oferta de emprego e educação, além de uma amplitude de fatores que incidem sobre comportamentos de indivíduos que decidem se engajar em uma carreira de delitos e atividades perniciosas ao tecido social.

Uma questão é que criminalidade, que ganha espaço devido à ineficiência nas atividades de segurança pública, gera uma série de externalidades negativas para a sociedade, tais como a redução da produção econômica, aumento dos custos com saúde pública e previdência, além de uma menor atratividade para investimentos estrangeiros e turismo. A criminalidade e a violência têm o condão de atingir diretamente a vida das pessoas, gerar medo, aumentar a

percepção de insegurança e limitar o direito de ir e vir.

As políticas de segurança pública visam, justamente, minimizar esses efeitos negativos e promover um ambiente mais seguro, o que precisa se dar por meio da adoção de medidas preventivas e repressivas, como policiamento ostensivo, investigação e utilização de técnicas especializadas de Inteligência. São necessárias, então, políticas públicas voltadas à área de Inteligência de segurança pública, com o objetivo de contribuir para a redução da criminalidade e da violência, o aumento da confiança da população, a melhoria da qualidade de vida e a atração de investimentos e turismo, o que promove um ambiente propício para o crescimento econômico e a prosperidade social.

Em virtude do constante desenvolvimento das sociedades atrelado às profundas alterações nas dinâmicas da Atividade de Inteligência, observadas recentemente a partir do acelerado processo da globalização e, notadamente, dos atentados ocorridos em 11 de setembro de 2001, nos EUA, várias nações soberanas promoveram a reorganização de seus sistemas de Inteligência para fomentar maior cooperação e integração.

A integração das agências de Inteligência é, portanto, uma necessidade premente para o enfrentamento da escalada do crime organizado e para a garantia da segurança da sociedade. Diante dessa demanda, foram desenvolvidas a Política Nacional de Inteligência (PNI, Decreto nº 8.793/2016), a Enint e demais documentos que delas derivam ou nelas têm fundamento com os objetivos primários de regulamentar a Atividade de Inteligência e promover a integração das agências de Inteligência.

Assim, a ausência desses protocolos pôde ser constatada principalmente nos últimos anos, pois o Brasil sediou uma série de eventos internacionais, que demandaram muitos esforços da comunidade de Inteligência no assessoramento do tomador de decisão e nas demandas operacionais. Embora, a depender do evento, tenha-se conferido a "gestão" ou o "comando" das ações a determinado órgão, não há como realizar todas as atividades que permeiam o espectro de atuação da Inteligência sem a reunião de diversos órgãos, devido à escassez de recursos humanos qualificados, à ausência de uniformização do conhecimento e de capacidades técnicas específicas.

Importa destacar que o princípio da compartimentação é uma das principais ferramentas utilizadas pela segurança pública para proteger informações sensíveis e evitar vazamentos. Esse princípio preconiza que as informações devem ser compartimentadas e distribuídas apenas para aqueles que possuem a necessidade e a autorização para acessá-las. No entanto, o secretismo excessivo na Inteligência de segurança pública pode ter consequências

negativas e causar, em caso extremo, abuso de poder e violação dos direitos humanos. Em muitos casos, a compartimentação pode gerar uma cultura de extremo sigilo e falta de transparência, o que pode levar a abusos e erros.

Um dos principais problemas de compartimentação excessiva é que ela pode dificultar a troca de informações entre as agências de segurança pública. Sem um compartilhamento adequado de informações, as agências podem trabalhar de forma mecanizada, sem uma visão completa do quadro geral da segurança pública, o que pode gerar falhas na prevenção e na resposta às ameaças.

Segundo Muniz (2018), a produção de protocolos entre agências é necessária para articulação, subordinação, complementaridade, coordenação, suplementação de recursos e produção de cadeia de comando de controle. Ou seja, protocolo entre agências, nas palavras do autor, permite que a Marinha, a Aeronáutica e o Exército atuem em conjunto com as polícias militar, federal e civil, o Corpo de Bombeiros, a Guarda Municipal, o Ministério Público e o sistema de justiça.

É preciso, portanto, repensar a abordagem utilizada na formulação de uma política de integração das agências de Inteligência, a fim de promover autêntica legitimação frente à sociedade civil e implementação adequada das medidas adotadas. Somente assim será possível o sucesso das políticas públicas no combate ao crime organizado e na promoção da segurança da sociedade. A implementação efetiva dessa política é essencial para alcançar os objetivos traçados na Enint, e que as informações coletadas sejam compartilhadas e utilizadas de forma estratégica para combater o crime organizado e melhorar a segurança da sociedade.

No entanto, a implementação dessa política pode encontrar diversos obstáculos. Um deles é a falta de recursos financeiros e materiais. A integração das agências de Inteligência exige a aquisição de tecnologias avançadas, bem como a capacitação e o treinamento dos agentes envolvidos. Sem recursos adequados, a implementação da política pública pode ser prejudicada e comprometer a evolução do trabalho das agências de Inteligência.

Frisa-se que política de Inteligência é política pública, portanto sujeita aos controles previstos legalmente, como ocorre no ciclo de políticas de qualquer outro setor. Precisa de orçamento, de algum tipo de programa de monitoramento e prestação de contas. A forma de atuação dos órgãos e seus procedimentos devem ser discutidos e alvos de elaboração política transparente. Só isso justifica e aprimora o dispêndio dos recursos públicos envolvidos, que merecem o maior nível possível de *accountability*.

Outro obstáculo é a resistência de algumas agências em compartilhar informações.

A cultura de compartimentalização na Inteligência de segurança pública pode ser o motivo de algumas agências resistirem ao compartilhamento de informações com outras, mesmo que essas informações sejam cruciais para a tomada de decisões estratégicas. Além disso, a falta de confiança entre as agências pode ser um obstáculo adicional para a implementação da política pública de integração.

É importante mencionar que a capacitação dos agentes envolvidos é um fator crítico de sucesso para que isso ocorra. É necessário que esses profissionais possuam conhecimentos técnicos avançados e estejam acostumados com as melhores práticas de Inteligência. A falta de capacitação pode prejudicar a qualidade das informações coletadas e comprometer a compreensão das ações estratégicas integradas.

Por fim, é essencial que haja uma estruturação clara do fluxo de informações e decisões entre as agências envolvidas na política pública de integração. É necessário que sejam definidos protocolos claros de comunicação e compartilhamento de informações, de modo a garantir a transparência e o acompanhamento das ações aprendidas. Portanto, é fundamental que sejam adotadas medidas para superar esses desafios e estimular que as informações coletadas sejam utilizadas de forma estratégica para segurança da sociedade.

Percepção dos ativos de Inteligência em relação à criação de protocolo de atuação integrada dos órgãos do Sisbin e do Sisp

A ausência de diretriz única e específica para nortear as atividades dos gestores e operadores de Inteligência, em um contexto de atuação integrada entre agências, dificulta a integração no âmbito da Inteligência, já que, sem o devido direcionamento, diversos fatores, principalmente aqueles relacionados à diversidade de órgãos e consequentes atribuições institucionais, podem impactar negativamente o desenvolvimento das ações.

Para entender melhor essa problemática, foi feito um levantamento de percepção com ativos de Inteligência, gestores e operadores, quanto à necessidade de elemento normativo apto a nortear suas ações em um contexto de atuação integrada entre agências de Inteligência dos órgãos integrantes do Sisp, que faz parte do – Sisbin, instituído pela Lei nº 9.883, de 7 de dezembro 1999, com o objetivo de integrar as ações de planejamento e execução das Atividades de Inteligência do Brasil.

O levantamento, que não conta com uma amostra representativa, foi realizado no ano de 2021 e consistiu no envio de questionários eletrônicos ao público de interesse desse estudo. Isto é, os

formulários foram direcionados aos gestores e operadores de órgãos integrantes do Sisbin e do Sisp atuantes em todo o território nacional, que receberam um *link* por *e-mail* para responder os itens que serão apresentados adiante. O processo se deu por meio de um formulário no *Google Forms*. Este foi distribuído individualmente aos integrantes da Atividade de Inteligência e aos responsáveis regionais e nacionais de agências de Inteligência, e solicitou-se a distribuição compartimentada aos profissionais ativos com experiência em atuação entre agências de Inteligência.

Da interpretação dos dados obtidos, observa-se que um dos maiores obstáculos à integração efetiva é o estado anímico dos ativos da Inteligência. Surgiram, no decurso das entrevistas, questões como: importância das atividades particulares e do órgão desempenhadas na atuação integrada; diferença salarial entre agentes de órgãos diferentes que desempenham a mesma atividade no contexto de atuação integrada; não-aceitação da "gestão" ou do "comando" por integrante de outra instituição, por vários motivos, por exemplo, idade, menos tempo de serviço público, etc.; diferença na disponibilidade de recursos por parte das instituições; má gestão no envio dos recursos humanos; desconhecimento sobre o papel da Inteligência e personalização da atividade.

As questões apontadas estão ligadas diretamente ao estado anímico dos atores e a suas expectativas quando da atuação integrada. A criação de protocolo para servir como diretriz apta a nortear a atuação entre agências de Inteligência mitigaria os impactos nas ações integradas, na medida em que, no referido protocolo, estariam dispostos vários aspectos que impactam a atuação integrada, já identificados nos diversos estudos sobre o assunto e referenciados na presente pesquisa.

A coleta de dados se deu junto a mais de 105 (cento e cinco) agentes de Inteligência e observou as seguintes características:

- 85,7% são integrantes de órgãos da segurança pública;
- 11,4% pertencem a outra instituição integrante do Sisbin ou do Sisp;
- 2,9% são integrantes das Forças Armadas;
- 70,5% atuam em instituição com circunscrição em todo o território nacional;
- 29,5% atuam em instituição com circunscrição estadual;
- 41,9% exercem suas funções na região Centro-Oeste;
- 32,4 exercem suas funções na região Sudeste;
- 11,4% exercem suas funções na região Sul;

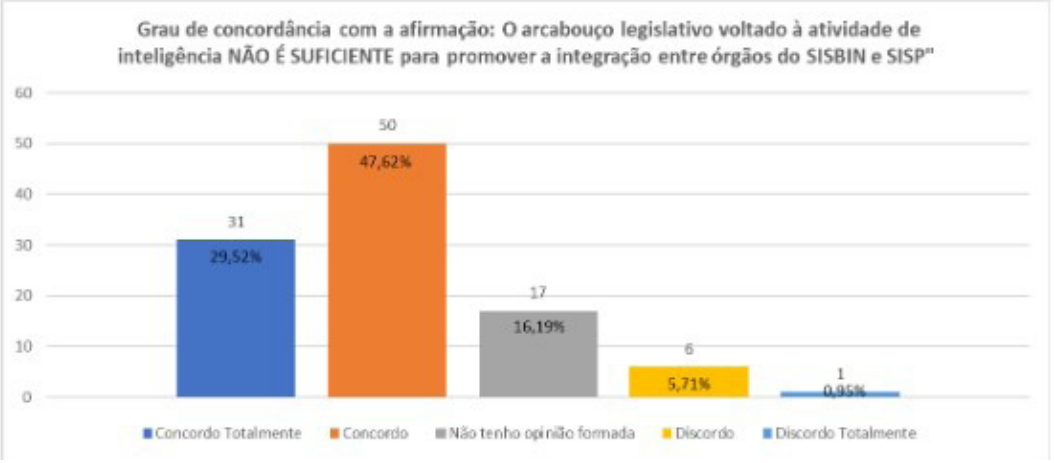
- 7,6% exercem suas funções na região Nordeste;
- 6,7% exercem suas funções na região Norte;
- 64,8% atuam ou atuaram como gestor público em sua instituição; e
- 83,8% já atuaram em ação que reuniu órgãos integrantes do Sisbin ou do Sisp.

No desenvolvimento da pesquisa, utilizamos a escala de Likert para mensurar a percepção dos ativos de Inteligência nos diferentes níveis de intensidade de opinião em relação a questões que circundam a temática estudada[1]. Durante o levantamento, os integrantes do Sisbin e do Sisp foram submetidos a questionamentos sobre a temática da necessidade de protocolos e atuação integrada entre agências de Inteligência. Nesses questionamentos, abordou-se assuntos sobre: suficiência e conhecimento da legislação; necessidade de criação de protocolos para disciplinar a atuação integrada e sua contribuição na mitigação das intercorrências no curso da ação; segurança jurídica nas decisões; otimização e dinamização das atividades; e se a ausência de referencial teórico contribui para inviabilizar a integração efetiva.

Os dados colhidos corroboram a posição de Gonçalves (2021) que afirma os baixos níveis de integração e a efemeridade da legislação no tocante à integração. Ressalta-se que, na aplicação do questionário, utilizou-se tanto a forma afirmativa negativa quanto a afirmativa positiva como forma de identificar a direção da atitude do respondente em relação à gradação de cada assertiva, já que isso tem efeito importante nos resultados e nas possibilidades de compreensão da realidade investigada.

1 A escala Likert, uma das metodologias de pesquisa mais utilizadas para realizar pesquisa de opinião, permite que se descubra o que o público pensa a respeito de um assunto ou tema, ao medir diferentes níveis de concordância e de intensidade.

Figura 1 - Grau de concordância com a insuficiência de legislação integrativa



Fonte: elaborada pelos autores.

A atual legislação fomenta a integração, mas não disciplina como esta deve ocorrer, e deixa um vácuo legislativo que tem sido preenchido pelo empirismo – desenvolvido, principalmente, após o ciclo de grandes eventos ocorridos no Brasil –, mas que, muitas vezes, pode ser afetado por questões de cunho pessoal, desprendidas dos princípios constitucionais e administrativos que regem a Administração Pública.

Os principais problemas que prejudicam a integração das agências surgem devido à falta de regramento mínimo apto a organizar, de maneira satisfatória, todos os fatores envolvidos no planejamento e na estruturação de uma ação integrada. Como destacado anteriormente, a partir da experiência profissional, os principais problemas que impactam a integração são: escassez de recursos; necessidade de apresentação de resultados imediatos ou em curto intervalo de tempo; resistência a mudanças por parte de órgãos e servidores; falta de consenso na tomada de decisão; lacuna legislativa sobre alguns pontos; desconfiança e disputa de poder entre órgãos; e rotatividade de servidores.

Ao considerar os problemas acima apresentados, constatamos que 88,6 % dos entrevistados já os vivenciaram em um contexto de atuação integrada entre agências de Inteligência. No universo de respondentes que já vivenciaram problemas no âmbito de ações interagências, verificamos que 93% consideram que a criação de um protocolo voltado especificamente para disciplinar a atuação entre órgãos do Sisp poderia contribuir para mitigar ou evitar eventuais problemas.

Ainda que se tenha uma contribuição efetiva na mitigação de eventos que atentem contra o regular andamento da integração, inevitavelmente, os protocolos

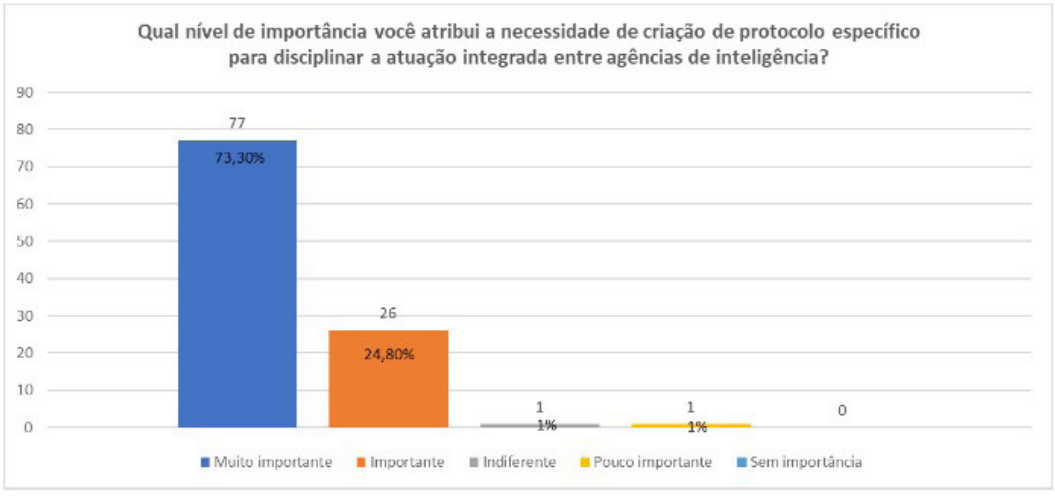
específicos não impedirão a ocorrência de todo e qualquer evento. Entretanto, servirão para conceder segurança jurídica aos gestores e operadores de Inteligência em suas decisões e permitirão a otimização dos recursos e a dinamização das atividades.

Essa conclusão corresponde ao entendimento de 95,2% dos participantes, quando a análise recai sobre a otimização de recursos da agência e a dinamização das atividades, porém esse percentual sobe para 98,1% dos participantes, quando o assunto é a segurança jurídica dos gestores e operadores na tomada de decisão.

Diante da ausência de regramento sobre o assunto, questionou-se os consultados acerca da necessidade de criação de protocolos para disciplinar a atuação integrada e sua contribuição na mitigação das intercorrências no curso da ação. O que se extrai da interpretação dos dados é o que se tenta demonstrar com a presente pesquisa. No universo dos pesquisados, não houve respondente que considerasse a criação de um protocolo específico para disciplinar a atuação integrada entre agências de Inteligência como assunto sem importância.

Nesse sentido, ressalta-se que 98,1% dos consultados consideram importante ou muito importante a criação de protocolo, e somente 1,9% se posicionaram como indiferentes ou consideram ser pouco importante.

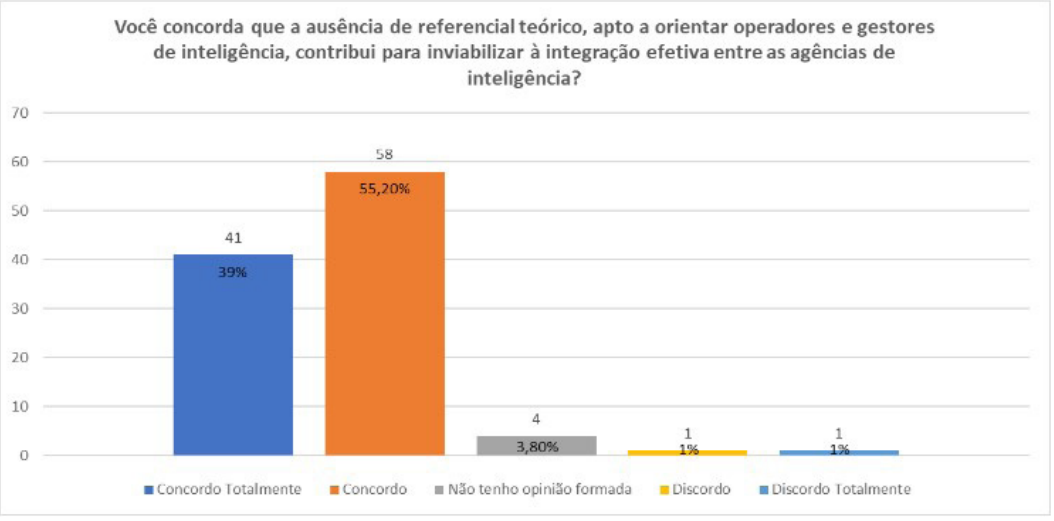
Figura 2 - Grau de importância atribuído à necessidade de criação de protocolos



Fonte: elaborado pelos autores.

A importância da normatização do assunto é asseverada quase que pela totalidade dos respondentes, mas um ponto que merece destaque é o fato de que somente 2% da totalidade dos colaboradores discorda do fato de que a ausência de diretriz, apta a orientar operadores e gestores de Inteligência, contribui para inviabilizar à integração efetiva entre as agências de Inteligência.

Figura 3 - Grau de concordância com a afirmação de que a ausência de referencial teórico contribui para inviabilizar a integração



Fonte: elaborada pelos autores.

Esse referencial precisa ser elaborado para viabilizar a criação do protocolo de integração. As diferentes organizações que trabalham com Inteligência de segurança pública precisam partilhar um conjunto de conceitos comuns, independentemente de serem organizações policiais, de fiscalização ou controle. Uma linguagem compartilhada facilitaria o intercâmbio entre agências e propiciaria um sentido de comunidade de Inteligência e, consequentemente, maior agilidade ou fluidez nas interações entre os órgãos envolvidos.

Considerações finais

O dinamismo das relações e a agilidade da resposta requerida no mundo globalizado exigem que o agente de Inteligência, no desempenho de sua atividade, esteja provido de ferramentas e garantias necessárias ao exercício de suas atribuições funcionais.

Ainda que em plena evolução legislativa, não se pode olvidar a existência de lacunas no tocante à integração das ações das

agências de Inteligência, principalmente, no que tange aos protocolos específicos para atuação integrada do Sisbin e do Sisp.

A essencialidade e a imprescindibilidade da criação de protocolos para atuação integrada entre agências refletem a percepção de parcela da comunidade de Inteligência que anseia por um referencial teórico na padronização e na orientação da atuação dos agentes de Inteligência, vez que sua existência visa a nortear a execução das ações integradas, de modo a evitar ou mitigar eventuais riscos decorrentes da ação, bem como otimizar os recursos disponíveis e entregar um serviço de excelência à sociedade.

Notoriamente, a ação integrativa passa por eventuais problemas que inviabilizam a integração, até que se consolide efetivamente. Há a necessidade de se produzir protocolos entre agências para articular, subordinar, coordenar, complementar e suplementar os recursos policiais e produzir cadeia de comando de controle. Isso evita que operações sejam feitas sem planejamento adequado e uma construção política transparente, o que envolve diagnósticos prévios e planos de ação substantivos (MUNIZ, 2018).

Dessa forma, a omissão legislativa quanto à edição de protocolos específicos, no âmbito da Atividade de Inteligência, como preceitua o arcabouço jurídico sobre a matéria, dificulta a integração e obstaculiza a construção do conhecimento de Inteligência, o que vergasta a utilidade da informação e, por conseguinte, o assessoramento estratégico.

Por fim, como agenda de estudos futuros, é preciso acompanhar de perto a atuação das agências e verificar se a integração está ocorrendo de forma efetiva e garantindo que os recursos estejam sendo direcionados para o fim comum e que os resultados esperados estejam sendo alcançados.

Um dos principais desafios enfrentados nessa etapa é a falta de dados e indicadores monitorados, o que torna difícil avaliar o desempenho das equipes e identificar possíveis problemas. Além disso, outro obstáculo comum é a resistência de algumas agências à implementação da política de integração, seja por questões culturais seja por interesses próprios. Nesse sentido, é importante que a política pública seja clara em relação às obrigações e responsabilidades de cada agência, além de estabelecer a operação efetiva de coordenação e controle. O presente trabalho não teve o propósito de fixar passos ou condições para elaboração de um protocolo de cooperação entre agências nem de estabelecer indicadores que permitam monitorar a implementação da integração. O objetivo foi realizar a análise da necessidade do fortalecimento de uma institucionalização que leve à efetiva integração.

O resultado final da análise é consoante com outros estudos recentes que apontam a limitação ou a insuficiência do arcabouço

normativo para implementação e efetivo funcionamento do Sisp (BRANDÃO, 2022; PYTLOWANCIV & SILVA, 2022). É preciso superar os desafios enfrentados, como a falta de dados e indicadores, a resistência de algumas forças e a falta de capacitação dos agentes responsáveis pelo monitoramento e pela avaliação, e buscar um processo efetivo de acompanhamento e correção de possíveis problemas identificados. Constatada a importância de criação de protocolos específicos para nortear as ações integradas no âmbito do Sisp, sugere-se o aprofundamento dos estudos, com a participação dos diferentes órgãos, a fim de se estabelecer requisitos mínimos para o exercício integrado da Atividade de Inteligência e conferir, assim, nesse aspecto, concretude ao Princípio Constitucional da Eficiência.

Referências

BATTAGLIA, M. G. B. A Inteligência Competitiva modelando o sistema de informação de clientes – Finep. *Ciência da Informação*, v. 29, n. 2, p. 200-214, 1999. Disponível em:https://www.scielo.br/j/ci/a/yM6goSWbVYwtnjRD8z4VwBJ/abstract/?lang=pt#. Acesso em: 20 maio 2023.

BRANDÃO, P. O Subsistema de Inteligência de Segurança Pública no Brasil: uma análise institucional. *In:* BRANDÃO, P.; CEPIK, M. *Inteligência de segurança pública:* teoria e prática no controle da criminalidade. Niterói: Impetus, 2013.

BRASIL. *Decreto nº 10.778, de 24 de agosto de 2021*. Aprova a Estratégia Nacional de Inteligência de Segurança Pública. Disponível em:https://portal.in.gov.br/web/dou/-/decreto-n-10778-de-24-de-agosto-de-2021-340728978. Acesso em: 20 maio 2023.

BRASIL. *Decreto nº 10.777, de 24 de agosto de 2021*. Institui a Política Nacional de Inteligência de Segurança Pública. Disponível em:http://planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10777.htm. Acesso em: 20 maio 2023.

BRASIL. *Decreto s/n, de 15 de dezembro de 2017*. Aprova a Estratégia Nacional de Inteligência. Disponível em: http://planalto.gov.br/ccivil_03/_ato2015-2018/2017/dsn/Dsn14503.htm. Acesso em: 20 maio 2023.

BRASIL. *Decreto nº 8.903, de 16 de novembro de 2016.* Institui o Programa de Proteção Integrada de Fronteiras e organiza a atuação de unidades da administração pública federal para sua execução. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8903.htm. Acesso em: 20 maio 2023.

BRASIL. *Decreto nº 8.793, de 29 de junho de 2016*. Fixa a Política Nacional de Inteligência. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2015-2018/decreto/D8793.htm. Acesso em: 20 maio 2023.

BRASIL. *Decreto nº 4.376, de 13 de setembro de 2002*. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei nº 9.883, de 7 de dezembro de 1999, e dá outras providências. Disponível em:http://www.planalto.gov.br/ccivil_03/decreto/2002/D4376compilado.htm. Acesso em: 20 maio 2023.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em:http://www.planalto.gov.br/ccivil_03/constituição/constiuicaocompilado.htm. Acesso em: 20 maio 2023.

BRASIL. Ministério da Defesa. *Política Nacional de Defesa e Estratégia Nacional de Defesa*. Brasília, DF: Ministério da Defesa. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf. Acesso em: 20 maio 2023.

CAPUANO, E. A. *et al*. Inteligência competitiva e suas conexões epistemológicas com a gestão da informação e do conhecimento. *Ciência da Informação*, v. 38, n. 2, p. 19-34, 2009. Disponível em:https://www.scielo.br/j/ci/a/Zz45KyPX8XnQCVCrqwFPDqg/?lang=pt. Acesso em: 29 maio 2023.

CRANE, A., In the company of spies: when competitive intelligence gathering becomes industrial espionage. *Business Horizons*, v. 48, n. 3, p. 233–240, 2005. Disponível em:https://doi.org/10.1016/j.bushor.2004.11.005 (https://www.sciencedirect.com/science/article/pii/S0007681304001302). Acesso em: 20 maio 2023.

CONDEIXA, F. DE M. S. P. Espionagem e direito. *Revista Brasileira de Inteligência*, n. 10, p. 21-40, 1 dez. 2015. Disponível em:https://rbi.enap.gov.br/index.php/RBI/article/view/123.

DO CARMO, B. A.; DE SOUZA, G. Atuação do enfermeiro na classificação de risco através do protocolo de Manchester: uma revisão da literatura. *Revista Eletrônica Acervo Saúde*. Disponível em: https://www.acervosaude.com.br/doc/REAS140.pdf. Acesso em: 20 maio 2023.

FERNANDES, F. C. Inteligência e gestão estratégica. *Revista Brasileira de Inteligência*, Brasília, n. 7, p. 21-30, jul. 2012.

GONÇALVES, J. V. *O Que Fazer Com Nossos Espiões? Considerações sobre a Atividade de Inteligência no Brasil*. Brasília: Agenda legislativa, cap. 12, p. 1-25. 2011. Disponível em: https://www12.senado.leg.br/publicações/estudos-legislativo/tipos-de-estudos/outras-publicacoes/agenda-legislativa/capitulo-12-o-que-fazer-com-nossos-espioes-consideracoes-sobre-a-atividade-de-inteligencia-no-brasil. Acesso em: 20 maio 2023.

GUEDES, L. C. A mãe das Inteligências. *Revista Brasileira de Inteligência*, v. 2, n. 2, p. 21-35, 1 abr. 2006. Disponível em: https://rbi.enap.gov.br/index.php/RBI/article/view/22. Acesso em: 20 maio 2023.

KAHANER, L. *Competitive intelligence:* how to gather, analyse, and use information to move your business to the top. New York: Simon & Schuter, 1996.

KENT, S. *Strategic intelligence for american world policy*. Rio de Janeiro: Biblioteca do

Exército, 1949.

MARCIAL, E. C. *Análise estratégica:* estudos de futuro no contexto da Inteligência competitiva. Brasília: Thesaurus, 2011.

MUNIZ, J. O.; ALMEIDA, R. R. Respondendo às balas: segurança pública sob intervenção das palavras entrevista com Jacqueline Muniz. *Trabalhos em Linguística Aplicada* [online]. 2018, v. 57, n. 2, p. 993-1014. Disponível em: https://doi.org/10.1590/01031813865239338734 1. Acesso em: 20 maio 2023.

PIMENTA, C. A. M. *et al. Guia para construção de protocolos assistenciais enfermagem*. São Paulo: Coren-SP, 2015. Disponível em: https://portal.coren-sp.gov.br/sites/default/files/Protocolo-web.pdf . Acesso em: 6 out. 2021.

PYTLOWANCIV, D.; SILVA, H. Análise da política e da estratégia nacionais de Inteligência de segurança pública sob a perspectiva das capacidades organizacionais. *Revista Brasileira de Ciências Policiais*, v. 13, n. 10, p. 241-265, 2022.

RIBEIRO, A. C. M. L.; DOS SANTOS, C. D. Isso não é uma pirâmide: revisando o modelo clássico de dado, informação, conhecimento e sabedoria. *Ciência da Informação*, v. 49, n. 2, p. 67-87, 2020. Disponível em: https://revista.ibict.br/ciinf/article/view/5066/5247. Acesso em: 29 maio 2023.

SILVA, José Afonso. *Curso de direito constitucional positivo*. 25. ed. São Paulo: Editora Malheiros, 2005.

TEIXEIRA, Valdeci de Assis; OSELAME, Gleidson Brandão; NEVES, Eduardo Borba. O Protocolo de Manchester no Sistema Único de Saúde e a atuação do enfermeiro. *Revista da Universidade Vale do Rio Verde*, Três Corações-MG, v. 12, n. 2, p. 905-920, ago/dez. 2014. Disponível em:http://periódicos.unincor.br/index.php/revistaunincor/article/view/1769. Acesso em: 23 nov. 2021.

Artigo

10

DETECÇÃO E CONTENÇÃO: MEDIDAS PARA A SALVAGUARDA DAS ÁREAS SENSÍVEIS E DE SEGURANÇA CONTRA DRONES IRREGULARES, DESCONHECIDOS E MALICIOSOS

DOI: https://doi.org/10.58960/rbi.2023.18.229

Eduardo Araújo da Silva *
Carlos Eduardo Valle Rosa **
Rodrigo Sande Souza ***

Resumo

O presente artigo tem por objetivo analisar as possibilidades de emprego dos meios de defesa contra drones irregulares, desconhecidos e maliciosos que, sobrevoando instalações patrimoniais consideradas sensíveis e de segurança, possam colocar em risco a segurança orgânica e a incolumidade dessas áreas; avultando-se princípios do Poder Aeroespacial e considerando disposições jurídico-normativas latentes. Como pressuposto metodológico norteador, recorreu-se a uma pesquisa de natureza exploratória, com fulcro na abordagem qualitativa, buscando-se a compreensão das informações coletadas não somente pela observação empírica sobre o assunto, mas, sobretudo, por fundamentações técnicas, normativas e doutrinárias sobre o tema. Não obstante seja uma solução tecnológica viável para o combate a drones indesejados, há que se observar fatores significativos como o custo operacional e os métodos de utilização dos equipamentos. Apontam-se a necessidade de se detectar e conter ameaças aéreas não tripuladas, bem como as possibilidades de implementação dessas medidas mitigadoras e, do mesmo modo, a indispensabilidade de discussões acerca das avaliações, por parte dos órgãos reguladores, dos possíveis impactos à aviação tripulada devido ao uso inadequado ou à revelia dessas ferramentas.

Palavras-chave: antidrone; contenção; detecção; drones; segurança.

DETECTION AND CONTAINMENT: MEASURES TO PROTECT RESERVED AND SECURITY AREAS AGAINST IRREGULAR, UNKNOWN AND MALICIOUS DRONES

Abstract

This article aims to analyze the possibilities of using means of defense against irregular, unknown and malicious drones that, flying over heritage installations considered reserved and security areas, could put the organic security and safety of these areas at risk; looming large over the principles of Aerospace Power and considering latent legal-normative provisions. As a guiding methodological

* Mestre em Educação pela Universidade Federal Rural do Rio de Janeiro (UFRRJ). Doutorando em Ciências Aeroespaciais pela Universidade da Força Aérea (UNIFA). Capitão Especialista em Controle de Tráfego Aéreo da Força Aérea Brasileira (FAB).

** Mestre em Ciências Aeroespaciais pela Universidade da Força Aérea (UNIFA). Doutor em Geografia pela Universidade Federal do Rio Grande do Norte (UFRN). Coronel Aviador da reserva da Força Aérea Brasileira (FAB) e professor da UNIFA.

*** Especialista em Autodefesa de Superfície de Aeródromos e em Segurança da Aviação Civil contra Atos de Interferência Ilícita (AVSEC). Primeiro-Tenente de Infantaria da Força Aérea Brasileira (FAB).

assumption, research of an exploratory nature was used, with a focus on the qualitative approach, seeking to understand the information collected not only through empirical observation on the subject, but, above all, through technical, normative and doctrinal foundations on the theme. Although it is a viable technological solution for combating unwanted drones, significant factors such as operational cost and methods of using the equipment must be taken into account. The need to detect and contain unmanned aerial threats is highlighted, as well as the possibilities of implementing these mitigating measures and, likewise, the indispensability of discussions regarding assessments, by regulatory bodies, of the possible impacts on manned aviation due to inappropriate use or failure to use these tools.

Keywords: *anti-drone; containment; detection; drone; security.*

DETECCIÓN Y CONTENCIÓN: MEDIDAS PARA PROTEGER ZONAS SENSIBLES Y DE SEGURIDAD CONTRA DRONES IRREGULARES, DESCONOCIDOS Y MALICIOSOS

Resumen

Este artículo tiene como objetivo analizar las posibilidades de utilizar medios de defensa contra drones irregulares, desconocidos y maliciosos que, sobrevolando instalaciones patrimoniales consideradas sensibles y de seguridad, podrían poner en riesgo la seguridad orgánica de dichas zonas; sobrevolando los principios del Poder Aeroespacial y considerando disposiciones jurídico-normativas latentes. Como presupuesto metodológico principal, se recurrió a una pesquisa de naturaleza exploratoria, con fulcro en el abordaje cualitativo, cercando la comprensión de las informaciones colectadas no solo por la observación empírica sobre el tema, pero, sobretodo, por fundamentaciones técnicas, normativas e doctrinarias sobre el tema. Aunque se trata de una solución tecnológica viable para combatir los drones no deseados, se deben tener en cuenta factores importantes como el coste operativo y los métodos de uso del equipo. Se destaca la necesidad de detectar y contener las amenazas aéreas no tripuladas, así como las posibilidades de implementar estas medidas mitigadoras y, asimismo, la indispensable discusión sobre las evaluaciones, por parte de los organismos reguladores, de los posibles impactos en la aviación tripulada por su uso inadecuado o falla. para utilizar estas herramientas.

Palabras clave: *anti-drones; contención; detección; dron; seguridad.*

Introdução

Como um fluxo natural da evolução dos meios tecnológicos, a aviação tem sido um dos setores que mais cresce em escala mundial. No Brasil, por exemplo, tem-se observado um crescimento contínuo das operações aéreas. Segundo o Anuário Estatístico de Tráfego Aéreo (2022, p. 218), do Departamento de Controle do Espaço Aéreo (DECEA), foram contabilizados 1.677.760 movimentos aéreos no ano de 2022, considerando-se pousos e decolagens, o que representa um aumento de 26% no número de operações em relação ao ano anterior.

Em meio a esse desenvolvimento permanente, nota-se, da mesma forma, um acelerado progresso no tocante à utilização das Aeronaves Não Tripuladas (UA, do acrônimo *Unmanned Aircraft*), ou drones, sobretudo nas atividades em que as imagens aéreas se fazem necessárias, como na topografia, resposta a desastres, inspeção de ativos, inteligência, vigilância, segurança pública e privada, pesquisa, agricultura de precisão, publicidade, dentre outras.

De acordo com dados do Sistema para solicitação de Acesso ao Espaço Aéreo Brasileiro por Aeronaves Não Tripuladas (SARPAS), em 2016, ano em que essa plataforma foi criada pelo DECEA, apenas 95 solicitações de voo foram registradas. No final de dezembro de 2022, esse número alcançou aproximadamente 311 mil pedidos.

Novos resultados são inevitáveis quando da aplicação de tecnologias disruptivas, devido às possibilidades que estas trazem para um contexto em contínua evolução. Segundo Christensen (1997), a inovação é um fenômeno capaz de constituir oportunidades novas, sendo uma ferramenta implementada pelos empreendedores em prol de vantagens frente aos concorrentes. No contexto do desenvolvimento da aviação, sendo reconhecido como pioneiro do Poder Aéreo, Giulio Douhet já sinalizava que esse crescimento seria um fator resultante inevitável.

> (...) as opiniões podem diferir, porém um fato certo é que o novo meio de transporte encontrou para si um lugar permanente. Em toda a história dos meios de transporte, esta máquina que o homem, após séculos de tentativas fracassadas, pôde criar com seu gênio e ousadia, fez o mais rápido e notável progresso. Não é possível predizer que estágio de desenvolvimento ela alcançará, porém tudo indica que um considerável progresso ainda lhe será reservado (DOUHET, 1978, p. 108).

Nesse mesmo sentido, o progresso da aviação promoveu o desenvolvimento de novas possibilidades operacionais, como o reconhecimento e a observação aérea, por exemplo, funções essenciais para as primeiras forças aéreas beligerantes. De acordo com Rosa (2014);

> (...) desde a primeira ação de aeronaves em combate, ocorrida em 23 de outubro de 1911, na Guerra entre a Turquia e a Itália, quando o Capitão Piazza decolou para reconhecer posições turcas, o poder aéreo pode prover consciência situacional para as

> forças no teatro de operações por meio da coleta, controle, difusão e processamento de informações sobre os elementos que integram o espaço de batalha (*ibidem*, p. 372).

Segundo Chernova *et al.* (2023), do canal de notícias CNN, em 3 de maio deste ano, a Rússia fez acusações à Ucrânia no sentido de responsabilizá-la pelo ataque noturno com drone ocorrido sobre a cidadela do Kremlin, que fora bloqueado devido às defesas eletrônicas já instaladas no local. O Presidente ucraniano, Vlolodymyr Zelensky, não confirmou tal afirmação. A CNN ratificou não existirem evidências que comprovem a origem do ataque. O fato coloca em voga novas tensões entre os Estados e exemplifica o uso malicioso do vetor não tripulado.

No Brasil, há indicadores que apontam casos de uso irregular dos drones. Embora haja um vasto arcabouço regulatório sobre o tema, e cada agência reguladora trate especificamente da sua área de atuação fiscalizando o segmento, observa-se que algumas restrições expressas não são cumpridas pelos usuários em sua totalidade.

Cabe frisar que, embora o termo drone seja mundialmente consagrado, ainda são encontradas expressões como Veículos Aéreos Não Tripulados (VANT), Aeronaves Remotamente Pilotadas (ARP), *Unmanned Aerial Vehicle* (UAV), *Remotely Piloted Aircraft* (RPA) e *small Unmanned Aircraft* (sUA), e seus sistemas: SisVANT, SARP, RPAS e sUAS.

Drone, para Iqbal (2021), Ahmed et al. (2022) e Stamate et al. (2023), definido como uma aeronave sem um piloto a bordo operada a partir de uma estação remota, é a abreviação do termo em inglês *Dynamic Remotely Operated Navigation Equipment*, que representa o acrônimo "Equipamento de Navegação Dinâmica Operado Remotamente". Esses autores usam o mesmo verbete para se referirem às plataformas remotas aéreas, terrestres, aquáticas e subaquáticas. Nesta pesquisa, utilizar-se-á a sigla UA para representar o componente aéreo não tripulado e UAS para configurar o macrossistema do segmento.

Por ser um estudo de natureza exploratória, de cunho qualitativo, procurou-se coletar dados e informações não só a partir de bibliografias, mas, também, casos concretos recentes e significativos para o desenvolvimento do tema. A busca se deu junto a fundamentações técnicas, normativas e doutrinárias, publicadas por órgãos reguladores, mídias sociais e instituições públicas e privadas que operacionalizam o uso dos drones. O referencial teórico se baseia em conceitos do Poder Aeroespacial, segurança operacional, interferência ilícita, espaço aéreo, meios não tripulados, segurança e defesa. Para Triviños (1987), o estudo descritivo tem como objetivo conhecer a realidade a partir da descrição de fatos e realidades.

O tema é discutido sob a égide de três

grandes áreas que se complementam: (i) o tráfego aéreo; (ii) a aviação; e (iii) a defesa em solo contra ameaças aéreas. As considerações dos autores também levam em conta as expertises que refletem suas áreas de atuação profissional, assim como pareceres técnicos e jurídicos.

A proposta do artigo é apresentar um análise sobre as possibilidades de emprego dos meios de defesa contra drones irregulares, desconhecidos e maliciosos que possam colocar em risco a segurança orgânica e a incolumidade das instalações consideradas sensíveis e de segurança, à luz da teoria do Poder Aeroespacial e das disposições jurídico-normativas mais latentes. O compêndio reúne observações a respeito de infraestruturas críticas e conceituações quanto às extensões sensíveis e de segurança, assim como medidas de restrição e bloqueio de sobrevoos indevidos.

O texto busca conceituar espaço aéreo, ordem e segurança pública, denotando ocorrências que envolvem voos irregulares, desconhecidos e maliciosos. A necessidade e os desafios para a implementação dos sistemas de contenção também são trazidos no estudo e, por fim, o artigo exemplifica algumas possibilidades de sistemas antidrones e suas capacidades.

Breves considerações sobre áreas sensíveis e de segurança

É muito comum a utilização do termo *segurança* no âmbito aeronáutico. Depara-se, a todo o tempo, com referências acerca da segurança operacional, segurança de voo, da aviação, aeroportuária, das instalações, de terceiros no solo e suas propriedades; assim como a palavra *sensível*, que traduz algo suscetível a estímulos ou vulnerável a impressões externas, aquilo que não deve ser invadido ou violado. Segundo a Instrução do Comando da Aeronáutica (ICA) 100-40/2023, que trata das UA e o acesso ao espaço aéreo brasileiro, são áreas de segurança:

> (...) refinarias, plataformas de exploração de petróleo, depósitos de combustível, estabelecimentos penais, áreas militares, usinas hidroelétricas, usinas termoelétricas, usinas nucleares, redes de abastecimento de água ou gás, barragens ou represas, redes de comunicação (como, por exemplo, sítios de antenas) ou de vigilância da navegação aérea (como, por exemplo, radares de vigilância aérea), que se forem danificadas provocarão sério impacto social, econômico, político ou à segurança (BRASIL, 2023).

Importa dizer que esse mesmo dispositivo preconiza que áreas de segurança não devem ser sobrevoadas sem a autorização de seus responsáveis. Os Estados possuem gerência sobre seus territórios e mares territoriais, sendo o mesmo válido para as porções de espaço aéreo sob o seu domínio geográfico. De acordo com o Art. 11 da Lei 7.565/86, que dispões sobre o Código Brasileiro de Aeronáutica (CBA), a União exerce completa e exclusiva soberania sobre o espaço aéreo acima de seu território e mar territorial. O mesmo Código expressa que cabe à Força Aérea planejar, gerenciar

e controlar as atividades relacionadas ao tráfego aéreo, a fim de manter o alto nível da segurança operacional

O Poder Aeroespacial de uma nação implica o exercício de soberania, e a soberania é a capacidade de exercê-lo. Nesse contexto, quando drones maliciosos voam sem anuência do órgão regulador, sem a possibilidade de serem controlados, ou buscando burlar esse controle, há uma clara cisão na questão do exercício da soberania, principalmente quando se fala em reflexos à segurança de áreas sensíveis ou incolumidade de pessoas.

Para Rosa (2022), a soberania possui relação direta com a capacidade de exercício de poder, assim como sua dinâmica com a habilidade de coerção por meio da força. O Poder Aeroespacial, considerado por Mesquita (2018) como uma evolução do Poder Aéreo, se configura como uma parcela do Poder Nacional. De acordo com a Doutrina Básica da Força Aérea Brasileira (DCA 1-1/20), o Poder Aeroespacial é:

> (…) a projeção do Poder Nacional resultante da integração dos recursos de que a Nação dispõe para a utilização do espaço aéreo e do espaço exterior, quer como instrumento de ação política e militar, quer como fator de desenvolvimento econômico e social, visando conquistar e manter os objetivos nacionais (BRASIL, 2020).

Para Ribeiro (2018), uma ameaça aérea pode ser representada de formas distintas, como, por exemplo, mísseis de cruzeiro e balísticos, vetores aéreos de asas fixas e rotativas, artefatos explosivos guiados, inclusive de forma remota e, da mesma maneira, as ARP. Diante de algumas violações de normas que estão em vigor, no que tange ao uso irregular, desconhecido ou malicioso dos drones, muitos podem ser os instrumentos para coibir tais práticas, devendo ocorrer uma certa inter-relação de diretrizes com fulcro nas legislações em vigor, nas boas práticas já aplicadas e na possível escassez de uma norma específica que trate do assunto. O artigo 21 do CBA prevê que órgãos competentes devem autorizar transportes de cargas perigosas e nocivas à segurança das pessoas e das aeronaves.

> Salvo com autorização especial de órgão competente, nenhuma aeronave poderá transportar explosivos, munições, arma de fogo, material bélico, equipamento destinado a levantamento aerofotogramétrico ou de prospecção, ou ainda quaisquer outros objetos ou substâncias consideradas perigosas para a segurança pública, da própria aeronave ou de seus ocupantes (BRASIL, 1986).

Áreas como usinas hidroelétricas, termoelétricas e nucleares, assim como redes de abastecimentos de água e gás, representam instalações que proveem elementos essenciais à vida, não podendo ser objeto de quaisquer interferências ilícitas. Igualmente aos sítios aeroportuários, esses estabelecimentos devem ser considerados sensíveis. Também são assim consideradas as organizações militares e de segurança pública, estabelecimentos prisionais, agências de inteligência, áreas dos povos indígenas, unidades de conservação e

reservas florestais.

O Decreto nº 11.200/22, que aprova o Plano Nacional de Segurança de Infraestruturas Críticas, subdivide essas áreas sensíveis nos seguintes setores: barragens, abastecimento, energia elétrica, petróleo, gás natural, biocombustíveis, transportes terrestres, aéreos e aquaviários, telecomunicações, radiodifusão, serviços postais, finanças, biossegurança, bioproteção e defesa. De forma simbólica, a Figura 1 representa esses setores.

Figura 1 - Sistema de Infraestrutura Crítica (SIC)

Fonte: https://www.gov.br/gsi

Segundo o GSI-PR,

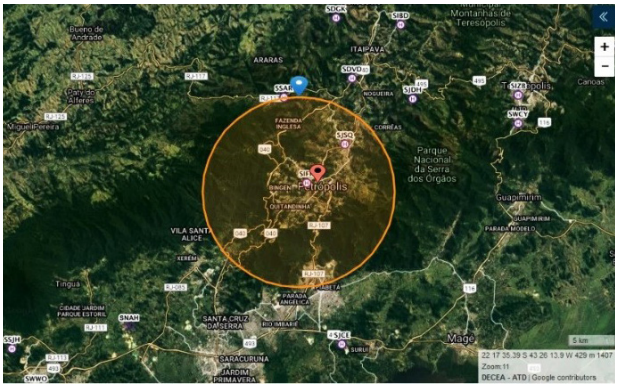
> (...) infraestruturas de comunicações, de energia, de transportes, de finanças, de águas, de defesa, entre outras, possuem dimensão estratégica, uma vez que desempenham papel essencial tanto para a segurança e soberania nacionais, como para a integração e o desenvolvimento econômico sustentável do País. Fatores que prejudiquem o adequado fornecimento dos serviços provenientes dessas infraestruturas podem acarretar transtornos e prejuízos ao Estado, à sociedade e ao meio ambiente (BRASIL, 2022).

Do mesmo modo, o Exército Brasileiro (EB) também destaca a proteção de infraestruturas críticas. Para a força terrestre, essas estruturas estratégicas terrestres devem ser protegidas, essencialmente:

> (...) em situação de crise, apoio à defesa civil em caso de calamidades naturais ou provocadas, inclusive em áreas contaminadas por agentes químicos, biológicos, radiológicos e nucleares; coordenação de segurança e atuação em Grandes Eventos; realização de operações de Garantia da Lei e da Ordem (GLO) e Garantia da Votação e Apuração em pleitos eleitorais e ações de prevenção e combate ao terrorismo, quando demandada pelo governo federal, entre outras operações subsidiárias (BRASIL, 2016).

Cada ente da Administração direta ou indireta, que atua na gestão ou no controle dessas áreas, tratará seus setores aos moldes das estruturas organizacionais próprias. E, conquanto haja uma diversidade de nomenclaturas sobre áreas sensíveis, de segurança, críticas, estratégicas, há de se observar que o DECEA, em sua legislação específica para o acesso ao espaço aéreo por UA, teve a preocupação em proteger tais estruturas. Silva (2023) ratifica que essas proteções de áreas específicas, por restrição ou bloqueio, são conhecidas respectivamente como *Flight Restriction Zone* (FRZ) e *No Fly Zones* (NFZ), como na Figura 2 abaixo.

Figura 2 - *Flight Restriction Zone* em Petrópolis/RJ



Fonte: DECEA

De acordo com item 2.1.72 da ICA 100-40/2023, uma FRZ é definida como:

> Área específica na qual o acesso de Aeronave Não Tripulada (UA) requer autorização mediante análise ATM do Órgão Regional, considerando as restrições previstas em função das alturas e distâncias de aeródromos e helipontos ou das áreas de segurança. A Zona de Aproximação ou de Decolagem (ZAD), a Zona de Entorno de Aeródromo (ZEA), a Zona de Entorno de Heliponto (ZEH) e as Áreas de Segurança são consideradas Zona de Restrição de Voo (FRZ) (BRASIL, 2023).

Em complemento, o item 2.1.73 da Instrução expressa que a NFZ é considerada uma área específica na qual o voo normalmente não é permitido. Sua origem é de ordem técnica e, por isso, é criada pelos fabricantes de UA.

Embora voos ilícitos possam ocorrer nos casos em que o piloto remoto não solicita o acesso ao espaço aéreo, essas metodologias de negação às operações já representam um primeiro filtro visando à manutenção da segurança operacional e das instalações em solo.

Apontamentos sobre espaço aéreo, ordem pública e segurança pública

Sobre as ações contra ameaças não tripuladas, muito se questiona acerca de "o que deve ser feito", "quem deve fazer"

e "como fazer". Basta pensar num drone sobrevoando, à revelia, uma pista de um aeroporto ou adentrando, pelo ar, a área patrimonial de uma unidade prisional. Cenários como esses têm sido comuns no território nacional e, por isso, é necessário discutir sobre o uso de equipamentos que visem à segurança orgânica e de seus recursos humanos.

O espaço aéreo é definido como a porção da atmosfera sobre o território de um Estado. E, nesse diapasão, o artigo 8º da Convenção de Aviação Civil Internacional (CACI) prevê que:

> Nenhuma aeronave capaz de navegar sem piloto poderá sobrevoar sem piloto o território de um Estado contratante sem autorização especial do citado Estado e de conformidade com os termos da mesma autorização. Cada Estado contratante se compromete a tomar as disposições necessárias para que o vôo sem piloto de tal aeronave nas regiões acessíveis de aeronaves civis seja controlada de modo a evitar todo perigo para as aeronaves civis (CACI, 1944).

O artigo 9º da CACI aponta que, por razões militares ou de segurança pública, os Estados poderão limitar ou proibir que as aeronaves de outros Estados voem sobre certas zonas do seu território. Nota-se que, mesmo sendo uma Convenção que legisla sobre a aviação civil em escala global, houve a preocupação pontual com as razões militares e de segurança pública.

Por mais que definições sejam específicas, consideram-se muito tênues as linhas entre estes três escopos: espaço aéreo, ordem pública e segurança pública. A ordem pública, consoante o artigo 2º do Decreto nº 88.777/83, é definido como sendo um:

> Conjunto de regras formais, que emanam do ordenamento jurídico da Nação, tendo por escopo regular as relações sociais de todos os níveis, do interesse público, estabelecendo um clima de convivência harmoniosa e pacífica, fiscalizado pelo poder de polícia, e constituindo uma situação ou condição que conduza ao bem comum (BRASIL, 1983).

Conforme o artigo 144 da CF/88, a segurança pública é dever do Estado, direito e responsabilidade de todos, devendo ser exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio. Para Lessa (2021), o conceito de ordem pública vai além, devendo ser considerado um estado de normalidade social, em que usufruto de direitos e cumprimento de deveres coexistem em harmonia, como um conjunto de princípios e normas.

Drones como vetores irregulares, desconhecidos ou maliciosos

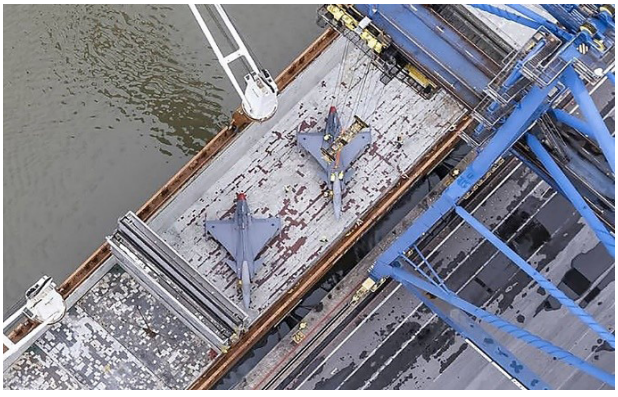
Tem sido recorrente o reporte de operações irregulares ou com características suspeitas com drones no espaço aéreo brasileiro. Não só por avistamentos de terceiros, mas por agentes da segurança pública e mídias sociais. Em 26 de março de 2023, um drone próximo à pista do Aeroporto em Guarulhos causou a suspensão das operações. Alguns voos foram alternados para outro sítio e aqueles que estavam

prontos para a decolagem precisaram se manter no solo, até a retomada do fluxo. A notícia foi veiculada pelo portal G1 de São Paulo, na data da ocorrência.

Voos irregulares de drones são aqueles que ocorrem sem autorização prévia do órgão regulador, que possuem restrição para certa operação e mesmo assim a executa ou, até mesmo, os que por alguma inconsistência técnica ou sistêmica deixam de cumprir suas configurações preestabelecidas e voam à revelia, podendo causar uma ocorrência inesperada e, quiçá, danosa.

Santa Catarina também foi palco de irregularidade com o uso de drone. Em 2022, os caças *Saab F-39 Gripen* foram filmados por um drone considerado desconhecido, pois, para o local e período, não havia no SARPAS a solicitação do voo. O fato se tornou público porque o piloto remoto postou o conteúdo em sua rede social *(instagram)* e o vídeo foi replicado por um outro usuário (no *youtube*). Ocorrências como essa, em que indícios de autoria e materialidade são facilmente observados, devem ser levadas ao conhecimento dos órgãos regionais do DECEA e Junta de Julgamento da Aeronáutica (JJAER), com vistas às apurações e aplicações das sanções administrativas cabíveis ao cometimento de irregularidades de tráfego aéreo. Na Figura 3 abaixo é possível observar as duas aeronaves da FAB sendo monitoradas pelo drone.

Figura 3 - Imagens dos caças Gripen captadas por drone irregular



Fonte: https://aeroin.net

Em 5 de abril de 2023, em Minas Gerais, um casal foi preso por usar um drone como ferramenta de entrega de drogas e celulares num complexo penitenciário da cidade de Belo Horizonte. O portal G1 ressaltou que movimento intenso de drones era abastecido por pagamentos de aproximadamente 200 reais por voo.

É possível que voos como esse não passem pelo devido processo de aprovação, e que os órgãos reguladores e de segurança não

tenham conhecimento sobre o voo, a não ser que seja por meio de avistamento ou denúncia. É um exemplo claro de voo malicioso. Uma das maiores dificuldades perante o avanço acelerado dessa tecnologia é a configuração dos dispositivos de defesa. A capacidade de detecção é imprescindível para que se planeje uma ação mitigadora.

Outro aspecto relevante é a contenção, visto que é uma ação que visa repelir, cessar ou capturar uma ameaça não tripulada. Há diversos autores que falam sobre *layers* (camadas) para uma composição eficaz de um sistema antidrone, conhecido como C-UAS, do acrônimo *Counter - Unmanned Aircraft Systems.* É possível encontrar referências que o subdvidem em: detecção, localização, identificação, contenção e captura. Outrossim, em um primeiro momento, entende-se que, para a realidade brasileira, detectar e conter sejam as aplicações mais importantes.

A concepção e o emprego como desafios para a implementação dos sistemas

Segundo Rosa (2023), por mais que o conflito na Ucrânia ainda não permita dirimir interrogações, em especial, no que concerne ao emprego do poder aeroespacial, os drones vem representando uma significativa relação custo-benefício. Para o autor, ainda que esses equipamentos não durem muito tempo, o baixo custo operacional, a capacidade de reconhecimento tático e ofensividade contra alvos definidos são pontos de grande relevância.

> Para os ucranianos, os UAV têm representado uma forma de substituição do poder aéreo convencional, na medida em que buscam utilizar os drones para prover certa falta de consciência situacional, atacar alvos com certa precisão, mesmo à noite, instigar um sentido de resiliência nacional e afetar o moral das tropas russas, o que extrapola o mero significado tático desse tipo de equipamento (ROSA, 2023).

As defesas antidrones têm sido foco dos avanços da tecnologia necessárias ao preparo e emprego das grandes potências mundiais. No segundo semestre de 2022, o Japão comprou 150 mísseis ar-ar de médio alcance, também fornecida à Ucrânia, para ser utilizada por um sistema específico contra a Rússia, de disparo terra-ar. Os sistemas antidrones utilizados nos conflitos armados vão muito além de detecção e contenção. O neutralizar, nesse contexto, não significa apenas o repelir. As ações corretivas levam intencionalmente em conta o fator destruição.

Figura 4 - Drone Octacopter e Granada RKG3 (Ucrânia)

Fonte: https://forcaaerea.com.br

No caso brasileiro, as concepções operacionais ainda permeiam as ações preventivas, havendo espaço para melhorias no que se refere a planejamentos futuros e construções normativas. Como se sabe, mesmo que as áreas de segurança, ou sensíveis, não estejam cobertas por espaços aéreos condicionados, ou seja, aqueles denominados restritos, perigosos ou proibidos, é esperado que os sobrevoos não ocorram sem que haja prévia autorização dos responsáveis pelo local. A ICA 100-40 prevê claramente a possibilidade de neutralização de uma UA quando esta se tratar de ameaça; o que deve ser avaliada é a definição de ameaça.

Acerca dos sobrevoos em áreas militares, já se tem um direcionamento importante que pode servir como doutrina norteadora para a concepção e o emprego de sistemas de defesa contra os drones indesejados. A pauta foi matéria de apreciação da Advocacia-Geral da União (AGU) que, por meio do Parecer nº 00067/2018/CONJUR-MD-CGU-AGU, tratou, na esfera da Consultoria Jurídica Junto ao Ministério da Defesa, unindo, assim, as Consultorias Jurídicas das três Forças Armadas, de fatos que expõem a perigo aparelhamento militar e outros.

Segundo o parecer, em que pese a neutralização seja entendida como erradicação de uma ameaça, restou ratificada a "inaplicabilidade" da Lei nº 9.614/98 (Lei do Abate), que visa ao combate a aeronaves hostis e suspeitas de tráfico, por meio de outra aeronave. Não é possível aplicar os protocolos previstos no Decreto nº 5.144/04 relativos à averiguação, intervenção, persuasão e destruição. Por outro lado, a AGU entende que "qualquer objeto ou pessoas que coloque em risco a segurança de uma Organização Militar, ou do próprio militar, legitima o contra-ataque por parte do agente que identificar a ameaça". O militar deverá agir de maneira proporcional, adequando os meios ao fim, executando a ação em *ultima ratio*, como última alternativa, certo de estar amparado por excludentes de ilicitude previstas no artigo 42 do Código Penal Militar (CPM), que preconiza não haver crime quando

o agente pratica o fato: I - em estado de necessidade; II - em legítima defesa; III - em estrito cumprimento do dever legal; e IV - em exercício regular de direito. Como se vê, não é tão simples a decisão de neutralizar um drone irregular, inesperado ou malicioso, pelo menos no que tange ao abate da aeronave.

Em abril de 2022, o Estudo Preparatório nº 003/COMPREP/2022 também analisou a "mitigação às ameaças pelo acesso irregular de UA em áreas militares". Com fulcro nas normas em vigor nacionais e internacionais, concluiu-se que, quando a Administração Pública Militar age na neutralização de drones ilegais ou invasores, está devidamente investida do poder-dever, repelindo a ameaça à segurança nacional e à incolumidade pública, devido à elevada potencialidade lesiva desses equipamentos. O estudo frisa que uma medida de neutralização, seja pela captura, interceptação ou abate, corresponde a um poder geral de cautela do Estado, que zela pelo espaço aéreo, defesa da pátria e da sociedade. Do mesmo modo, permanecem as recomendações para que as ações se mantenham respaldadas nas excludentes do CPM.

Observações sobre sitemas antidrones e suas capacidades

No tocante aos C-UAS, ou sistemas antridrones, o melhor cenário é a implantação de um equipamento com baixo custo operacional, de fácil manuseio, totalmente eficiente, não vulnerável a contramedidas e que não cause efeitos colaterais a outros sistemas essenciais. Como já foi visto, são vários *layers* propostos pelos fabricantes, contudo, o ideal seria um sistema capaz de detectar, localizar, identificar, bloquear e capturar. Neste momento, já se pode dizer que neutralizar reúne os verbos bloquear, capturar, e até mesmo o destruir ou abater.

Em junho de 2021, o 2º Simpósio de Defesa Anti-SARP, realizado pelo EB na Escola de Artilharia de Costa e Antiaérea (EsACosAAe) no Rio de Janeiro, expôs algumas formas de aplicação dos drones e possíveis contextos referentes aos Sistema de Armas, ou seja, o emprego do drone com armamento de ataque ar-superfície e ar-ar.

Na oportunidade, observou-se que países em conflitos armados já utilizam os Dispositivos Explosivos Improvisados (IED – *Improves Explosive Device*), sendo os artefatos aerotransportados e com significativo poder de destruição. Outro modelo apresentado foi o de Munição de Precisão (PGM – *Precision-Guided Munition*), com o potencial de ser remotamente guiado ao alvo específico. Os drones de "munição vagante" ou *Loitering Munition*, são conhecidos literalmente como "suicidas" ou *Kamikazes*. O *Switchblade* tem sido um desses vagantes

mortais de grande utilização na guerra entre Ucrânia e Rússia. O Enxame de drones, ou *drone swarm*, foi um tema de bastante curiosidade para quem acompanhou o evento, pois o agrupamento de pequenos drones, a partir de sistemas de Inteligência Artificial (IA), pode iniciar um novo cenário aéreo sem precedentes.

Os sistemas de detecção, rastreamento e identificação atuam, na maioria das vezes, nos protocolos dos *links* de comando e controle (*Enlace C2*) entre o Controle Remoto (RC) ou Estação Remota de Pilotagem (RPS) e o drone. É comum a utilização de sistemas que apenas escaneiam espectros de frequência, com o fito de neutralizar o voo, "cortando" o *Enlace*. Com a perda de sinal, o drone pode retornar ao ponto de partida ou local onde está o piloto *(Return To Home)*, ficar pairado no ar *(Hover)* ou apenas pousar *(Landing)*. Na conjuntura da detecção, cabe uma breve classificação dos C-UAS, suas metodologias, vantagens e desvantagens.

O sistema Radar, segundo Lima Filho (2020), age por meio da assinatura radar resultante do encontro entre a UA e pulsos de frequência emitidas pelo sensor. O alcance é de 5 km, e pode ser usado na detecção de grandes quantidades de plotes. Para os "enxames" é um emprego viável. Contudo, há uma certa dificuldade de se detectar drones próximos ao solo.

Considerado um dos mais utilizados no mundo, o sensor de Radiofrequência, de acordo com Narang (2019), atua com o método de varredura das frequências de operação, detectando a posição das aeronaves e dos operadores. Esse sistema requer a linha de visada com o drone e com a RPS, para identificar sua posição, bem como dois sensores no mínimo formando uma triangulação de sinais. Uma vantagem é o baixo custo operacional, porém, em ambientes urbanos é extremamente difícil o isolamento das emissões e suas bandas de comunicação.

No sistema Eletro-Ótico, há a necessidade de utilização de câmera para monitoramento do ambiente. Dessa maneira, o sensor detecta os drones por meio de sua assinatura visual (MICHEL, 2019; NARANG, 2019). A vantagem da ferramenta é a possibilidade de "classificar" alvos, entretanto, sob degradação meteorológica, sua efetividade é reduzida.

O sistema Infravermelho (IR) apresenta assinatura térmica como diferencial, e isso é bom, uma vez que, havendo um banco de dados com assinaturas já conhecidas previamente, fica mais fácil subsidiar a detecção. Em contrapartida, seu alcance é de apenas 100 metros, apresentando também vulnerabilidade quando degradadas as condições meteorológicas. O sensor não costuma ser empregado isoladamente, atuando em conjunto com outros, de forma complementar, principalmente com o eletro-óptico. (LIMA FILHO, 2020, p. 24)

O reconhecimento sonoro, metodologia do sistema Acústico, é pouco conhecido no universo da detecção de drones. Ele que se baseia no ruído produzido pelos motores das aeronaves. Como os microfones são sensíveis, recomenda-se que já se tenha uma biblioteca de sons de drones para adestrar a ação do equipamento. O sistema não é tão eficiente nos ambientes urbanos, assim como não apresenta bons resultados na presença de drones silenciosos.

O *Laser* também é considerado um sistema antidrone, inclusive como técnica de destruição *(hard kill)*. Integrado a outros sistemas de detecção e localização, e após receber informações sobre a direção de onde vem uma ameaça, é esperado que o sistema realize o traqueamento e enquadramento do alvo.

Há sistemas de defesa que empregam equipamentos em concomitância, reunindo dois ou mais instrumentos antidrones. Como cada sistema possui vantagens e desvantagens, quando se juntam as capacidades de detecção, rastreamento e identificação, o sucesso da neutralização se torna mais palpável. Diante disso, uma metodologia recomendada é a Combinação de Sensores.

Uma vez detectadas, localizadas ou identificadas as ameaças não tripuladas, várias podem ser as formas de neutralização, no entanto, os meios cinéticos (que se referem ao deslocamento de um corpo para se chocar ao drone invasor), como projéteis, redes, mísseis ou outros drones nem sempre são as melhores opções, já que podem gerar danos colaterais a terceiros no solo e no ar caso o alvo não seja atingido. Meios não cinéticos são possibilidades operacionais mais plausíveis, ainda mais quando se tratam de falsificações dos sinais *(spoofing)*, interferências de radiofrequências *(jamming)*, até mesmo armamentos emissores de micro-ondas e lasers. Michel (2019) chama a atenção para a técnica do ofuscamento *(dazzling)*, que é a utilização de um feixe de luz para comprometer a câmera de um drone.

Como já dito, uma grande preocupação das autoridades da aviação é a interferência nas frequências de telecomunicações aeronáuticas, nos sensores e auxílios à navegação, por isso, para utilizar sistemas antidrones, seja na detecção ou contenção, é preciso gerenciar os riscos.

Considerações finais

O estudo apontou, preliminarmente, o notório desenvolvimento da aviação como um resultado inevitável do avanço tecnológico. Esse crescimento não ficaria restrito aos meios tripulados, pois, desde que o Homem criou o avião, já se pensava em aeronaves sem tripulação a bordo para missões específicas como as de reconhecimento, observação e ataque. O estudo ressaltou a acelerada evolução dos drones em escala global e, do mesmo modo, no Brasil, como tecnologia disruptiva, que

a cada dia apresenta novas possibilidades operacionais em atividades como topografia, resposta a desastres, inspeção de ativos, inteligência, vigilância, segurança pública e privada, pesquisa, agricultura de precisão, publicidade, dentre outras.

Sendo uma pesquisa qualitativa e de natureza exploratória, a coleta de informações, a partir de bibliografias e casos concretos, considerando disposições jurídico-normativos latentes, permitiu observar que, por mais que haja um vasto rol de legislações nacionais que regulam o tema, há indícios de irregularidades por parte dos usuários. Por vezes, alguns voos de drones são considerados irregulares, desconhecidos e maliciosos, gerando riscos às áreas sensíveis e de segurança, colocando em perigo a segurança orgânica e a incolumidade de seus agentes.

Foram salientados os conceitos de espaço aéreo, ordem pública e segurança pública. Nesse sentido, viu-se que uma ameaça não tripulada pode ao mesmo tempo causar prejuízos à navegação aérea, aos terceiros no solo e às propriedades, assim como perturbar a ordem e ferir os preceitos da segurança coletiva.

O trabalho ressalta o desafio de criar concepções operacionais e formas de emprego de sistemas C-UAS, devido às relações entre custo operacional, capacidades, recursos disponíveis, vantagens e desvantagens. Levou-se em consideração a realidade brasileira, em que esses sistemas são implementados ainda no campo da prevenção, sendo a "detecção" e "contenção" medidas consideradas leves, apenas para repelirem voos indesejados. Contudo, a pesquisa frisou que a neutralização pode ser implementada como um *layer* para destruir a ameaça.

Foram apresentados sistemas antidrones de detecção, como o Radar, Radiofrequência, Eletro-ótico, Infravermelho, Acústico e Laser, além da possibilidade da Combinação de Sensores. Viu-se que é possível utilizar a acústica para guiar um dispositivo que utiliza alcance visual, implementando, por conseguinte, aplicações com radares, sensores de infravermelho e eletro-ópticos. Do mesmo modo, há como empregar detectores de radiofrequência e radares para guiar sensores eletro-ópticos e, a partir da consolidação das informações recebidas em uma central de comando e controle, realizar o traqueamento e enquadramento das ameaças. Ou seja, uma neutralização pode ser mais ou menos severa, a depender de cada cenário operacional.

Observou-se que o emprego de meios contra uma aeronave não tripulada indesejada faz parte do contexto da neutralização. Embora sejam possibilidades operacionais já utilizadas em alguns cenários, esses meios denominados meios cinéticos e não cinéticos devem ser objeto de escolhas planejadas, considerando os prejuízos que possam advir de suas aplicabilidades.

Conquanto não haja legislação específica que regule o tema e o emprego dessas tecnologias, propõe-se a tomada de decisão colaborativa por meio de ações interagências, em que cada envolvido possa efetivamente atuar de acordo com sua área de responsabilidade.

No tocante aos órgãos reguladores do UAS brasileiro, frente às ocorrências nas proximidades dos aeroportos, acredita-se ser possível uma análise mais profunda sobre os meios existentes de detecção e contenção, assim como testes mais eficientes, no sentido de adequar tais sistemas ao cenário da aviação, mitigando os possíveis prejuízos operacionais. Por parte dos órgãos que atuam em prol da preservação da ordem pública e da incolumidade das pessoas e do patrimônio, espera-se que as ações fiscalizatórias não deixem de existir, uma vez que infringir as normas vigentes já configura a irregularidade. Aos responsáveis pelas infraestruturas críticas, áreas sensíveis e de segurança, aconselha-se a coordenação para o estabelecimento das FRZ. Com as zonas de restrição criadas, há de se ter pelo menos um controle sobre os voos solicitados. Diante das abordagens feitas no presente ensaio, o que se vislumbra, por fim, é que o estudo suscite novas reflexões e sirva como fonte de pesquisas para o aprimoramento de trabalhos futuros ou em desenvolvimento sobre a pauta.

Referências

AHMED, F., MOHANTA, J.C., KESHARI, A. *et al. Recent Advances in Unmanned Aerial Vehicles: A Review.* Arabian Journal for Science and Engineering 47:7963–7984 (2022). Disponível em: https://doi.org/10.1007/s13369-022-06738-0. Acesso em 12 maio 2023.

BOWER, J. L.; CHRISTENSEN, C. M. *Disruptive Technologies: Catching the Wave.* Harvard Business Review, p. 43 - 53. 1995.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Tráfego Aéreo. ICA 100-40. Rio de Janeiro, 2023. *Aeronaves Não Tripuladas e o Acesso ao Espaço Aéreo Brasileiro*. Disponível em: https://publicacoes.decea.mil.br. Acesso em 22 jul. 2023.

BRASIL. Agência Nacional de Aviação Civil. RBAC-E nº 94. *Requisitos gerais para aeronaves não tripuladas de uso civil.* 2021. Disponível em: https://www.anac.gov.br/assuntos/legislacao/legislacao-1/rbha-e-rbac/rbac/rbac-e-94. Acesso em 16 maio 2023.

BRASIL. Comando da Aeronáutica. DCA 1-1. *Doutrina Básica da Força Aérea Brasileira.* Vol. I e II. 2020. Disponível em: https://www.sislaer.fab.mil.br. Acesso em 11 maio 2022.

BRASIL. *Decreto nº 5144, de 16 de julho de 2004*. Regulamenta o §§ 1o, 2o e 3o do art. 303 da Lei no 7.565, de 19 de dezembro de 1986, que dispõe sobre o Código Brasileiro de Aeronáutica, no que concerne às aeronaves hostis ou suspeitas de tráfico de substâncias entorpecentes e drogas afins. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2004/Decreto/D5144.htm. Acesso em: 18 out 2023.

BRASIL. *Lei nº 9.614, de 5 de março de 1998*. Altera a Lei nº 7.565, de 19 de dezembro de 1986, para incluir hipótese destruição de aeronave. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L9614.htm . Acesso em: 18 out 2023.

BRASIL. *Decreto-Lei nº 1001, de 21 de outubro de 1969.* Código Penal Militar. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del1001.htm#:~:text=Os%20militares%20estrangeiros%2C%20quando%20em,em%20tratados%20ou%20conven%C3%A7%C3%B5es%20internacionais.&text=Art.,-12. Acesso em: 18 out 2023.

CANADA. International Civil Aviation Organization. *Manual on Remotely Piloted*

Aircraft Systems (RPAS). Doc 10019. 1st. ed. Montreal, 2015. Disponível em: https://store.icao.int/en/manual-on-remotely-piloted-aircraft-systems-rpas-doc-10019. Acesso em 18 maio 2023.

CHERNOVA, Anna; SHUKLA, Seb. *Kremlin says Ukraine is behind May 3 drone attacks on Moscow.* Londres. 2023. Disponível em: https://edition.cnn.com/europe/live-news/russia-ukraine-war-news-05-25-23#h_f95f41e145ffed2a0eb58f56b266e6ee. Acesso em 25 maio 2023.

CHRISTENSEN, C. M. *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail.* Boston, Mass.: Harvard Business School Press, 1997.

DOUGHERTY, Martin J. *Drones:* Guia das Aeronaves Não Tripuladas que Estão Tomando Conta de Nossos Céus. São Paulo: M.Books do Brasil Editora, 2019.

DOUHET, G. G. *O Domínio do Ar.* Tradução: Escola de Aperfeiçoamento de Oficiais da Aeronáutica. Brasília, DF: Editora Italiana Limitada, 1978. Instituto Histórico-Cultural da Aeronáutica. (Coleção Aeronáutica. Arte Militar e Poder Aeroespacial, v. 2).

HAMBLING, David. *Swarm troopers:* como os pequenos drones irão conquistar o mundo. Tradução: Paulo Baciuk - Rio de Janeiro: Biblioteca do Exército, 2018.

IGBAL, Mohammad. *Use of Dynamic Remotely Operated Navigation Equipment (DRONE) in Geographical and Environmental Research:* Bangladeshi Perspectives. 2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3922387. Acesso em 18 mar. 2023.

LESSA, Sávio. Artigo: *O que é Segurança Pública?* Portal Amazômia. 2021. Disponível em: https://portalamazonia.com/seguranca-publica-e-cidadania/artigo-o-que-e-seguranca-publica-1. Acesso em 12 mar. 2023.

LIMA FILHO, Paulo Davi de Barros. *A defesa anti-SARP na Força Terrestre.* Trabalho de Conclusão de Curso (Especialização em Ciências Militares). Curso de Comando e Estado-Maior (ECEME): Rio de Janeiro, Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/8868/1/MO%206310%20-%20BARROS%20LIMA.pdf. Acesso em 20 maio 2023.

MESQUITA, Ivan Muniz. *O Poder Aeroespacial e a Estratégia Nacional de Defesa (END)*. Revista da Escola Superior de Guerra, v. 33, n. 67, p. 82-97, jan./abr. 2018. Disponível em: https://revista.esg.br/index.php/revistadaesg/article/view/908. Acesso em 18 maio

2023.

MICHEL, Arthur Holland. *Counter-drone systems.* Washington D.C., 2019. Disponível em: https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-EditionWeb.pdf.

NARANG, R. K. *Armed sUAS Swarm: Big Threat of Small UAS–C-sUAS Development and Threat Mitigation by India.* Asian Defence Review, p. 75–100, 2019. Disponível em: http://im.rediff.com/news/2021/jul/armedsuasswarmbigthreatofsmalluas.pdf Acesso em 20 maio 2023.

RIBEIRO, Leonardo Serra et al. *Possibilidade de emprego de atuadores não cinéticos na defesa antiaérea contra aeronaves remotamente pilotadas.* 2018. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/3491/1/TCC_Cap%20Serra.pdf. Acesso em 22 abr. 2022.

ROSA, Carlos Eduardo Valle. *Poder Aeroespacial na guerra da Ucrânia.* 2023. Disponível em: https://velhogeneral.com.br/2023/04/04/poder-aeroespacial-na-guerra-da-ucrania. Acesso em 12 maio 2023.

ROSA, Carlos Eduardo Valle. *Geopolítica Aeroespacial: Conhecimento Geográfico e Abordagem Estratégica*. São Paulo: Editora Dialética, 2022.

ROSA, Carlos Eduardo Valle. *Poder Aéreo - Guia de Estudos.* 1ª Ed. Rio de Janeiro: Luzes, 2014.

SILVA, Eduardo Araújo. *Operações Aéreas Especiais:* Drones, Busca e Salvamento e Resposta a Desastres. Monografia (Bacharelado em Segurança Pública e Social). DSP/InEAC/UFF. Rio de Janeiro, 2023.

STAMATE, Mihai-Alin; PUPAZA Cristina; NICOLESCU, Florin-Adrian; MOLDOVEANU, Cristian-Emil. *Improvement of Hexacopter UAVs Attitude Parameters Employing Control and Decision Support Systems.* 2023. Disponível em: https://www.mdpi.com/1424-8220/23/3/1446. Acesso em 11 maio 2023.

Drone perto da pista do Aeroporto em Guarulhos suspende pousos e decolagens. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2023/03/26/drone-perto-da-pista-do-aeroporto-em-guarulhos-suspende-pousos-e-decolagens.ghtml. Acesso em: 18 out. 2023

Chegada dos caças Gripen em porto brasileiro é captada por drones. Disponível em: https://aeroin.net/chegada-dos-cacas-gripen-em-porto-brasileiro-e-captada-por-drones/. Acesso

em: 18 out. 2023

Casal é preso suspeito de usar drone para arremessar celulares e drogas para presídio, na Grande BH. Disponível em: https://g1.globo.com/mg/minas-gerais/noticia/2023/04/05/casal-e-preso-suspeito-de-usar-drone-para-arremessar-celulares-e-drogas-para-presidio-na-grande-bh.ghtml. Acesso em: 18 out. 2023.

Artigo

11

ATIVIDADE DE INTELIGÊNCIA APLICADA À GESTÃO DA POLÍTICA DE SOCIOEDUCAÇÃO NO BRASIL: reflexões preliminares

DOI: https://doi.org/10.58960/rbi.2023.18.233

Ricardo Peres Costa *
Jeremias dos Santos **

Resumo

Este artigo descreve a importância da Atividade de Inteligência aplicada à gestão da política de Socioeducação no Brasil. A análise está sustentada numa perspectiva teórico-metodológica de pesquisa documental, de abordagem descritiva e observação assistemática, fruto de experiências vividas pelos autores na gestão do sistema socioeducativo, em particular do Instituto de Atendimento Socioeducativo do Estado do Espírito Santo (Iases). Discute-se a aplicabilidade da Atividade de Inteligência, baseadas nos seus princípios, fundamentos e metodologias próprias, em subsídios aos planejamentos e ações preventivas, na manutenção da ordem e da segurança nas unidades socioeducativas. Conclui-se que, juntamente com outras ações, estratégias e outros projetos pedagógicos, a Atividade pode contribuir para um ambiente adequado ao desenvolvimento das rotinas previstas e necessárias à concretização da finalidade precípua da Socioeducação.

Palavras-chave: sistema socioeducativo; Atividade de Inteligência; adolescentes em conflito com a lei.

INTELLIGENCE ACTIVITY APPLIED TO THE MANAGEMENT OF SOCIO-EDUCATION POLICY IN BRAZIL: preliminary reflections

Abstract

This article describes the importance of Intelligence activity applied to the management of socio-education policy in Brazil. The analysis is based on a theoretical-methodological perspective of documentary research, with a descriptive approach and unsystematic observation, the result of experiences lived by the authors in the management of the socio-educational system, in particular the Institute of Socio-Educational Assistance of the State of Espírito Santo (Iases). The applicability of the Intelligence activity is discussed, based on its own principles, fundamentals and methodologies, in subsidies for planning and preventive actions, in the maintenance of order and security in socio-educational units. It is concluded that, together with other actions, strategies and pedagogical projects, the activity can contribute to an adequate environment for the development of the foreseen and necessary routines to materialize the main purpose of Socio-education.

***Keywords*:** *Socioeducational system; Intelligence activity; young people in conflict with the law.*

* Especialista em Educação, Pobreza e Desigualdade Social pela Universidade Federal do Paraná (UFPR). Mestre e Doutor em Serviço Social e Política Social pela Universidade Estadual de Londrina/PR (UEL/PR). Pesquisador na área de socioeducação na Texas Tech University.

** Especialista em Gestão e Políticas de Segurança Pública pela Universidade Federal do Espírito Santo (UFES) e em Ciências Criminais pela Universidade do Amazonas (UNAMA/LFG). Mestre em Segurança Pública pela Universidade de Vila Velha (UVV). Coautor do livro Tratado de Inteligência Aplicada à Investigação Criminal. Delegado de Polícia (PCES).

ACTIVIDAD DE INTELIGENCIA APLICADA A LA GESTIÓN DE LA POLÍTICA SOCIOEDUCATIVA EN BRASIL: reflexiones preliminares

Resumen

Este artículo describe la importancia de la actividad de Inteligencia aplicada a la gestión de la política socioeducativa en Brasil. El análisis se sustenta en una perspectiva teórico-metodológica de investigación documental, con enfoque descriptivo y observación no sistemática, fruto de las experiencias vividas por los autores en la gestión del sistema socioeducativo, en particular del Instituto de Asistencia Socioeducativa de el Estado de Espíritu Santo (Iases). Se discute la aplicabilidad de la actividad de Inteligencia, a partir de sus propios principios, fundamentos y metodologías, en los subsidios para la planificación y acciones preventivas, en el mantenimiento del orden y la seguridad en las unidades socioeducativas. Se concluye que, junto con otras acciones, estrategias y proyectos pedagógicos, la actividad puede contribuir a un ambiente adecuado para el desarrollo de las rutinas previstas y necesarias para materializar el propósito principal de la Socioeducación.

Palabras clave: *sistema socioeducativo; actividad de inteligencia; adolescentes en conflicto con la ley.*

Introdução

A política destinada ao adolescente autor de ato infracional e sentenciado ao cumprimento de uma medida socioeducativa é intitulada de Socioeducação. É uma política pública demandada pela União em articulação com estados e municípios que executam os serviços e programas que visam a cumprir a decisão judicial mediante sentença estabelecida aos adolescentes que cometeram ato infracional e foram responsabilizados com a privação, a restrição de liberdade ou uma das medidas em meio aberto.

Esta previsão legal está registrada no Estatuto da Criança e do Adolescente, Lei federal nº 8.069/1990 e, mais recentemente, na Lei nº 12.594, de 18 de janeiro de 2012, que instituiu o Sistema Nacional de Atendimento Socioeducativo (Sinase) e regulamentou a execução das medidas socioeducativas destinadas a adolescentes que praticaram atos infracionais.

Neste diapasão, este artigo parte da análise de que a Atividade de Inteligência no Sistema Socioeducativo é uma matéria ainda em franco desenvolvimento e implantação e, por vezes, vista com certa ressalva ou preconceito por aqueles que fazem a gestão do sistema.

As Atividades de Inteligência foram estruturadas pela Lei nº 9.883, de 17 de dezembro de 1999, que instituiu o Sistema Brasileiro de Inteligência (Sisbin) e estabeleceu a Agência Brasileira de Inteligência (Abin) como o seu órgão central, com o encargo de planejar, executar, coordenar, supervisionar e controlar essas atividades (BRASIL, 1999). Dessa forma, partimos do reconhecimento que a Atividade de Inteligência pode ser uma ferramenta importante para o exercício permanente e sistemático de ações especializadas para identificação, acompanhamento e avaliação de ameaças reais ou potenciais no âmbito da execução de um programa socioeducativo.

A escassez de artigos neste periódico vinculado à Escola de Inteligência (Esint) da Abin e em outros periódicos temáticos sobre a disseminação de estudos, reflexões e debates acerca de temas relacionados com a Atividade de Inteligência na Socioeducação é a expressão de que ainda temos muito a desenvolver neste campo de pesquisa voltado à produção de conhecimentos sobre medidas socioeducativas, em especial, de privação de liberdade.

Para sustentar a análise, adotamos a perspectiva teórico-metodológica de pesquisa bibliográfica e abordagem descritiva. Algumas informações ou abstrações da realidade são, enfim, fruto de observação assistemática, livre, executada de forma direta e carregada de subjetividades durante visitas a unidades socioeducativas, em contato informal

com agentes da Socioeducação e da rede de execução das medidas socioeducativas.

O texto está organizado em duas seções: a primeira procura brevemente descrever os marcos legais do Sinase, os dados de uma realidade que exigem ações de segurança preventiva e interventiva e a descrição de algumas experiências de Núcleos, Coordenações e Divisões de Inteligência Socioeducativa. Na última seção, procura-se demonstrar que a Atividade de Inteligência nas Unidades Socioeducativas pode ser compreendida como toda e qualquer ação que, durante a rotina de trabalho, busque captar informações para melhor executar a medida socioeducativa.

Sistema nacional de atendimento socioeducativo e a integração com as demais políticas

O Sistema Nacional de Atendimento Socioeducativo (Sinase) foi instituído pela Lei nº 12.594, de 18 de janeiro de 2012, e tem por finalidade regulamentar a execução das medidas socioeducativas destinadas a adolescente que pratique ato infracional. No seu artigo 1º, § 1º, a referida lei conceitua sobre o entendimento de Sinase, conforme a seguir:

> Entende-se por Sinase o conjunto ordenado de princípios, regras e critérios que envolvem a execução de medidas socioeducativas, incluindo-se nele, por adesão, os sistemas estaduais, distrital e municipais, bem como todos os planos, políticas e programas específicos de atendimento a adolescente em conflito com a lei (BRASIL, 2012, Art. 1º).

Outra derivação conceitual é a palavra Socioeducação, que é o termo utilizado para se denominar a política de atendimento de adolescentes em conflito com a lei no Brasil, mediante a execução de umas das seis medidas socioeducativas previstas no artigo 112 da Lei nº 8.069, de 13 de julho de 1990. Os objetivos específicos foram consignados na previsão legal do artigo 1º, § 2º, da Lei 12.594/12, conforme a seguir:

> I - a responsabilização do adolescente quanto às consequências lesivas do ato infracional, sempre que possível incentivando a sua reparação; II - a integração social do adolescente e a garantia de seus direitos individuais e sociais, por meio do cumprimento de seu plano individual de atendimento; e III - a desaprovação da conduta infracional, efetivando as disposições da sentença como parâmetro máximo de privação de liberdade ou restrição de direitos, observados os limites previstos em lei (BRASIL, 2012, Art. 1º).

O marco legal nos possibilita refletir e contextualizar que a política de Socioeducação deve ser executada de forma integrada junto aos entes federados. Estados e municípios gozam de certa autonomia sobre a organização da política local do atendimento socioeducativo, mas, enquanto participantes do Sinase (Art. 1° §1° da Lei nº 12.594/2012), devem seguir as linhas estratégicas previstas para a política no âmbito nacional, conforme designado no Art. 7° da Lei nº12.594/2012.

Notadamente em relação à segurança e à integridade no que concerne aos

direitos e garantias dos adolescentes em cumprimento de medida privativa de liberdade na modalidade internação, algumas ações devem ser planejadas e contar com as atribuições e competências transversais dos órgãos afetos à segurança dos indivíduos no seio da sociedade.

Prescreve a Lei nº 12.594/2012 que os programas de atendimento deverão ser inscritos no Conselho Estadual ou Distrital dos Direitos da Criança e do Adolescente e, conforme o caso, como um dos requisitos obrigatórios, além da especificação do regime, apresentar a indicação da estrutura material, dos recursos humanos e das estratégias de segurança, conforme Art. 11, inciso II, compatíveis com as necessidades do respectivo programa socioeducativo. Desta citada obrigação, extrai-se ser dever da gestão socioeducativa ter um plano estratégico e tático de segurança socioeducativa.

A segurança socioeducativa sempre, e ainda mais quando associada à Atividade de Inteligência, poderá ser instrumento para melhorar a qualidade no assessoramento da gestão, e pode garantir, por exemplo, o que prescreve o inciso II, do § 2º, artigo 1º da Lei do Sinase: "II - a integração social do adolescente e a garantia de seus direitos individuais e sociais, por meio do cumprimento de seu plano individual de atendimento" (BRASIL, 2012, Art. 1º).

Algumas pesquisas demonstram que, em determinadas unidades de cumprimento da medida socioeducativa de internação, adolescentes são separados, muitas vezes isolados, sob o pretexto de se preservar a sua integridade física, evitar confrontos e agressões mútuas entre adolescentes.

Apesar dos poucos estudos realizados sobre o tema, algumas pesquisas (NERI, 2009; MALLART, 2014; PAIVA, 2019; AVILAR, FERNANDES, 2019; NASCIMENTO, FERNANDES, 2019; MIRANDA, PAIVA, 2019; LEITE & BEZERRA, 2019; SILVA, 2020) apontam que as unidades socioeducativas têm sofrido mudanças no clima organizacional em razão da influência que as facções criminosas têm despertado nos adolescentes. Essa interferência externa trouxe reflexos ao *modus operandi* dos adolescentes, já que essas dinâmicas, outrora comuns apenas no sistema prisional, passaram a ser reproduzidas pelos socioeducandos no interior das unidades.

Não se nega a existência destas realidades. Inclusive, iniciativas de Norte a Sul do país têm sido realizadas para despertar os agentes envolvidos com a rede socioeducativa sobre a necessidade de melhor compreender e definir estratégias de enfrentamento e superação.[1] A esse respeito, a Lei do

1 "Iases capacita servidores em Atividade de Inteligência" (IASES, 2017); "Tem início seminário que debate a segurança na socioeducação" (CNMP, 2017); "Profissionais debatem procedimentos de segurança e inteligência na socioeducação" (FASEPA, 2019); "SJSPS promove seminário sobre a relevância do sistema de inteligência no sistema prisional e socioeducativo" (REGINATO, 2022); "Capacitação sobre Inteligência mobiliza profissionais de segurança de Minas e mais seis estados" (AGÊNCIA MINAS, 2022).

SINASE, no seu Artigo 48, § 2º, dispõe:

> É vedada a aplicação de sanção disciplinar de isolamento a adolescente interno, exceto seja essa imprescindível para garantia da segurança de outros internos ou do próprio adolescente a quem seja imposta a sanção, sendo necessária ainda comunicação ao defensor, ao Ministério Público e à autoridade judiciária em até 24 (vinte e quatro) horas (BRASIL, 2012, Art. 48º).

Verifica-se que, para a garantia plena da integridade do adolescente ou de outrem, a redação é clara quando menciona o princípio da brevidade e da excepcionalidade, e dá a entender que, em casos específicos, o procedimento poderá ser executado para a resguarda do indivíduo.

O programa de privação de liberdade e semiliberdade tem requisitos específicos para a inscrição, entre estes, a definição das estratégias para a gestão de conflitos, vedada a previsão de isolamento cautelar, exceto nos casos previstos em lei. A direção do estabelecimento socioeducativo deve adotar, em caráter excepcional, medidas para proteção do interno em casos de risco à sua integridade física, à sua vida, ou à de outrem, comunicando, de imediato, o sistema de Justiça.

Não se pode admitir que fatos excepcionais sejam a regra, por dois motivos principais: primeiro, que não se estaria proporcionando ao socioeducando a possibilidade de integração social e a garantia dos seus direitos individuais e sociais, segundo, uma decisão de gestão que admite se invocar a todo o momento a exceção supramencionada, admite o próprio fracasso da efetividade de medida socioeducativa. A gestão do programa de atendimento deve pautar as suas ações na proposta pedagógica, que pode oferecer elementos de segurança preventiva e evitar situações de segurança interventiva.

Dispõem os marcos legais que o Sinase é coordenado pela União e integrado aos demais sistemas responsáveis pela execução das medidas socioeducativas. A Resolução nº 119 recomendou e a Lei nº 12.594/2012 estabeleceu, no seu artigo 3º, parágrafo 3º, que à Secretaria de Direitos Humanos da Presidência da República (SDH/PR) competem as funções executiva e de gestão do Sinase, em integração operacional com as demais políticas setoriais e com demais entes federativos (BRASIL, 2012).

Neste aspecto, a previsão é expressa para que todos os sistemas nacionais de operacionalização de políticas públicas, especialmente nas áreas da saúde, educação, assistência social, trabalho e segurança pública devem integrar a proposta de atenção ao adolescente em cumprimento de medida socioeducativa.

Além da Lei nº 12.594 de 2012, outros documentos orientadores, a exemplo das Resoluções nº 113 e 119, de 2006, expedidas pelo Conselho Nacional dos Direitos da Criança e do Adolescente (Conanda), tratam da expressa necessidade de integrar um sistema de garantia de

direitos para estes adolescentes e jovens.

A resolução nº 113, de 19 de abril de 2006, expedida pelo Conanda, dispõe sobre os parâmetros para a institucionalização e o fortalecimento do Sistema de Garantia dos Direitos da Criança e do Adolescente. Quanto à sua configuração, dispõe o artigo 1º:

> O Sistema de Garantia dos Direitos da Criança e do Adolescente constitui-se na articulação e integração das instâncias públicas governamentais e da sociedade civil, na aplicação de instrumentos normativos e no funcionamento dos mecanismos de promoção, defesa e controle para a efetivação dos direitos humanos da criança e do adolescente, nos níveis Federal, Estadual, Distrital e Municipal (CONANDA, 2006a).

Enquanto o parágrafo primeiro destaca que o sistema articular-se-á com todos os sistemas nacionais de operacionalização de políticas públicas, o que se tem observado, ao menos de modo assistemático, é que, embora, taxativamente, o citado dispositivo preveja articulação com as forças de segurança pública, alguns atores desta política resistem, especialmente, quando se trata de dialogar com agentes vinculados às agências de Inteligência.

Por certo, desconhecem a previsão legal, a natureza e a competência da Abin: "As Atividades de Inteligência serão desenvolvidas, no que se refere aos limites de sua extensão e ao uso de técnicas e meios sigilosos, em observância aos direitos e às garantias individuais e com fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado" (BRASIL, 1999, Art. 3º).

A questão que se apresenta é a seguinte: quando se trata de abordar o tema integração com o Sistema de Segurança, existe, declaradamente, alguma resistência, muito possível por equívoco de interpretação ou preconceito.

Importa mencionar que, conforme a mesma lei (BRASIL, 1999), entende-se como Inteligência a Atividade que objetiva a obtenção, a análise e a 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, sobre a salvaguarda e a segurança da sociedade e do Estado, com a finalidade de assessorar a tomada de decisão política, estratégica, tática ou operacional, através do conhecimento de informações sobre o tema.

Dessa forma, a integração entre os órgãos correlatos à execução de medida socioeducativa é ainda mais necessária, pois o pleno funcionamento da atividade depende de integração e de um profícuo fluxo de informações para que se alcance a missão e se consiga antecipar e produzir conhecimento para assessoramento ao processo decisório dos gestores.

Alguns dados da realidade

O arcabouço jurídico definiu que uma unidade socioeducativa é a base física necessária para a organização e o funcionamento de um programa de atendimento (BRASIL, 2012, Art. 1.º § 4.º). Segundo os dados do Levantamento Anual Sinase 2017, naquele ano, existiam "484 unidades de atendimento socioeducativo no país, considerando as modalidades de atendimento de internação, internação provisória, semiliberdade, internação sanção e atendimento inicial" (BRASIL, 2019, p. 64).

É neste universo caracterizado no espectro das estruturas arquitetônicas como muralhas, grades, cercas, concertinas, quadrantes delimitadores, controle de acesso, câmeras de vídeo monitoramento, celas, portas, cadeados, salas de aulas, ginásio, alas, dormitórios, corredores, setores administrativos, técnicos, de segurança (COSTA, 2020) que se constituem centros socioeducativos pelo Brasil. Uns mais equipados, outros nem tanto.

Não raro, são registradas, em várias unidades de atendimento socioeducativo pelo Brasil, conflitos entre adolescentes, agressividade contra agentes de segurança socioeducativo, motins e rebeliões que causam danos materiais nas unidades, depredação do patrimônio público, agressões entre adolescentes e agentes e, inclusive, alguns óbitos.

Na Pesquisa do Levantamento Anual do Sinase, foi sistematizado que "46 adolescentes vinculados às Unidades de Atendimento Socioeducativo em privação e restrição de liberdade foram a óbito" em 2017 (BRASIL, 2019, p. 58), e a região Nordeste[2] figura com o maior índice, 51% da totalidade que equivale a 25 casos.

Os relatos são inúmeros e quase todos os estados já passaram por essa realidade crítica. Se considerarmos dados dos últimos cinco anos, encontraremos inúmeras notícias: Paraíba[3], Ceará[4] sofrem com esses eventos anualmente desde 2008; Piauí, Rondônia, Minas Gerais, Rio de Janeiro, São Paulo, Mato Grosso do Sul e o Distrito Federal têm registros de óbitos e motins.

Os desafios a qualquer Atividade de Inteligência, de segurança preventiva ou interventiva é, de certa forma, sucumbida quando as instituições estão neste caos de superlotação:

> O Case de Caruaru tem capacidade para

2 Para exemplificar a situação na região, em 2016, sete adolescentes foram mortos durante rebelião na Funase da cidade de Caruaru/PE. Entre as vítimas, uma foi decapitada, enquanto as demais morreram carbonizadas por um incêndio provocado pelos internos, que atearam fogo aos colchões. Em quase todos os casos, o órgão gestor alega de forma genérica que as determinações foram em decorrência de brigas entre grupos rivais (DIÁRIO DE PERNAMBUCO, 2016).

3 No estado do Paraíba, sete adolescentes foram mortos em meados de 2017 durante uma rebelião dentro de unidade de internação conhecida como Lar dos Garotos.

4 Segundo nota pública do Cedeca Ceará de outubro de 2019, já era a oitava morte em unidades do sistema socioeducativo do Ceará desde novembro de 2017 (CEDECA, 2019).

> 90 adolescentes. Antes da rebelião, estava com 160 jovens. [...] Com capacidade para receber 98 adolescentes, a Funase de Abreu e Lima abrigava 285 pessoas. [...] Na terça-feira passada, uma rebelião registrada na unidade da Funase de Timbaúba, Zona da Mata Norte de Pernambuco, deixou quatro adolescentes mortos. Durante a rebelião, os internos queimaram móveis e colchões. O prédio foi danificado (DIÁRIO DE PERNAMBUCO, 2016, p. 2).

O fato é que não se pode ignorar esses eventos críticos nas unidades socioeducativas e, com eles, deve-se agir de forma especializada. "A crise, pela sua natureza e capacidade de comprometer infraestruturas críticas e direitos fundamentais, deve possuir um tratamento especial" (MONTAGNA, 2022, p. 8). A Atividade de Inteligência pode contribuir para que medidas preventivas sejam implementadas e esses eventos não venham a ocorrer.

Todavia, em ambientes com alto nível de tensão, violência e agressividade, torna-se inviável a aplicação do programa previsto pelas equipes técnicas profissionais, planos táticos não são executados, rotinas pedagógicas são suspensas ou canceladas e, por consequência, não se pode alcançar a efetiva Socioeducação. Estudos e pesquisas, ainda que escassos, demonstram que a reincidência é uma realidade (COSTA, 2020).

Vários fatores podem contribuir para isso; contudo, não se pode ter dúvidas de que o cumprimento da medida socioeducativa de internação em ambiente hostil, violento e inadequado não pode propiciar ao socioeducando o atingimento das suas metas, da mesma forma que profissionais técnicos nestes mesmos ambientes não poderão desenvolver as suas habilidades e competências na plenitude.

Diversos episódios e situações evidenciam uma transformação social na maneira de se relacionar e executar determinadas rotinas nas unidades de socioeducação. Uma série de novos problemas sociais surge na vida cotidiana de moradores das periferias, em virtude da existência de facções criminosas que contribuem para a produção organizacional de uma sujeição criminal (MISSE, 2006), e, aparentemente, aspectos dessa nova governança do crime têm impactado também a regulação da vida na privação de liberdade de adolescentes. A compreensão dessa complexidade e as suas composições nos diferentes contextos de privação de liberdade se impõem como um desafio (PAIVA, 2019).

Por isso, a importância de se ter estratégias de ações de segurança preventiva, subsidiadas com Atividades de Inteligência, para, junto com as demais ações, possa-se ter uma unidade de cumprimento de medida socioeducativa de internação estabilizada, que respeite direitos, previna danos de todas as espécies e garanta a toda a comunidade socioeducativa uma convivência harmônica, saudável e segura, onde se possa desenvolver e se efetivar estas medidas.

Em face de uma crise aguda, crítica e danosa à vida e ao patrimônio, a comunicação oficial para a imprensa, familiares, organizações sociais que atuam nas unidades como as igrejas ou conselhos é fundamental. "Em qualquer gabinete de crise um dos segmentos mais importantes é o responsável pela comunicação com a mídia" (MONTAGNA, 2022, p. 12).

Segundo o Sinese (CONANDA, 2006), são três os níveis em que se deve adotar medidas de segurança para a garantia das integridades física, psicológica e moral dos adolescentes: (i) no relacionamento entre os adolescentes; (ii) no relacionamento dos adolescentes com os profissionais; e (iii) no relacionamento dos adolescentes com a realidade externa.

E, nesta lógica, deduz-se que a Inteligência pode agir ao antecipar ocorrências de rebeliões, fugas, tomadas de reféns ou entradas de materiais ilícitos no interior da unidade socioeducativa, e proporcionar condições estáveis à administração socioeducativa e aos demais órgãos, como o de segurança pública.

Algumas experiências de Núcleos, Coordenações e Divisões de Inteligência na Socioeducação

Diante de contextos adversos em algumas Unidades da Federação durante o período de 2016-2017, a Coordenação Geral do Sinase, instância vinculada à Secretaria Nacional dos Direitos da Criança e do Adolescente, órgão do Ministério de Direitos Humanos, realizou reuniões técnicas, encontros e seminários com o Fórum Nacional de Dirigentes Governamentais de Entidades Executoras de Políticas de Promoção e Defesa da Criança e do Adolescente (Fonacriad), Conselho Nacional do Ministério Público (CNMP), Conselho Nacional de Justiça (CNJ), Secretaria Nacional de Segurança Pública (Senasp), entre outros parceiros e especialistas dedicados a debater a Segurança na Socioeducação e o uso da Atividade de Inteligência.

O CNMP promoveu o "Seminário Perspectiva de Segurança na Socioeducação" em agosto de 2017, em que tratou da Atividade de Inteligência na Socioeducação: uma possibilidade para segurança e proteção à comunidade socioeducativa.

A discussão do tema da Atividade de Inteligência aliada à segurança socioeducativa foi iniciada. Contudo, o universo socioeducativo ainda carregado de preconceitos inibiu o avanço de produção de protocolos, parâmetros e diálogos, inclusive com a Abin e com o Subsistema de Inteligência de Segurança Pública (Sisp) dos estados e do Distrito Federal. Algumas iniciativas em âmbito estadual foram realizadas, p. ex., encontros, cursos e a criação de Núcleos, Coordenações ou Divisões de Inteligência aplicada à gestão

da Socioeducação. Espírito Santo, Rio de Janeiro, Santa Catariana, Minas Gerais e o Distrito Federal já implementaram ou reconhecem a necessidade de fazer uso da Inteligência na Socioeducação.

No Instituto de Atendimento Socioeducativo (Iases), existe a Instrução de Serviço nº 0585-P, de 30 de novembro de 2017, que dispôs sobre o Sistema de Inteligência Socioeducativa no Iases (SIIASES); no Rio de Janeiro existe a Coordenadoria de Segurança e Inteligência do Degase (CSINT); no Distrito Federal, existem os Núcleos de Inteligência nas unidades socioeducativas e no âmbito da gestão do sistema; em Minas Gerais foi criada, no âmbito da Subsecretaria de Atendimento Socioeducativo (Suase), a Agência Central de inteligência Socioeducativa (Acis); em Santa Catarina, criou-se a Divisão de Inteligência Socioeducativa (Dise), subordinada diretamente à Gerência de Inteligência (Geint) da Diretoria de Inteligência e Informação (Dinf).

No estado do Espírito Santo, o movimento de reconhecimento e institucionalização iniciou-se em outubro de 2016, quando novos gestores assumiram a Diretoria de Ações Estratégicas (DAE) do Iases. Esta diretoria é responsável, entre outras atribuições, pelas Atividades de Inteligência e segurança socioeducativa. Inicialmente, ocorreram debates internos com os demais diretores e gerentes de unidades socioeducativas do Iases. Os conceitos, princípios, fundamentos e metodologia da Atividade de Inteligência foram sendo incorporados à gestão central e às unidades socioeducativas do estado.

Quase um ano depois, conseguiu-se visualizar os resultados obtidos com destaque para a redução de violência, depredações, motins e rebeliões, e, consequentemente, aumento dos atendimentos pelas equipes técnicas, convívio na escola e na frequência de cursos profissionalizantes.

Em primeiro de dezembro do ano de 2017, foi publicado, no Diário Oficial do Estado do Espírito Santo, o Sistema de Inteligência Socioeducativa do Instituto de Atendimento Socioeducativo (SIIASES), pela Instrução de Serviço nº 0585-P, de 30 de novembro de 2017. Neste documento, está previsto que:

> A Atividade de Inteligência socioeducativa do Iases é o exercício permanente e sistemático de ações especializadas para identificação, acompanhamento e avaliação de ameaças reais ou potenciais no âmbito da Socioeducação, orientadas para produção e salvaguarda de conhecimentos necessários para assessorar o Iases na tomada de decisões, para o planejamento e execução de uma política socioeducativa, prevenindo atos que atentem à segurança e proteção da comunidade socioeducativa e da sociedade (IASES, 2017, Art. 3.º).

Com isso, a Atividade de Inteligência socioeducativa do Iases passa a ser conceituada, e inicia-se também um processo histórico que contribuirá para

adoção da Atividade em outros órgãos socioeducativos dos estados. A experiência do Espírito Santo também é realizada no Rio de Janeiro, que possui a Coordenadoria de Segurança e Inteligência (CSINT).

Importante destaque foi o reconhecimento da Atividade de Inteligência no Sistema Socioeducativo, o que fica fortalecido com acordos de cooperação e parcerias, especialmente com a Secretaria de Segurança Pública em capacitações, entre outras iniciativas, sempre de acordo com a estrita observância aos preceitos legais e doutrinários.

Em Santa Catarina, no Departamento de Administração Socioeducativa (Dease), vinculado à Secretaria de Estado da Administração Prisional e Socioeducativa, foi publicado o Decreto nº 2.379, em dezembro de 2022, que aprovou o Regimento Interno da Secretaria de Estado da Administração Prisional e Socioeducativa e estabeleceu dentre outras providências sobre o tema de interesse deste artigo:

> Art. 39. À Divisão de Inteligência Socioeducativa (DISE), subordinada diretamente à GEINT, compete: I – compilar, controlar e analisar dados de inteligência referentes ao sistema socioeducativo, submetendo-os à apreciação da GEINT; II – intermediar as ações da DINF e dos órgãos de inteligência previstos no Decreto nº 1.778, de 2022, e em alterações posteriores; e III – exercer outras Atividades de Inteligência determinadas pela GEINT no âmbito do sistema socioeducativo (SANTA CATARINA, 2022, p. 22-23).

O Distrito Federal organizou Núcleos de Inteligência nas unidades socioeducativas. No âmbito da gestão do sistema, publicou o Decreto nº 37.896, de 27 de dezembro de 2016, que aprovou o Regimento Interno da Secretaria de Estado de Políticas para Crianças, Adolescentes e Juventude do Distrito Federal. Esse decreto previu, no artigo 10, que a Unidade de Inteligência é de assessoramento superior, subordinada diretamente ao Secretário de Estado e possui como competência:

> I- planejar, orientar, integrar, supervisionar e coordenar as Atividades de Inteligência do Sistema Socioeducativo, respeitadas as peculiaridades e a autonomia dos órgãos que compõem esse sistema; [...] V- produzir conhecimentos de inteligência para subsidiar a elaboração de diretrizes e planos operacionais para os programas, projetos e atividades da Secretaria (DISTRITO FEDERAL, 2016, Art. 10º).

Neste sentido, a Atividade de Inteligência na socioeducação tem se constituído, cada vez mais, como uma ferramenta de gestão. O seu exercício diário de captação, extração e socialização de informações não deve ser desempenhado exclusivamente pelos agentes socioeducativos, mas por todos os membros do corpo funcional. Ou seja, a Atividade subsidia a gestão para garantir a existência de uma segurança preventiva que contribua para a tomada de decisão, para a pactuação, a elaboração e a execução dos instrumentos pedagógicos do programa socioeducativo. Além disso, esse compartilhamento de informações proporciona integração entre os setores do

programa socioeducativo e contribua para o fortalecimento do trabalho coletivo.

Em Minas Gerais, a Subsecretaria de Atendimento Socioeducativo (Suase) é o órgão gestor que elabora, coordena e executa a política de atendimento ao adolescente autor de ato infracional no estado. Vinculada à Secretaria de Estado de Justiça e Segurança Pública (Sejusp), publicou, em 2021, a Resolução Sejusp nº 211, onde prevê sobre a Agência Central de Inteligência Socioeducativa (Acis) da Subsecretaria de Atendimento Socioeducativo do Estado de Minas Gerais. A resolução é bem detalhada sobre competência, recursos humanos, atribuições e estrutura física da agência.

> (...) tem a finalidade de produzir, salvaguardar e promover a difusão, de forma cooperativa e integrada, do conhecimento decorrente da Atividade de Inteligência, com vistas a prever, prevenir, neutralizar e reprimir atos criminosos no âmbito do Sistema Socioeducativo, que sejam de interesse da segurança da sociedade e do Estado (MINAS GERAIS, 2021, Art. 2º).

Atividade de Inteligência na Socioeducação

Compreendemos que a segurança e a disciplina são instrumentos indispensáveis à viabilização do percurso socioeducativo e de um atendimento individualizado do adolescente. Constituem-se como condição imprescindível para se atingir os objetivos da medida socioeducativa diante das determinações emanadas dos ordenamentos jurídicos.

O processo socioeducativo do adolescente se inicia no momento em que entra no programa socioeducativo. Os procedimentos de recepção, inclusão, acolhimento, integração e desenvolvimento do percurso formativo devem estar previstos no Projeto Político Pedagógico. Desde a entrada do adolescente até o seu desligamento, o papel dos profissionais deve orientar-se sobre os eixos estruturantes, a responsabilização e a integração social.

O clima institucional nem sempre está favorável. Muitas vezes, a rotina está permeada por altos níveis de tensão, estresse, violência, subjugação e agressividade, o que torna inviável e inexequível a Jornada Pedagógica. As equipes multiprofissionais não conseguem executar as suas atribuições, as rotinas pedagógicas são suspensas, os atendimentos psicossociais são adiados ou executados sob um contexto desfavorável.

O ambiente tensionado, hostil e inadequado desfavorece a execução da medida socioeducativa, neste caso, de qualquer natureza. O socioeducando pouco se envolve nas atividades propostas, e os profissionais não conseguem desenvolver as suas atribuições. Nesse sentido, a Atividade de Inteligência poderá se constituir em uma ferramenta que possibilite desvelar as determinações deste ambiente desfavorável. Assim, a Atividade de Inteligência das Unidades Socioeducativas pode ser compreendida como toda e qualquer ação

que, durante a rotina de trabalho, busque obter informações que possam assessorar a gestão do programa socioeducativo do ponto de vista da segurança preventiva e interventiva, além de subsidiar a tomada de decisões que previnam ações de conflito entre os adolescentes e as equipes multidisciplinares.

A Atividade de Inteligência na Unidade Socioeducativa tem como principal objetivo subsidiar a direção para melhorar a gestão da segurança institucional, que é atividade mediadora, facilitadora e garantidora de tranquilidade. Assim, representa um instrumento para que seja viável a realização das atividades diversas atividades, tais como escolares, profissionalizantes, culturais, de lazer e saúde, entre outras, conforme determinam os marcos legais da Socioeducação. Portanto, a execução dessa tarefa na rotina de trabalho, além de assessorar a gestão da segurança, também proporciona o acesso a informações que dão subsídios à realização de uma jornada pedagógica.

Para a direção da unidade, as informações fornecidas pelo setor de inteligência fundamentam as decisões tomadas, especialmente em casos mais complexos, e proporcionam maior legalidade, proporcionalidade e legitimidade. Além disso, promovem mediações em possíveis conflitos com as equipes de trabalho e podem, ainda, prevenir casos de suicídio de adolescentes acautelados.

O exercício diário e contínuo da Atividade de Inteligência, desempenhado não exclusivamente pelos agentes de segurança socioeducativos, mas por todos os servidores, além de garantir a segurança e subsidiar a tomada de decisão, também viabiliza melhor elaboração e execução dos instrumentos pedagógicos, p. ex., o Estudo de Caso e o Plano Individual de Atendimento, que são fundamentais na execução da medida socioeducativa e na efetivação do trabalho interdisciplinar e intersetorial, conforme prevê o Art. 54 da Lei do Sinase (BRASIL, 2012).

Diante do exposto, nota-se que a Atividade de Inteligência na Socioeducação vai muito além da segurança, apesar de essa ser a principal finalidade; contudo, devido à complexidade do trabalho socioeducativo, observa-se que o compartilhamento de informações proporciona maior integração entre os setores, fortalece o trabalho em equipe, subsidia-o e fundamenta a tomada de decisão, fato que ocasiona à direção melhores condições para gestão institucional; porém, muito além disso, torna-a responsabilidade de todos, ajuda a fortalecer a comunidade socioeducativa e a qualificar ainda mais o trabalho ofertado.

Considerações finais

A Atividade de Inteligência Socioeducativa visa a obtenção, a análise e a disseminação de informações que possam interferir positiva ou negativamente na execução

do trabalho da segurança institucional. A produção de conhecimentos de Inteligência durante a execução da medida socioeducativa de internação revela-se importante na medida em que mitiga o risco de eventos adversos, antecipando ameaças e identificando vulnerabilidades. Da mesma forma, contribui para o processo de planejamento de políticas e de tomada de decisões, ampliando a garantia dos direitos fundamentais de adolescentes e jovens privados de liberdade. A produção de conhecimentos também apoia a segurança de toda a comunidade socioeducativa, ou seja, todos que, de alguma forma, atuam, interagem ou compartilham momentos em visitas ou prestação de assistência, como a religiosa, entre outras, nas unidades de internação.

Compreendemos que a Atividade de Inteligência é uma função típica do Estado e deve ser empregada em temas fundamentais, estruturais e estratégicos; valendo-se do uso de técnicas apropriadas poderá fazer diferença significativa no cotidiano de gestão da Socioeducação. A utilização desse instrumento, com efeito, tem aplicação em realidades de instabilidade e de tensão permanentes, tais como aquelas encontradas em algumas unidades socioeducativas, especialmente diante do aumento da violência e a infiltração de facções criminosas. Assim, a Inteligência Socioeducativa poderá compor as categorias especializadas da Atividade de Inteligência, como a Inteligência Fiscal, a Previdenciária, a Financeira, a Penitenciária e a de Segurança Pública.

Em que pese a sua importância, a aplicação da Atividade de Inteligência na gestão da política de Socioeducação no Brasil, ainda é um tema pouco debatido no âmbito da infância e da juventude, mas já tem servido de base para se combater situações de violência contra crianças e adolescentes. Apesar disso, poucos estados têm compreendido essa prática como norteadora para a ampliação da garantia de direitos fundamentais, isto é, um instrumento para a prevenção de situações conflituosas e para a garantia da segurança e manutenção da vida.

Referências

AGÊNCIA MINAS. *Capacitação sobre Inteligência mobiliza profissionais de segurança de Minas e mais seis estados.* Publicado em 16 maio de 2022. Disponível em: https://www.agenciaminas.mg.gov.br/noticia/capacitacao-sobre-inteligencia-mobiliza-profissionais-de-seguranca-de-minas-e-mais-seis-estados. Acessado em 24 out. 2023.

BRASIL. *Lei nº 12.594, de 18 de janeiro de 2012.* Institui o Sistema Nacional de Atendimento Socioeducativo (SINASE). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12594.htm. Acesso em 5 maio. 2023.

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. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9883.htm. Acesso em 20 abr. 2023.

CONANDA. *Resolução 119, de 11 de dezembro de 2006*: dispõe sobre o Sistema Nacional de Atendimento Socioeducativo e dá outras providências. Brasília: CONANDA, 2006. Disponível em: http://www.mdh.gov.br/assuntos/criancas-e-adolescentes/pdf/SinaseResoluoConanda.pdf. Acesso em 5 mai. 2023.

CONANDA. *Resolução 113, de 19 de abril de 2006*. Brasília: CONANDA, 2006a. Disponível em: http://www.direitosdacrianca.gov.br/conanda/resolucoes/113-resolucao-113-de-19-de-abril-de-2006/view. Acesso em 24 de maio. 2023.

COSTA, Ricardo Peres da. *O trabalho do agente de segurança socioeducativo na socioeducação:* processos de estranhamento e alienação na construção de uma identidade profissional. 406 f. (Tese, Serviço Social e Política Social). Londrina, PR: Universidade Estadual de Londrina (UEL), 2020.

DIÁRIO DE PERNAMBUCO. *Sete adolescentes mortos durante rebelião na Funase de Caruaru.* Publicado em: 31/10/2016. Disponível em: https://www.diariodepernambuco.com.br/noticia/vidaurbana/2016/10/rebeliao-na-funase-de-caruaru-deixa-sete-adolescentes-mortos.html. Acesso em 24 out. 2023.

DISTRITO FEDERAL. *Decreto nº 37.896, de 27 de dezembro de 2016*. Disponível: http://www.crianca.df.gov.br/wp-conteudo/uploads/2018/02/DECRETO-REGIMENTO-INTERNO-DA-SECRETARIA-DE-ESTADO-DE-POLITICAS-PARA-CRIAN%C3%87AS-1.pdf. Acesso em 24 out. 2023.

FASEPA. *Profissionais debatem procedimentos de segurança e Iteligência na socioeducação*. Disponível em: http://www.fasepa.pa.gov.br/?q=node/1326. 2019. Acesso em: 24 out. 2023.

IASES. *Instrução de Serviço Nº 0585-P de 30 de novembro de 2017*. Disponível em: https://iases.es.gov.br/Media/iases/Arquivos/SISTEMA%20DE%20INTELIG%C3%8ANCIA%20DO%20IASES%20-%20SIIASES.pdf. Acesso em 24 out. 2023.

IASES. *Iases capacita servidores em Atividade de Inteligência***.** Disponível em: https://iases.es.gov.br/Not%C3%ADcia/iases-capacita-servidores-em-atividade-de-inteligencia. 2017. Acesso em 24 out. 2023.

MINAS GERAIS. *Resolução nº 211 de 2021.* Publicada em 1º de setembro de 2021. DIOMG. Disponível em: https://www.jornalminasgerais.mg.gov.br. Acesso em: 24 out. 2023.

MISSE, Michel. Notas sobre a sujeição criminal de crianças e adolescentes. *In*: SENTO-SÉ, João T; PAIVA, Vanilda P. (orgs.). *Juventude em conflito com a lei.* Rio de Janeiro: Garamond, 2006. (2006).

MONTAGNA, Adauton. Crise e Inteligência: a Atividade de Inteligência no gerenciamento de crises. *Revista Brasileira de Inteligência*. Brasília: Abin, nº 17, dez. 2022.

MPGO. *Atividade de Inteligência no Sistema do Estatuto da Criança e do Adolescente: Aspectos Teóricos e Práticos*. Disponível em: http://www.mpgo.mp.br/portal/noticia/atividade-de-inteligencia-eca--2#.YPW9FehKjIU. 2017. Acesso em 24 out. 2023

REGINATO, Gisele. *SJSPS promove seminário sobre a relevância do Sistema de Inteligência no sistema prisional e socioeducativo.* Disponível em: https://www.fase.rs.gov.br/sjsps-promove-seminario-sobre-a-relevancia-do-sistema-de-inteligencia-no-sistema-prisional-e-socioeducativo. Acesso em: 24 out. 2023.

PAIVA, Luiz Fábio Silva. *Aqui não tem gangue, tem facção:* as transformações sociais do crime em Fortaleza, Brasil. *Caderno CRH*, Salvador, v. 32, nº 85, p. 165-184, jan./abr. 2019. (2019).

SANTA CATARINA. *Decreto nº 2.379, de 28 de dezembro de 2022*. Aprova o Regimento Interno da Secretaria de Estado da Administração Prisional e Socioeducativa e estabelece outras providências.

Artigo

12

GNOSEOLOGIA DAS CIÊNCIAS HUMANAS E PRODUÇÃO DO CONHECIMENTO DE INTELIGÊNCIA

DOI: https://doi.org/10.58960/rbi.2023.18.234

Henrique Geaquinto Herkenhoff *
Rogério Bubach **

Resumo

Este artigo analisa o impacto e as consequências dos vieses cognitivos no processo de produção de conhecimento da Atividade de Inteligência, principalmente, sob o entendimento de que a cognição implica dar significado ao que é percebido e integrá-lo em um todo oportuno e útil para decisão dos formuladores de política. Ao partir de contribuições recentes sobre o tema, perpassa pelas estratégias utilizadas para identificar e mitigar os efeitos dos vieses cognitivos e sua verdadeira eficácia no trabalho dos analistas de Inteligência, principalmente, sobre os produtos resultantes de seu esforço cognitivo. Aborda, mesmo sem extensão, a gnoseologia da ciência, a reivindicação de participação das "ciências" humanas e a contextualização dessas com a Atividade de Inteligência, e alcança aspectos dos processos consciente e inconsciente aplicados na produção do conhecimento de Inteligência e em seus propósitos. Discute estratégias para o gerenciamento de riscos da cognição humana e apresenta alternativas que podem fomentar o trabalho dos órgãos de Inteligência, principalmente, na atividade de análise das informações.

Palavras-chave: viés cognitivo; análise de Inteligência; falhas de Inteligência.

GNOSEOLOGY OF HUMAN SCIENCES AND PRODUCTION OF INTELLIGENCE KNOWLEDGE

Abstract

It analyzes the impact and consequences of cognitive biases in the knowledge production process of intelligence activity, mainly under the understanding that cognition implies giving meaning to what is perceived and integrating it into a timely and useful whole for the decision of the policy makers. Based on recent contributions on the topic, goes through the strategies used to identify and mitigate the effects of cognitive biases and their true effectiveness in the work of intelligence analysts, mainly about the products resulting from their cognitive effort. It addresses, even without extension, the gnoseology of science, the claim of participation of human "sciences" and the contextualization of these with the activity of intelligence, reaching aspects of the conscious and unconscious process applied in the production of knowledge of intelligence and its purposes. Discusses strategies for risk management of human cognition, presenting alternatives that can encourage the work of intelligence agencies, mainly

* Doutor em Direito Civil pela Universidade de São Paulo (USP). Atuou como membro do Ministério Público Federal, como desembargador no Tribunal Regional Federal da 3ª região e como secretário de estado de segurança pública do Espírito Santo. Advogado e professor na Universidade de Vila Velha /ES (UVV).

** Mestre em Segurança Pública pela Universidade Vila Velha. Especialização em Segurança Pública pela Universidade Federal do Espírito Santos (UFES). Graduação em Direito pela Universidade Vila Velha. Graduação no Curso de Contrainteligência da Subsecretaria de Estado de Inteligência/ Secretaria de Estado de Segurança Pública e Defesa Social do estado do Espírito Santo.

in the activity of analyzing information.

Keywords**:** *cognitive bias; Intelligence analysis; Intelligence failures.*

GNOSEOLOGÍA DE LAS CIENCIAS HUMANAS Y PRODUCCIÓN DE CONOCIMIENTO DE INTELIGENCIA

Resumen

Este artículo analiza el impacto y las consecuencias de los sesgos cognitivos en el proceso de producción de conocimiento de la actividad de Inteligencia, principalmente bajo el entendido de que cognición implica dar significado a lo percibido e integrarlo en un todo oportuno y útil para la toma de decisiones de los formuladores de políticas. Con base en contribuciones recientes sobre el tema, se abordan las estrategias utilizadas para identificar y mitigar los efectos de los sesgos cognitivos y su verdadera efectividad en el trabajo de los analistas de Inteligencia, principalmente en los productos resultantes de su esfuerzo cognitivo. Aborda, aún sin extensión, la gnoseología de la ciencia, la pretensión de participación de las "ciencias" humanas y su contextualización con la actividad de la Inteligencia, y alcanza aspectos de los procesos conscientes e inconscientes aplicados en la producción del conocimiento de la Inteligencia y sus propósitos. . Discute estrategias para gestionar los riesgos de la cognición humana y presenta alternativas que pueden promover el trabajo de las agencias de Inteligencia, principalmente en la actividad de análisis de información.

Palabras clave: *sesgo cognitivo; análisis de inteligencia; fallas de inteligencia.*

Introdução

O presente artigo já estava bastante adiantado quando o número 14 desta revista trouxe o excelente artigo "Vieses cognitivos na Atividade de Inteligência", que destaca como o analista de Inteligência pode ser conduzido ao erro por mecanismos desenvolvidos naturalmente pela mente humana, tais como os vieses de representatividade, *status quo*; ancoragem e ajustamento, confirmação, disponibilidade, espelhamento de imagem e atribuição. De maneira muito semelhante, já Bacon identificava quatro espécies de obstáculos epistemológicos ou cognitivos: os *idola tribus*, os *idola specus*, os *idola fori* e os *idola theatri* (PENNA, 1986, p. 36). A linha de pensamento defendida pelos autores Christiano Ambros e Daniel Lodetti pode ilusoriamente parecer oposta à que sustentaremos adiante, de maneira que nos permitiremos, à guisa de introdução, tecer alguns comentários a respeito desse trabalho, que traz, em si mesmo, contra-argumentos importantes.

Como é público e notório, desde que restou comprovado não haver armas de destruição em massa no Iraque em 2003 e, principalmente, desde o atentado contra as Torres Gêmeas em 2001, tanto dentro das próprias instituições quanto na imprensa e no meio político, cresceu, exponencialmente, o interesse em estudar e prevenir supostas falhas nos serviços de Inteligência. Uma das soluções encontradas foi a utilização das chamadas técnicas de análise estruturada, e passou-se "de um modelo em que o analista processava individualmente a informação, de uma maneira intuitiva, para outro em que se incentiva a colaboração em grupo durante o processo analítico" (AMBROS; LODETTI, 2019, p. 22).

Contudo, os próprios vieses na avaliação retrospectiva desses eventos colocam em dúvida a importância, e mesmo a existência, dessas supostas falhas nos serviços estadunidenses de informação (SÁNCHEZ, *in* FERNANDEZ, 2016, p. 183-189; TURNER, 2005, p. 1-2) e, especialmente, sua atribuição a vieses analíticos (DOWLING, 2005; ZEGART, 2007), a não ser que a acomodação[1] – inclusive em produzir apenas sob encomenda (BODNAR, 2003, *passim*; MARTIN, 2002, p. 38) –, a incompetência gerencial e a falta de integração entre agências (LOWENTHAL, 2015, p. 179) possam ser consideradas um fenômeno cognitivo:

> Para o indivíduo inexperiente, não é bom quando o acaso não lhe presta esse serviço; pois, se um relatório confirma o outro, dá-lhe veracidade, diminuindo a desconfiança, dando novas nuances a imagem formada, até que somos forçados, pela necessidade, a tomar, com urgência, uma resolução que em breve se descobrirá ser uma decisão equivocada e que todos esses relatórios continham

1 É verdade que as heurísticas são inerentemente conservadoras dos padrões anteriores (SINCLAIR, 2010, p. 9), mas não podem ser consideradas o único fator de acomodação.

> apenas mentiras, exageros, erros etc. Enfim, para resumir, a maioria dos relatórios são enganosos e a timidez do homem age como um multiplicador de engodos e falsidades (CLAUSEWITZ, 2005, p. 63-64).

Aliás, o viés de exagerar nossa própria capacidade de influenciar decisão alheia (AMBROS; LODETTI, *op. cit.*) tem um irmão gêmeo: o de subestimar a força adversa ou superestimar a habilidade ou o dever de se prever e evitar certos eventos. Analistas de Inteligência não são oráculos. Em particular, a nação estadunidense simplesmente não é capaz de aceitar (TURNER, 2005, p. 1-2) que seu país, por diversos fatores, é um alvo cobiçado, tem dimensões continentais, abriga comunidades populacionais extremamente variadas, comercia e, ao mesmo tempo, envolve-se em atritos por todo o planeta etc., e, portanto, simplesmente não está a salvo de conflitos de baixa intensidade em seu próprio território. Ademais, falhas grotescas podem não resultar em nenhum prejuízo, enquanto pequenas imperfeições podem permitir desastres concretos: avaliar uma falha por suas consequências distorce a viabilidade de prevenção.

Por outro lado, esses atalhos mentais são absolutamente indispensáveis, ainda que possam eventualmente ter efeitos colaterais negativos. Quando a imagem de um leão aumenta continuamente, a primeira reação é fugir o mais rápido possível. Talvez fosse uma ilusão de ótica, talvez o leão não estivesse à caça, mas a verdade é que não existe nenhum descendente daqueles cujos cérebros hesitaram em colocar as pernas para correr (FEARN, 2004, p. 91). Uma análise concentrada no erro e desgarrada dos êxitos também incidirá na "lei dos pequenos números", e dará ênfase exagerada a momentos "patológicos" dos processos de produção do conhecimento; afinal de contas, os advogados somente atuam nos casos em que os contratos foram descumpridos, mas essa não é a situação mais frequente no mundo dos negócios. Em outras palavras, ideias preconcebidas, vieses e análises automáticas de nossos sentidos, todos esses processos mentais desenvolvidos evolutivamente pelo ser humano, são, essencialmente, muito bons: apenas não custa tomar algum cuidado para prevenir situações que nos levariam a erros evitáveis (BARRUTIETA, *in* FERNANDEZ, 2016, p. 26-27).

A cognição implica, exatamente, dar significado ao que é percebido e integrá-lo, e isso não pode ser feito, em termos concretos, senão a partir da cognição acumulada por aquele ser humano individualizado (ROSITO, 2006). Os vieses não são um defeito no processo cognitivo, mas parte integrante e essencial dele. Não há como, atualmente, entender como Sócrates era entendido em sua época, como tampouco duas pessoas o podem entender exatamente igual. Portanto, não apenas não é viável, como sequer conveniente, efetivamente impedir, mas apenas controlar os vieses cognitivos, até

porque o erro é próprio de toda atividade humana, e esses vieses somente representam uma ameaça à parte quando possam sem induzidos ou manipulados por uma força adversa.

Métodos estruturados de análise tendem, sim, a se tornar lentos e, burocráticos, embora isso possa ser, em larga medida, reduzido, uma vez que os arcabouços preconizados sejam vistos como apoio e não como prisões do pensamento, e permitam que sejam integrados ao repertório de ferramentas de raciocínio automático. Ou seja, esses mecanismos para prevenção de heurísticas podem ser apropriados pelos analistas como processos inconscientes tão naturais e imediatos quanto os próprios vieses; é possível treiná-los em vez de engessá-los.

Também é possível reduzir a lentidão pela utilização da informática, mas isso aumenta o engessamento e adiciona o sério risco de se criar o conforto da ilusão matemática: se alimentarmos um *software* com dados arbitrariamente estimados, o computador nos fornecerá gráficos vistosos e transformará uma completa ausência de informações numa "verdade" inquestionável, com a agravante de aparentar precisão até nas casas centesimais (DEMO, 2000, p. 22-35). Até começar a parecer ordem, o caos não é perigoso (GUNTHER, 2013, p. 68). Além disso, é mais fácil comprar equipamentos de informática de última geração que "vendê-los" a instituições e servidores da geração anterior (BODNAR, 2003, p. 151-152).

Por fim, a informática nada mais faz do que substituir os vieses humanos por *biases* algorítmicos (O'NEILL, 2016, *passim*; CRAWFORD, 2012; CRAWFORD & CALO, 2016), que têm a mesma tendência de consolidar preconceitos na amostragem decisória, além de igualmente não ser possível saber o percurso lógico-argumentativo que levou à decisão. Algoritmos não seriam mais que opiniões codificadas; podem conter vieses de quem os elaborou ou de quem os está utilizando, ou simplesmente provenientes de uma amostragem insatisfatória na base de dados. Embora capazes de "aprender", em última análise, os *softwares* tendem, mais que o ser humano, a replicar decisões ou análises anteriores. Computadores erram menos porque variam menos. Quanto mais forem capazes de criatividade e iniciativa, mais se aproximarão dos seres humanos na possibilidade de equívoco. Portanto, mesmo que utilizem inteligência artificial, continuará necessário auditar permanentemente sua transparência, sua escala de enviesamento e seu dano potencial.

A análise coletiva da informação tem vantagens evidentes, principalmente em temas complexos e inter ou multidisciplinares, bem como quando se aproximam os consumidores e os produtores de Inteligência. Contudo, além

de exigir maior quantidade de pessoal e aumentar o tempo de processamento, implica menor compartimentação e gera riscos, tais como a interferência de relações interpessoais (amizade ou antipatia, admiração ou despeito, liderança ou oposição) e, principalmente, um fenômeno que talvez não possa ser caracterizado como um viés cognitivo, mas que causa muito mais estragos: o efeito manada ou, como chamava Nietzsche (1981, p. 128/129), o espírito de rebanho. Na cena cinematográfica mencionada por Sinclair (2010, p. 8), após um anúncio ininteligível pelo alto-falante, um trem se aproxima da estação, e todos se dirigem para aquela plataforma, por imaginar que embarcariam, mas o veículo passa direto; os passageiros não se dirigiram ao trem errado porque tomaram decisões individuais enviesadas, mas porque se influenciaram mutuamente; o primeiro que fez menção de se mover para a plataforma da esquerda sentiu sua decisão confirmada ao ser imitado pelos demais. Ainda que a heurística possa ter contribuído para deflagrar o processo decisório equivocado, ele se acelerou e sustentou coletivamente.

De fato, tanto nos serviços de Inteligência como nos processos decisórios ou nas corretoras das Bolsas de Valores, é fácil perceber que a maior parte dos seres humanos prefere errar coletivamente a acertar sozinho (HOLT, 1994, p. 86-87; SCHULSKY, 1991, p. 63; SANCHEZ, *in* VELASCO, NAVARRO; ARCOS, 2008, p. 99). Se todos os analistas de mercado recomendam a aquisição de uma ação, é improvável que apenas um deles diga exatamente o oposto; dificilmente um deles realmente recomendará a seus clientes uma carteira de investimentos exatamente igual a sua própria, pois mesmo acertar sozinho pode levar alguém à fogueira. Há, portanto, muito mais segurança e muito mais prêmios em aderir ao pensamento predominante (NIETZSCHE, 1981, p. 193 e 242-243; PIAGET, 1978, p. 77) esteja ele, correto ou equivocado, algo que até Galileu praticou mais de uma vez (LENTIN, 1997, p. 65; RUSSEL, 1969, p. 29-30).

Por fim, frequentemente, existem prêmios por fazer ou dizer aquilo que seus superiores querem que seja feito ou dito (HOLT, 1994, p. 84; SCHULSKY, 1991, p. 62; TURNER, 2005, p. 3; SANCHEZ, *in* VELASCO, NAVARRO; ARCOS, 2008, p. 94-95). Uma vez que se tenha tomado a decisão de declarar guerra a um outro país, é preciso justificá-la; qualquer voz que se levante em outra direção será, no mínimo, desprezada, quando não vista como traição. E o suposto enviesamento de uma análise frequentemente não é mais do que viés de quem recebe a informação ou de quem toma conhecimento dela; há larga dose de cinismo nas críticas, tanto da imprensa quanto de oposicionistas. (HOLT, 1994, p. 85).

Gnoseologia da ciência, das "ciências" humanas e da Inteligência

Aparentemente, existe um equívoco fundamental de se imaginar que todo e qualquer conhecimento tem a mesma natureza, as mesmas limitações, as mesmas fontes e deve ser produzido pelo mesmo método. Nada mais falso.

O analista de Inteligência geralmente vai entregar um produto escrito que, em seguida, será difundido e chegará aos consumidores finais. Ora, o processo de produção do conhecimento científico apenas começa quando o do conhecimento de Inteligência termina. Depois de redigir seu artigo científico, o acadêmico o submeterá a algum periódico especializado, que o remeterá a dupla revisão cega por pares, a fim de decidir se esse trabalho sequer merece ser publicado. A partir de então, se ele despertar interesse na comunidade acadêmica, outros pesquisadores repetirão o estudo com o mesmo experimento ou, mais frequentemente, com experimentos diferentes, em busca de falseá-lo (POPPER, 2013a, p. 37 *et seq*.). Só depois de granjear, ao mesmo tempo, importância e reconhecimento, um determinado postulado será aceito pela comunidade científica como uma verdade provisória, sempre no aguardo de um falseamento não alcançado por ora. Nas ditas "ciências" humanas, não existe a possibilidade seja de falseamento ou refutação definitiva, seja de prova, mas apenas de convencimento parcial da comunidade de estudiosos, razão pela qual convivem indefinidamente correntes de pensamento, por exemplo, a freudiana, a lacaniana, a junguiana, a Gestalt, a Psicologia Comportamental e outras.

Seja em tese, seja concretamente, o "sujeito" do conhecimento científico é sempre abstrato e, inclusive, inumano: uma reação química ocorre igualmente quando estudada por um terrestre ou um marciano; aliás, ocorre igualmente, independentemente de ser observada ou não, sempre da mesma maneira, não importa a que tempo. Não existe, portanto, nenhuma possibilidade de enviesamento e nem mesmo faz sentido falar em "referencial teórico", já que nenhum postulado da Física parte do pressuposto de que são verdadeiras as correntes de pensamento formadas a partir de Karl Marx ou Max Webber, como geralmente ocorre no campo da Economia ou da Sociologia. Já o sujeito cognoscente nas "ciências" humanas é um dado indivíduo que, no máximo, será questionado pela comunidade de estudiosos quando expuser suas opiniões. É inevitável que seu conhecimento esteja impregnado por sua visão de mundo, sua personalidade, seus valores, suas idiossincrasias e, portanto, também seus vieses cognitivos. A cognição, fora do campo das ciências naturais e dos conhecimentos abstratos (matemática pura, física teórica etc.), é um processo

psicológico concreto, histórico e datado. Com mais forte razão, o conhecimento de Inteligência enfrenta esse campo de falibilidade, mas não porque o processo de produzi-lo seja falho, e sim porque se trata de um risco inerente.

Outro ponto a ser sempre sublinhado é que um dado ainda não admitido como científico pode perfeitamente ser considerado útil, tanto nas ciências aplicadas como, com mais forte razão, na Inteligência, cujo papel não é, em última análise, apresentar certezas absolutas, mas sim reduzir incertezas quanto aos fatos no momento decisório.

Como prevenir os vieses de cognição viciados

Repita-se, os vieses de cognição não são, em si mesmos, vícios no processo de produção das "ciências" humanas ou do conhecimento de Inteligência. Apenas devemos estar sempre advertidos sobre eles. Um bom trabalho de sociologia aponta seu referencial teórico e, assim, facilita o trabalho do leitor crítico, isto é, do bom consumidor de conhecimento sociológico.

Cria-se ciclos esquemáticos de produção de conhecimento de Inteligência, e, mais modernamente, processos estruturados de análise, muito interessantes como ferramenta didática e sistematizadora do trabalho dos funcionários dos órgãos de Inteligência. São muito úteis para viabilizar o trabalho em equipe, mas não se deve ignorar o fato de que a maior parte do conhecimento levado aos decisores não vem das ciências da natureza, mas tem base platônica, e a retrospectiva é pouco mais segura do que a prospectiva, na medida em que "até o passado é incerto".[2] Ademais, mesmo em relação às ciências da natureza, simplesmente não é possível – nem importante – reconstruir racionalmente as fases que conduziram o cientista à descoberta (POPPER, 2013a, p. 30). Na verdade, nem tudo que escapa a nosso consciente é necessariamente irracional, e a neurociência ainda está longe de resolver o problema da consciência (TEIXEIRA, 2012, *passim*).

> Todo o erro da velha psicologia, no que concerne aos processos lógicos, provém invariavelmente da consideração do pensamento, da razão, como entidades acima das necessidades naturais, no domínio da mais refinada abstração. O pensamento surge como qualquer coisa de superior, que necessita unicamente estar em acordo consigo mesmo por meio das regras rigorosas da lógica pura [...] (MENEZES, 1971, p. 112).

> [...] não existe um método lógico de conceber ideias novas ou de reconstruir logicamente esse processo. Minha maneira de ver pode ser expressa na afirmativa de que toda descoberta encerra um 'elemento irracional' ou uma 'intuição criadora' no sentido de Bergson. De modo Similar, Einstein fala da 'busca daquelas leis universais [...] com base nas quais é possível obter, por dedução pura, uma imagem do universo. Não há caminho lógico", diz ele, 'que leve a essas [...] leis. Elas só podem

2 Frase frequentemente atribuída a Pedro Malan, ex-Ministro da Economia, mas também a Gustavo Loyola, ex-Presidente do Banco Central.

> ser alcançadas por intuição, alicerçada em algo assim como um amor intelectual (Einfuhlung) aos objetos de experiência" (POPPER, 2013a, p. 31).

A par disso, também não se deve ignorar nem desvalorizar integralmente aquilo que venha de fontes "irracionais", tais como a intuição (CARMELLO, 2000, *passim*), a opinião, os fatos comunicados simbolicamente ou mesmo a análise dos discursos, especialmente quando possam ser confirmados por outras fontes mais "tradicionais" ou quando, simplesmente, não seja possível adiar a deliberação. Segundo a teoria do fechamento cognitivo, "algumas propriedades e teorias são acessíveis para alguns tipos de mentes e não para outros" (MCGINN *apud* VICENTINI, 1999, p. 42). O método cartesiano, tão louvado por sua aparente infalibilidade, simplesmente não é aplicável às ciências naturais (LENTIN, 1997, p. 98 *et seq*.) e muito menos poderia resumir as possibilidades de conhecimento humano.

Conhecimento e inconsciente

Sigmund Freud, um dos pioneiros e o mais conhecido estudioso da mente inconsciente, teve Carl Gustav Jung como discípulo, inicialmente, e dissidente, posteriormente. Freud, em rápido resumo, descreveu a mente humana como formada por duas estruturas inconscientes: o id, responsável pelos desejos, e o superego, que tende à repressão de toda volição; essas estruturas seriam completadas por uma outra consciente, o ego, incumbido não apenas de arbitrar a relação conflituosa entre as estruturas inconscientes, mas também de intermediá-la com o ambiente externo.

Jung propôs uma estrutura total da psique,[3] o *Selbst* (si mesmo, *self*, em inglês), da qual a parte consciente (ego) é somente uma pequena fração, responsável pela realização do *self* por meio da articulação do indivíduo com o meio exterior (JUNG *et al.*, 1999, p. 161 *et seq*.). A parte que permanece inconsciente é tão racional, inteligente, arguta e observadora quanto a consciente, porém é muito maior e mais capaz de guardar memórias ou informações ou de realizar operações mentais. Essa estruturação, que, para efeitos exclusivamente didáticos, poderíamos dizer dividida em "mentes" que funcionam concomitantemente, seria extremamente útil para permitir ao ser humano se concentrar em atividades de importância imediata, sem, apesar disso, deixar de perceber, registrar e elaborar intelectualmente outras informações que seus sentidos lhe trouxessem ao mesmo tempo e que, inclusive, são muito mais numerosas e menos organizadas (BARBER; LEGGE, 1976, *passim*), nem sobrecarregar o consciente com memórias e informações que não tenham importância imediata. Deste modo, tanto o analista

3 Bom exemplo de que, no conhecimento de base platônica, duas "verdades" podem coexistir.

quanto as fontes humanas detêm muito mais conhecimento inconsciente do que consciente.

> Este material torna-se inconsciente porque – simplesmente – não há lugar para ele no consciente. Alguns de nossos pensamentos perdem a sua energia emocional e tornam-se subliminares (isto é, não recebem mais a mesma atenção do nosso consciente) porque parecem ter deixado de nos interessar e não têm mais ligação conosco, ou então porque existe algum motivo para que desejemos afastá-lo de vista (JUNG, 1999, p. 37).

O problema é que o desenvolvimento da racionalidade humana foi, progressivamente, dificultando que a mente inconsciente pudesse devolver ao ego as informações e raciocínios que já tem prontos e disponíveis e que agora se tornaram necessários; logo, o ego precisa servir-se, cada vez mais e com menos efetividade, de mecanismos tais como os *insights*, as epifanias, as revelações, os *dèjá-vu*, os sonhos, as intuições, os atos instintivos etc., quase sempre por meio de símbolos e arquétipos, sensações, calafrios e "vozes interiores", que o avisam para fazer ou não fazer algo imediatamente, sem que se compreenda porquê.

Algumas pessoas têm o ego mais (introvertidas) e outras menos (extrovertidas) acessível à parte inconsciente do *self* (JUNG, 1999, p. 60), mas, no geral, o homem moderno oscila entre desprezar completamente ou dar importância secundária às informações que lhe vêm de origem desconhecida, às conclusões de raciocínios que não lembra haver feito, ao passo que os povos menos "desenvolvidos" entram mais fácil e sistematicamente em contato com seu inconsciente (JUNG, 1999, p. 52).

E, assim, nós, seres racionais, modernos, inteligentes e não místicos simplesmente esquecemos de que, por exemplo, segundo muitas fontes de difícil comprovação[4], Dimitri Mendeleev teria sonhado com a tabela periódica, isto é, em algum momento, sua mente consciente, incapaz de resolver o problema científico de que se ocupava, recebeu a solução que seu *alter ego* já tinha pronta. Da mesma forma, reza a lenda de que Isaac Newton teria repentinamente "criado" a teoria da gravidade quando uma maçã caiu sobre sua cabeça enquanto estava adormecido. Não são poucas as narrativas de descobertas científicas ora um tanto casuais, ora surgidas em sonhos, epifanias e outros fenômenos claramente relacionados ao inconsciente (FREIRE-MAIA, 1992, p. 155). "O advento de um pensamento feliz é fruto dos esforços anteriores do investigador, mas não é, em si, uma ação de sua parte. Ao contrário, trata-se de algo que acontece a ele [...]" (Michael Polanyi, Personal Knowledge: towards a Post-Critical Philosophy. Nova York, Harper & Row, 1962 *apud* ALVES, 1990, p. 145). No mesmo sentido, Popper (2013b, p. 155-156) e Fearn (2004, p. 73-

4 Por exemplo: https://www.manualdaquimica.com/cientistas-que-contribuiram-para-quimica/mendeleiev-criadortabela-periodica.htm e https://alunosonline.uol.com.br/quimica/mendeleiev.html. Acesso em: 6 abr. 2019.

75).

Em resumo, não têm sustentação científica a ideia de que apenas o pensamento e o conhecimento conscientes são racionais, ou, mesmo, que só aquilo que é consciente pode produzir racionalidade. Apenas eles não nos deixam tão confortáveis e, talvez – apenas talvez – sejam, mesmo, merecedores de maior gerenciamento.

Conhecimento e sua representação

Conforme Heuer Junior (1999, p. 1), "quando falamos em melhorar a análise de Inteligência, geralmente nos referimos à qualidade da escrita, tipos de produtos analíticos, relações entre analistas de Inteligência e consumidores de Inteligência, ou organização". Nesse sentido, não bastasse as preocupações do analista, especificamente com os fenômenos decorrentes do funcionamento de seu intelecto, entre eles, os próprios vieses, por vezes, esses profissionais, precisam lidar com as dificuldades de apresentar um produto que atenda aos anseios dos formuladores de políticas ou que, ao menos, represente com fidedignidade o que se tem em termos de informação sobre determinado assunto. O profissional de Inteligência, principalmente o analista, precisa, continuamente, estar atento à representação do resultado de seu trabalho – o conhecimento de Inteligência – ou, ao menos, em como expressar, com rigor, o conceito de sua percepção sobre o que ele significa. Via de regra, a representação do resultado do processo cognitivo do analista, que atua só ou em grupo, com exceções evidentes, constitui-se em relatórios no formato texto, ou ainda, em breves relatos, entre um compromisso e outro, na agenda dos formuladores de política.

Se considerarmos, ainda, que grande parte da matéria-prima do que esse analista recebe para a formulação de seu trabalho também foi obtida por meio de relatórios no formato texto ou de registros em bases de dados, preenchidos com impressões e percepções de outros sobre os assuntos estudados, podemos concluir que a representação do resultado do processo de "análise" por meio dos signos (palavras), concatenados em suas frases, orações e parágrafos no corpo de texto, é essencial na representação do pensamento e no entendimento da realidade.

Destarte, apesar de todo apego e todo rigor aos modelos empregados, esse material acaba por representar apenas uma parcela de percepção dessa realidade, amplamente dependente das capacidades sensitiva e cognitiva de cada indivíduo envolvido no processo de produção. Mantidas as condições ideais, o processo cognitivo imprimirá, inevitavelmente, as percepções individuais aos produtos que entrega. Assim, mesmo com todo o esforço do analista em identificar e controlar os possíveis vieses cognitivos

capazes de impactar seu trabalho, ele ainda poderá, por um mero descuido ou desconhecimento, transmitir por representação, escrita ou falada, sem o rigor da lógica e da gramática, um conceito que não expresse o entendimento da mensagem ou a sensibilização de seus interlocutores quanto ao significado do que pretendia apresentar. A preocupação com o bom emprego da lógica e a correção gramatical passa a ser, como afirma Heuer Junior (1999), tão relevante na qualidade do produto, quanto o controle dos atalhos de seu raciocínio.

Considerações finais

Como visto, o sujeito do conhecimento de Inteligência é concreto e identificável, ainda quando seja coletiva sua produção. A cognição, neste caso, portanto, não é um processo abstrato que possa ser planejado e exercitado formalmente, ainda que se possa desenvolver ferramentas de cunho didático e uniformizador. Trata-se de um processo psicológico, idiossincrático, localizado no tempo e no espaço, não inteiramente consciente, sujeito a falhas individuais ou coletivas.

Reconheça-se o risco inerente a toda análise enviesada ou não totalmente consciente, mas não é necessário desprezá-la, apenas gerenciar esse risco para o diminuir o quanto possível e, quando não for possível eliminá-lo, deixar um registro de sua falibilidade reconhecível pelo consumidor final.

Há, essencialmente, quatro maneiras conhecidas de se reduzir as falhas cognitivas: pela seleção (ROSITO, 2006) e pelo treinamento dos analistas; pela revisão do produto; pela produção coletiva, que também reduz as falhas de representação; e pela adoção de técnicas estruturadas de análise e/ou ferramentas computacionais (AMBROS; LODETTI, 2019). Elas não são excludentes entre si, mas a seleção e o treinamento adequados são, de longe, as menos dispendiosas, as que menos retardam a produção e menos conduzem a outros vícios, tais como a ilusão matemática, as análises emolduradas, a falta de criatividade e iniciativa e a precariedade da Inteligência de advertência.

Quando são obrigados a preencher grandes formulários a quem ninguém presta realmente atenção (até porque o consumidor sempre quer saltar para a conclusão), os analistas perdem um tempo precioso e tendem a se rebelar (e gastar energia) ou a se acomodar (e perde criatividade e iniciativa). No entanto, depois de alguns anos, é provável que seu inconsciente tenha se apropriado de todas as ferramentas formais que lhe foram impostas por seus superiores. Em algum momento, ele se verá fazendo uma Análise de Hipóteses Concorrentes antes de colocar um novo sabão em pó em seu carrinho de supermercado. Ora, esse processo de apropriação de novas ferramentas inconscientes e acoplamento àquelas que herdamos de nossos ancestrais pode ser provocado intencionalmente e

ocorrer de maneira muito mais rápida. Atalhos mentais são muito úteis e quase sempre funcionam exatamente como deveriam. As ilusões de ótica são raras, e há sempre algum mágico ou livrinhos interessantes para nos divertir com elas. Já sabemos que elas existem, embora raramente nos prejudiquem de verdade. Ora, não é difícil conceber exercícios inofensivos em que os vieses cognitivos nos preguem peças e técnicas estruturadas sejam introduzidas como parte da maneira natural de pensar, tal como é possível ensinar quase todos a guiar automóveis ou disparar armas de fogo. Da mesma forma, é possível treinar alguém a estar, ao mesmo tempo, atento a seu conhecimento inconsciente e desconfiado dele. É possível que, em algum grau bastante elevado (mas nunca absoluto), o controle dos processos inconscientes de cognição seja tão automático quanto os próprios processos, o que gera produtos extremamente confiáveis, com a vantagem de abranger muito mais do que a mente consciente, a menor parte que nosso *self* tem a oferecer.

Algumas pessoas jamais conseguirão adquirir certas habilidades e, por isso, poderão estar na profissão errada ou serem eliminadas como parte do processo de recrutamento (no Brasil, o concurso público). As que forem aprovadas deverão ser incessantemente aperfeiçoadas, especialmente quando designadas para a função de análise.

Nada disso exclui a revisão dos produtos apresentados, a análise retrospectiva criteriosa das falhas mais importantes, a produção coletiva do conhecimento de Inteligência, a utilização de técnicas estruturadas ou de ferramentas de informática. Contudo, o que sugerimos acima tende a ser menos dispendioso, mais fácil de digerir pela "velha guarda", mais fácil de impor aos novatos, mais rápido e menos burocrático, evita o engessamento e a falta de criatividade, de iniciativa e de colaboração, a inacessibilidade da informação disponível, que, no final das contas, são, claramente, as principais falhas dos serviços de Inteligência.

A utilidade potencial da Inteligência artificial não pode ser menosprezada, mas ela tampouco será a panaceia universal dos serviços de Inteligência e, certamente, não dispensará os mesmos cuidados com o enviesamento.

Referências

ALVES, Rubem. *Filosofia da Ciência*, 13. ed. São Paulo: ed. Brasiliense, 1990.

AMBROS, Christiano; LODETTI, Daniel. Vieses cognitivos na Atividade de Inteligência: conceitos, categorias e métodos de mitigação. *Revista Brasileira de Inteligência.* Brasília: Abin, n. 14, dez. 2019.

BARBER, Paul J.; LEGGE, David. *Percepção e informação.* Rio de Janeiro: Zahar Editores, 1976.

BODNAR, John W. *Warning analysis fir the information age*: rethinking the intelligence process. Washington (DC) Joint Military Intelligence College, 2003.

CARMELLO, Eduardo. *O poder da informação intuitiva.* São Paulo: Ed. Gente, 2000.

CLAUSEWITZ, Carl von. *Da guerra: a arte da estratégia*. São Paulo: Tahyu, 2005.

CRAWFORD, Kate. The Hidden Biases in Big Data. *Harvard Business Review*. Disponível em: https://hbr.org/2013/04/the-hidden-biases-in-big-data. Acesso em: 7 jun. 2020.

CRAWFORD, Kate; CALO, Ryan. There is a blind spot in AI research. *NATURE,* vol. 538. 20 October 2016. Disponível em: https://www.microsoft.com/en-us/research/wpcontent/uploads/2017/10/538311a.pdf. Acesso em: 7 de jun. 2020.

DEMO, Pedro. *Certeza da incerteza:* ambivalências do conhecimento e da vida. Brasília, Ed. Plano, 2000.

DOWLING, Thomas. *Failures of imagination:* thoughts on the 9/11Comission Report, in Learning with professionals. Washington (DC): Joint Military Intelligence College, 2005.

FEARN, Nicholas. *Aprendendo a filosofar em 25 lições*. Rio de Janeiro: Jorge Zahar, 2004.

FERNANDEZ, Antonio M. Díaz (Director). *Espionaje para políticos*. Valencia: Tirant lo Blanch, 2016.

FREIRE-MAIA, Newton. *A ciência por dentro*. 2. ed. Petrópolis: Vozes, 1990.

GUNTHER, Max. *Os axiomas de Zurique*. Rio de Janeiro: Ed. Record, 2013.

HEUER JUNIOR, Richards J. *Psychology of intelligence analysis.* Center for the Study

in Intelligence. CIA, 1999. Disponível em: https://www.cia.gov/library. Acesso em: 30 set. 2018.

HOLT, Pat M. *Secret Intelligence and public policy*: A dilema of democracy. Washington (DC): CQ Press, 1994.

JUNG, Carl Gustav... (*et al.*) *O Homem e seus símbolos*. 17ª impressão. Rio de Janeiro: Nova Fronteira, 1999.

LENTIN, Jean-Pierre. *Penso, logo me engano:* breve história do besteirol científico, 4. ed. São Paulo: Ática, 1997.

LOWENTHAL, Mark M. *Intelligence.* 6 ed. Washington (DC): Sage/CQPress, 2015.

MARTIN, Alain Paul. *Harnessing the power of Intelligence, Counterintelligence & surprise events*. Canada: Executive dot org, 2002.

MENEZES, Djacir. *O problema da realidade objetiva.* Rio de Janeiro: Tempo Brasileiro/ MEC, 1971.

NIETZSCHE, Friedrich W. *A gaia ciência*. 3. ed. São Paulo: Hemus, 1981.

O'NEILL Catherine. *Weapons of Math destruction:* how big data increases inequality and threatens democracy. New York: Brodway Books, 2016.

PENNA, Antônio Gomes. *Cognitivismo, consciência e comportamento político.* São Paulo: Vértice, 1986.

PIAGET, Jean. Sabedoria e ilusões da filosofia, *in A epistemologia genética* [...]. São Paulo, Abril Cultural, 1978.

POPPER, Karl Raimund. *A lógica da pesquisa científica*. 2 ed. São Paulo: Cultrix, 2013a.

POPPER, Karl Raimund. *Os dois problemas fundamentais da teoria do conhecimento*. São Paulo, Ed. UNESP, 2013b.

ROSITO, Guilherme Augusto. Abordagem fenomenológica e metodologia de produção de conhecimentos, *in Revista Brasileira de Inteligência*. Brasília: Abin, v. 2, n. 3, set. 2006.

RUSSEL, Bertrand. *A perspectiva científica*. 3. ed. São Paulo: Companhia Editora Nacional, 1969.

SCHULSKY, Abram N. *Silent warfare*: understanding de world of intelligence. Washignton (DC): Brassey's US, 1991.

SINCLAIR, Robert S. *Thinking and writing*: cognitive science and Intelligence analysis. Washington (DC): Center for the Study of Intelligence, 2010.

TEIXEIRA, João Fernandes. *Filosofia do Cérebro.* São Paulo: Paulus, 2012.

TURNER, Michael A. *Why secret Intelligence fails*. Dulles (Virginia): Totomac Books, 2005.

VELASCO, Fernando; NAVARRO, Diego; ARCOS, Rubén (eds.) *La Inteligência como disciplina científica***.** Madrid: Plaza y Valdes ed./Ministerio de Defensa, 2008.

VICENTINI, Max Rogério. *Como percebemos o mundo que nos cerca?* Bauru: EDUSC, 1999.

ZEGART, Amy B. *Spying Blind*: the CIA, the FBI and the origins of 9/11. Princeton/ Oxford: Princeton Universty Press, 2007.

Artigo

13

INTERAÇÃO INTELIGÊNCIA-MÍDIA: OS CASOS BND, CNI E MOSSAD

DOI: https://doi.org/10.58960/rbi.2023.18.235

Luciano Gonczarowska-Jorge *

Resumo

A relação entre serviços de Inteligência e a mídia é complexa pela natureza das duas atividades: uma essencialmente secreta, a outra essencialmente pública. É dessa relação que se origina a pergunta-problema: como serviços de Inteligência projetam boa imagem institucional, se o serviço é secreto? Este trabalho analisa o modelo de interação entre as Inteligências alemã, espanhola e israelense e suas respectivas mídias por meio do estudo de fontes bibliográficas, da pesquisa em imprensa, da legislação local sobre Inteligência e liberdade de imprensa e das manifestações de ex-servidores. A forma como se desenvolvem os modelos de relacionamento depende do contexto político-social de cada país, do convencimento da sociedade acerca da importância da Inteligência e das prerrogativas e dos instrumentos legais à disposição. Esta pesquisa conclui que a conquista de imagem institucional positiva pelas Inteligências usa de manutenção de contatos privilegiados com membros especializados da mídia, vazamentos controlados e esforços de comunicação com o sistema político.

Palavras-chave: Serviços de Inteligência; Mossad; BND; CNI; mídia.

MEDIA INTELLIGENCE INTERACTIONS: THE CASES OF BND, CNI AND MOSSAD

Abstract

Intelligence services and the media have a complex relationship due to both activities´ natures: one is essentially secret, the other is essentially public. From this troubled entanglement, a question arises: How do intelligence services project a good institutional image if the service is secret? This paper analyzes the model of interaction between German, Spanish, and Israeli intelligence and their respective media using bibliographic sources, press research, local legislation on intelligence and freedom of the press, and the manifestations of ex-servicemen. The models depend on the political and social context of each country, on society's belief in the importance of intelligence, and on the legal prerogatives and instruments at the service's disposal. This research concludes that the achievement of a positive institutional image by intelligence is backed by privileged contacts with specialized members of the media, controlled leaks, and communication efforts with the political system.

***Keywords*:** *Intelligence Services; Mossad; BND; CNI; media.*

* Bacharel em Relações Internacionais pela Universidade de Brasília (UnB). Especialista em Defesa pela Escola Superior de Guerra (ESG). Servidor Público Federal.

LAS INTERACCIONES ENTRE INTELIGENCIA Y MEDIOS DE COMUNICACIÓN: LOS CASOS BND, CNI Y MOSSAD

Resumen

La relación entre los servicios de inteligencia y los medios de comunicación es compleja debido a la naturaleza de ambas actividades, una esencialmente secreta y la otra esencialmente pública. De esta relación surge la pregunta-problema: ¿cómo proyectan los servicios de inteligencia una buena imagen institucional, si el servicio es secreto? Este trabajo analiza el modelo de interacción entre la Inteligencia alemana, española e israelí y sus respectivos medios de comunicación a través del estudio de fuentes bibliográficas, investigaciones de prensa, legislación local sobre Inteligencia y libertad de prensa y las manifestaciones de ex funcionarios. La forma en que se desarrollan los modelos de relación depende del contexto político y social de cada país, de la convicción de la sociedad sobre la importancia de la inteligencia y de prerrogativas e instrumentos legales de que disponen. Esta investigación concluye que la consecución de una imagen institucional positiva por parte de la Inteligencia utiliza el mantenimiento de contactos privilegiados con miembros expertos de los medios de comunicación, las filtraciones controladas y los esfuerzos de comunicación con el sistema político.

Palabras clave*: *Servicios de Inteligencia; Mossad; BND; CNI; medios de comunicación.

Introdução

Serviços de Inteligência e mídia compartilham a mesma função principal: informar. Grande parte de seus métodos em democracias também são compartilhados, p. ex., uso de fontes humanas, pesquisas em fontes abertas e necessidade de confirmação independente de dados (JOHNSON, 1986; RUEDA RIEU, 2014). Os contrastes, entretanto, não são banais. Uma das principais diferenças são os usuários. Enquanto a Inteligência busca informar, em especial, as principais autoridades do país, a imprensa busca informar a sociedade sobre as principais autoridades do país. Da mesma forma, enquanto o segredo é pré-requisito para o sucesso de operações de Inteligência, a publicidade e a exposição pública são a essência para o sucesso do jornalismo (WILKINSON apud HESS, 2012).

O interesse da mídia pela Atividade de Inteligência se dá, principalmente por quatro razões:

> (i) fascinação da mídia com segredos, essenciais na Inteligência;
>
> (ii) o papel democrático da imprensa em expor malfeitos e, tendo em vista o sigilo da Atividade de Inteligência, muitos acreditam que há quantidade considerável de erros escondidos;
>
> (iii) os temas de interesse da Inteligência são assuntos de interesse preferencial da mídia: espionagem, defesa nacional, crime, as crises nacionais; e, finalmente,
>
> (iv) as reportagens sobre Inteligência são boas porque lucrativas (SHPIRO, 2010).

Para a Inteligência, em regimes democráticos, a cobertura da mídia é extremamente importante, pois afeta a imagem pública dos serviços, o que implica vantagem na competição interburocrática por recursos orçamentários. Além disso, os esforços de recrutamento dos melhores candidatos disponíveis dependem do interesse e do reconhecimento da atividade (HULNICK, 2010). Quantidade significativa de publicações nas imprensas alemã, espanhola e israelense são oriundas da abertura dos concursos públicos para preenchimento dos cargos nas instituições. Os esforços de comunicação como propaganda institucional explícita em cada caso são úteis para pesquisa e, no caso de Israel, foram diligentemente geridos como um dos raros contatos oficiais entre o Mossad e a imprensa, o que gerou ampla publicidade positiva gratuita (MAGEN, 2017). É dessa relação de segredo e necessidade de imagem pública positiva que se origina a pergunta-problema deste trabalho: como serviços projetam uma boa imagem institucional, se o serviço é secreto?

Este estudo apresenta contexto histórico em que os serviços externos de Inteligência

da Alemanha e de Israel e o Serviço de Inteligência espanhol (que congrega as funções interna e externa) desenvolveram sua relação com a mídia e buscaram melhorar a percepção pública sobre si em quatro aspectos: a percepção pública sobre eles, a relação entre legislação de Inteligência e liberdade de imprensa, as estratégias de comunicação adotadas e as últimas tendências percebidas.

A metodologia utilizada abrange pesquisa bibliográfica, acesso aos sites dos serviços, pesquisa de legislação e análise de manifestações sobre as Inteligências feitas por seus ex-agentes em mídias sociais, além da pesquisa nos sites de veículos de imprensa.

Alemanha: abertura defensiva

Histórico

A República Federal da Alemanha (RFA; *Bundesrepublik Deutschland* (BRD), chamada, informalmente, Alemanha Ocidental) possui dois serviços federais de Inteligência: o Serviço de Inteligência Federal Alemão (BND, *Bundesnachrichtendienst*), de atuação externa, e a Agência Federal de Proteção da Constituição (BfV, *Bundesamt für Verfassungsschutz*), de atuação interna. Para os propósitos deste artigo, apenas a estratégia de relacionamento do BND com a mídia será estudada.

O BND surgiu em contexto de resistência da sociedade alemã a organizações secretas, em razão dos traumas e da violência deixados pelos grupos secretos nazistas e pela própria má fama do serviço secreto da então República Democrática da Alemanha (RDA, *Deutsche Demokratische* Republik, que existiu de 7 out. 1949 a 3 out. 1990 e era chamada, informalmente, de Alemanha Oriental), a Stasi *(Staatssicherheitsdienst)* (HESS, 2012). Para se estabelecer na democrática sociedade alemã do pós-guerra, desenvolveu estratégia chamada de Abertura Defensiva (SHPIRO, 2010), cuja finalidade era erigir apoio político e social para a manutenção da existência do serviço em face a um ambiente interno hostil e uma imprensa livre recém-criada e francamente investigativa.

O BND é oriundo da Organização Gehlen, entidade semiprivada para espionagem no leste europeu financiada pela Agência Central de Inteligência dos Estados Unidos (*Central Intelligence Agency*, CIA). Em 1956, foi formalmente vinculada ao Estado alemão ocidental, sob chefia do ex-General de Exército Reinhard Gehlen, que permaneceu à frente do órgão até 1968. Nesse período, o BND se envolveu na política doméstica da Alemanha ocidental e recebeu críticas da imprensa por não antecipar crises; muitas daquelas eram injustas, como se evidenciou com a desclassificação de documentos.

Legislação

A legislação alemã ocidental pós-nazismo não criou salvaguardas para a proteção de segredos de Estado ou o resguardo da Inteligência, o que deixou o BND sem meios legais para a proteção de suas atividades frente ao jornalismo. A Lei Básica (*Grundgesetz*), como é chamada a constituição da RFA, foi criada em 1949, após a fundação dos primeiros jornais da Alemanha ocidental pós-nazismo (*Süddeutsche Zeitung*, 1945; *Die Welt* e *Diese Woche*, 1946; *Der Spigel*, 1947) e em um período em que não havia Forças Armadas ou Serviços de Inteligência alemães. Em seu Art. 5º, parágrafo 1º, foi estabelecida a liberdade de imprensa e a proibição da censura. Apenas em 20 dez. 1990, foi criada a Lei do BND, com mecanismos de resguardo ao serviço.

Principais crises com a mídia

Escândalos divulgados pela mídia ainda nas décadas de 1960 e 1970 sedimentaram a liberdade de imprensa como valor social alemão e conformaram a relação e a estratégia do BND frente à mídia:

> (i) Caso *Fallex* 62: exposição da situação deplorável das tropas alemãs ocidentais em exercício da OTAN em outubro de 1962 pela revista *Der Spiegel*. O então Ministro da Defesa (Bundeswehr), Franz Josef Strauss, apoiado pelo Chanceler Konrad Adenauer, reagiu violentamente, o que culminou em ações de busca e apreensão na editoria do jornal e na casa de seu editor, além do fechamento da redação do periódico por um mês. A reação da sociedade alemã ocidental, inclusive com marchas e protestos públicos, garantiu que a queda de braço entre imprensa e Estado pendesse favoravelmente à liberdade de imprensa, inclusive com importantes alterações legais que protegeram a integridade de jornais e da residência de seus editores.

(ii) Caso *Die Zeit* 63: escândalo relativo a grampos realizados pelo BfV e pelo BND oriundos do Tratado de 1955 entre RFA e OTAN sobre o *Status* das Forças (de Ocupação), que permitia, conforme seu Art. 5º, Parágrafo 2º, às Forças Aliadas interceptar comunicações na Alemanha Ocidental para fins de Defesa. Como resultado do escândalo, foi criada, sobre o Art. 10 da Lei Básica, a Lei G 10, que protegia a privacidade dos cidadãos alemães.

(iii) O escândalo do SPD *Ostpolitik* 70: reportagem do jornal suíço *Basler National Zeitung* expôs que o partido de esquerda *Sozialdemokratische Partei Deutschlands* (SPD), então à frente do governo alemão ocidental, buscou intermédio dos comunistas

italianos para reaproximação com países da Europa oriental. Conforme investigação parlamentar apurou, o BND proveu informações ao partido de oposição *Christlich Demokratische Union Deutschlands* (CDU) sobre essa iniciativa, em um caso de interferência política. Historicamente, o BND era ligado aos partidos de direita na Alemanha ocidental (SHPIRO, 2010).

Da criação até a reforma do BND em 1972, a Inteligência alemã ocidental tratou a imprensa como alvo de operações de Inteligência. A relação com a mídia ficou a cargo da Seção 923, que mantinha contatos regulares com aproximadamente 200 jornalistas na RFA. Em 1972, a Seção 923 foi absorvida pelo recém-criado Escritório de Monitoramento da Mídia, que, na década de 1990, transformou-se no Escritório de Imprensa (HESS, 2012; SHPIRO, 2010).

Abertura defensiva

Desde 1956, os chefes do BND atuaram em busca de legitimidade pública para suas ações e se percebiam em constante estado de incerteza acerca do futuro do serviço, de seu orçamento e de sua autoridade. Para reverter esse quadro, foi desenvolvida a estratégia de Abertura Defensiva, segundo nomenclatura de Shpiro (2010), que se compunha de quatro elementos principais: a) monitoramento da mídia, b) proporcionalidade da resposta c) equilíbrio entre negação e compartilhamento de informações, e d) recompensa a jornalistas, em vez de ameaça.

O BND monitorava a produção da imprensa com duas finalidades: antecipar ou minorar críticas e obter imagem positiva da instituição. O monitoramento interno era feito, inicialmente, pela leitura de jornais na sede em Munique, em Berlim e em Hamburgo, onde informações negativas eram processadas pelo *staff* de imprensa e encaminhadas para resposta superior.

Além disso, o BND adotou abordagem operacional no trato com a mídia alemã, ao recrutar jornalistas, cuja remuneração poderia atingir 900 marcos alemães na década de 1970 (aproximadamente R$ 10.500 mensais em valores atualizados de outubro de 2021). Eles deveriam antecipar notícias negativas, como reportado no caso *Münchner Merkur*, em que o chefe da redação Rudolf Lambrecht foi surpreendido pelo acesso antecipado que o então Presidente do BND, Klaus Kinkel, obteve a dados secretos que o jornal havia recebido. Associações de apoio à imprensa, p. ex., a *Internationale Association Deutcher Medienleut* (Associação de Correspondentes Internacionais da Alemanha, em tradução livre), serviram para cobertura operacional e aproximação com sindicatos de jornalistas. Por fim, monitorou-se a formação de novos grupos de mídia (*Bund Deutscher Publizisten*, criado em 1966, e a *Gesellschaft zur Foerderung Oeffentlicher Verantwortung*,

criada em 1971).

A abordagem também foi executada a fim de se criar imagem positiva do BND por meio de vazamento controlado[1] de dados, manuais e operações para jornalistas de confiança. Isso se destacou na publicação de, pelo menos, três livros dos autores Eva Jentsch, Heiner Emde e da dupla Heinz Höhne e Herman Zolling, cujas publicações apresentaram o BND com mais familiaridade e destacavam a capacidade operacional do órgão. A publicação de Höhne e Zolling, *Pullach Intern*, foi escrita para o semanal *Der Spiegel*, e transformado em livro *best-seller* nos anos 1970.

Além da publicação de livros, o serviço alemão também realizou investidas em rádios e TVs (SCHMIDT-EENBOOM, 1997). E contatou a *Deutsche Welle*, rádio estatal da Alemanha ocidental, e as redes de TV WDR e ZDF, às quais foram entregues materiais secretos para apresentadores de TV a fim de valorizar a capacidade operacional e valor do BND[2].

O BND buscou manter a proporcionalidade de resposta aos críticos conforme o nível de dano, em especial, ao priorizar aspectos políticos aos possíveis danos operacionais. No início de sua existência, em pelo menos duas ocasiões[3], o BND vazou informações sobre falhas de Inteligência do BfV, tanto para fragilizar rivais na burocracia de Inteligência quanto para tentar calar o então presidente do BfV, Günther Nollau, crítico vocal da atuação do serviço externo alemão.

Duas falhas em controlar a narrativa estão expressas nos livros de Erich Schmidt-Eenboom (1997), crítico da história do BND, e de Udo Ulfkotte (apud SHPIRO, 2010), a quem o BND proveu informações, inclusive secretas, mas cujo viés negativo do livro levou a instituição a tentar impedir sua publicação, até mesmo por via judicial. A adoção de medidas legais contra Ulfkotte é destacada exceção, pois o trabalho do Escritório de Imprensa "era conduzido silenciosamente, nos bastidores, e o BND evitava buscar apoio das cortes e do Judiciário principalmente porque suas chefias temiam que a perda de uma batalha judicial poderia abrir as portas para publicações ainda mais adversas" (SHPIRO, 2010, p. 490).

O terceiro elemento da estratégia do BND foi equilibrar o compartilhamento e a negação de informações, e evitar o uso do "nada a declarar". Isso foi realizado por meio da publicação regular de *releases*

1 Vazamentos controlados são informações sigilosas ou secretas entregues a um jornalista ou veículo de mídia por interesse e anuência da cúpula da instituição.

2 Der Spiegel, 47/1994, p. 74. Disponível em: https://www.spiegel.de/spiegel/print/index-1994-47.html. Acesso em: 28 set. 2023.

3 Em 1958, o BND foi acusado de vazar informações para artigo de Maynhardt Nayhauss sobre ação má sucedida de contraespionagem em que CIA e BfV atuaram em conjunto. Em 1972, um dos contatos de imprensa do BND escreveu reportagens críticas à gestão de Nollau no serviço interno. Nollau era adversário público do trabalho do BND.

encaminhados para órgãos de imprensa e pela criação de *newsletter* periódica chamada *Vereinigter Wirtschaftsdiet* (Economia Unida)[4], distribuída a lideranças políticas, econômicas e do Executivo.

Em 1996, sob a presidência de Hansjörg Geiger, o BND criou a figura do porta-voz, encarregado de ser a face pública de interlocução com jornalistas e a sociedade. O Escritório de Imprensa também passou a adotar política mais aberta de entrevistas, conversa de bastidores e preparação de material para mídia. Desde 1999, o BND faz palestras públicas e *briefings*. O *release* para a mídia de 27 out. 2021 foi um resumo da apresentação que o BND, o BfV e a Contrainteligência Militar (MAD) fizeram ao órgão de controle parlamentar alemão. Apresentou as principais ameaças identificadas (extremismo de direita, espionagem e terrorismo), as medidas tomadas para melhorar a eficiência dos órgãos e o trabalho conjunto (REPÚBLICA FEDERAL DA ALEMANHA, 2021).

O quarto elemento na relação do BND com a mídia foi baseada em estímulo via benefícios, desde pagamento regular de salários a outras vantagens, como vazamentos controlados para auxiliar na escalada da reputação de jornalistas e, assim, manter relacionamento de confiança positivo.

Considerações finais sobre o BND

Para Shpiro (2010), não está claro quão bem-sucedida foi a estratégia do BND para a mídia. Embora ela tenha moderado e evitado críticas eventuais, ainda assim, a imprensa *mainstream* mantém postura crítica em relação ao serviço. Politicamente, entretanto, a mudança da sede do BND para Berlim em 2018 demonstra sucesso nas relações com o *establishment* político e o reconhecimento da importância da Inteligência pela sociedade e pelo governo alemães.

Espanha: acesso privilegiado

O Centro Nacional de Inteligência (CNI) é o serviço de Inteligência da Espanha. Criado em 2002, sucessor do *Centro Superior de Información de la Defensa* (CESID, Centro Superior de Informação de Defesa), é um serviço unitário, ou seja, responsável pelas atuações interna e externa. Para os propósitos deste trabalho, serão estudados tanto o CESID quanto o CNI, criados no período democrático espanhol pós-ditatura do general Francisco Franco.

Os serviços de Inteligência espanhóis surgiram e se desenvolveram quase à margem do interesse da sociedade e da imprensa, e focaram sua atuação nas relações com o Executivo. Em razão desse desinteresse, combinado com o

4 Atualmente, o BND mantém um programa chamado Proteção da Economia (Wirtschaftsschutz), em que compartilha informações de interesse com empresas alemãs a fim de resguardá-las contra ações adversas.

reconhecimento burocrático de sua necessidade de existir, o modelo de relação com o público e com a imprensa evoluiu de iniciativas descontínuas e assistemáticas no período do CESID para estratégia de acesso privilegiado para alguns poucos pesquisadores e periódicos, o que culminou em visão positiva do CNI frente ao público.

Histórico

O CESID foi estabelecido em 1979, durante a transição democrática após a ditadura de Franco. Combinou elementos do regime anterior, p. ex., pessoal egresso dos serviços de repressão, com elementos da democracia, p. ex., vinculação ao Ministério da Defesa comandado por um civil. Em sua formação, 100% do pessoal era militar, dominância funcional que se manteve até a extinção, quando esse percentual caiu para 70% em 2002 (NUMERIANO, 2011).

Desde o início, não se questionou, no sistema político espanhol, a necessidade de serviço de Inteligência com capacidade operacional efetiva, principalmente, em razão dos atentados perpetrados pelo *Euskadi Ta Askatasuna* (ETA, Pátria Basca e Liberdade) no fim dos anos 1970 e início dos 1980. A atuação do serviço deveria ser interna e externa, por causa das bases internacionais, em especial na França, dos *etarras* e outros grupos secessionistas (FERNÁNDEZ, 2012).

Apesar disso, a tentativa de golpe militar com apoio de membros do CESID contra o governo socialista de Felipe González em 1982 acarretou mudanças para assegurar maior controle civil. Em 30 set. 1982, Alberto Oliart, Ministro da Defesa (MD), estabeleceu a Ordem Ministerial 15, que colocou o CESID sob alçada do Primeiro Ministro (PM). Em 5 jan. 1984, a Lei Orgânica nº 1 reduziu a autonomia do MD e definiu que, somente com autorização do PM, a Defesa e, por consequência, a Inteligência, poderiam realizar ações de política militar e de defesa. Na mesma legislação, foi criado o controle parlamentar sobre as atividades de Defesa. Ainda em 1984, com o Decreto Real nº 135, estabeleceu-se que o CESID estava organicamente vinculado ao MD, mas funcionalmente ao PM. Para Numeriano, "Esta medida buscava imunizar a área de Inteligência contra a contaminação política militar, blindando-a institucionalmente no seio do governo" (NUMERIANO, 2012, p. 157).

Legislação e relação com a imprensa

Para efeitos da relação com a imprensa, o segredo de Estado na Espanha é protegido, em especial, por três legislações de interesse. A Lei dos Segredos Oficiais (Lei 9, de 5 abr. 1968), alterada pela Lei 48, de 7 out. 1978, e, posteriormente, a lei de regulação do Centro Nacional de Inteligência (CNI), Lei 11, de 6 maio 2002.

Para Rueda Rieu (2012), a legislação espanhola é extremamente restritiva para o acesso aos segredos de Estado, o que afetou significativamente a capacidade de o jornalismo espanhol desvelar e expor informações sobre os serviços secretos. Ele identifica 8 principais fontes de informação sobre o CNI-CESID:

(i) agentes e ex-agentes anônimos;

(ii) vazamentos do próprio governo;

(iii) parlamentares da *Comisión de Fondos Reservados*, da Câmara dos Deputados da Espanha;

(iv) o Gabinete de Imprensa do CNI, em ações de propaganda institucional;

(v) a cúpula do CNI, que teria ampla linha de comunicação de bastidores com jornalistas e editores de periódicos;

(vi) ex-colaboradores e fontes do CNI-CESID, como no caso Tarik Ouazzani[5] e Maria Isabel del Barrío;

(vii) órgãos da burocracia espanhola rivais, como polícias, militares, diplomatas e outros; e

(viii) fontes materiais, como manuais e normas internas do CNI-CESID.

Principais crises com a mídia

A limitação legal não impediu que escândalos reportados pela mídia espanhola na década de 1990 levassem à extinção do CESID e à criação do CNI. Segundo Diáz Fernandez (2012), houve três escândalos principais da Inteligência Espanhola.

O primeiro foi o vazamento dos microfilmes do coronel Perote, chefe do *Agrupación Operativa de Misiones Especiales* (AOME, Grupamento Operacional de Missões Especiais, em tradução livre) de 1982 a 1991, em que foram expostas escutas ilegais de jornalistas, ministros, empresários e políticos; até o Rei Juan Carlos II foi grampeado. Perote possuía ilegalmente 1.245 microfilmes com informações classificadas do CESID. O banqueiro Mario Conde, do banco Banesto, buscou adquiri-los para se alavancar em negociação com o *Banco de España*, que interviera nos negócios do banqueiro por má gestão. As informações dos microfilmes foram entregues à imprensa, em especial ao jornal *El Mundo*, que publicou várias reportagens nos anos de 1995 e 1996 sobre atos ilegais ou questionáveis do CESID.

A estratégia da imprensa foi divulgar as informações aos poucos, pedir confirmação do governo espanhol e esperar. Quando o governo negava algo que estava nos microfilmes, *El Mundo*, *ABC* e *Vanguardia*

5 O caso de Ouazanni foi tentativa de recrutamento de fonte com acesso ao Rei do Marrocos e a possíveis alvos jihadistas via controle do pedido de cidadania espanhola, ao qual o marroquino era postulante. O alvo da tentativa buscou a imprensa. O caso del Barrío foi uma fonte envolvida em crime que foi exposta pelos serviços policiais espanhóis.

publicavam os dados de microfilmes, desmoralizavam e acuavam o governo.

A segunda crise se refere aos Grupos Antiterroristas de Liberação (GAL), paramilitares que participaram de guerra não declarada contra o ETA, e cuja ligação com o governo espanhol sempre fora negada. Os vazamentos provaram a ligação e deixaram o governo socialista em crise com parte de sua base eleitoral na Catalunha e levaram a um mal-estar com o governo francês, visto que parte dos ataques do GAL ocorria nos territórios franceses onde se homiziavam os *etarras*.

O terceiro principal escândalo se refere ao vazamento de operação sobre o Herri Batasuna, partido político cuja ligação com o ETA ainda não era clara em 1998, mas banido posteriormente por integrar a estrutura do grupo terrorista. A exposição do caso acarretou o desmantelamento de operação iniciada pelo CESID em 1992 e expôs o nome de servidores, meios, objetivos e técnicas operacionais, o que, segundo declarações do próprio Centro, causou grave prejuízo operacional à instituição e à segurança de seus servidores pessoalmente expostos.

Como resposta à profunda crise de 1995-1996, caíram o então vice-Primeiro Ministro, Narcís Serra, o Ministro da Defesa Julián García Vargas e longevo o Diretor Geral do CESID, general Emílio Manglano.

Ações de comunicação e criação do CNI

Em 15 abr. 1997, o então diretor do CESID, Javier Calderón, anunciou, à imprensa, plano em três fases para melhorar a imagem institucional do serviço: (i) entrevista para mídia, (ii) publicação de livro, (iii) aparições na televisão.

Nos meses seguintes, concedeu entrevista para o semanal *Tiempo*; deu, à escritora Pilar Urbano, acesso ao CESID, e ela, posteriormente, publicou o livro "*Yo entré en el CESID"*; e, por fim, Calderón participou do programa de televisão "*Caiga quién caiga"* (CQC), da emissora *Telecinco*. Manteve política de portas abertas para políticos, juízes e jornalistas (RUEDA RIEU, 2014). Antes de Calderón, há o registro da reportagem da TV Antena 3, em abr. 1994, em que a equipe de reportagem falava positivamente da atuação do CESID. Segundo Ramon Reig (REIG apud RUEDA RIEU, 2014), foi ação de propaganda institucional travestida de reportagem.

Apesar do esforço descontínuo de melhoria da imagem pública tentado por Calderón, o governo espanhol decidiu encerrar as atividades do CESID e criar o CNI. Para Díaz Fernández, a ausência de qualquer estratégia perene de comunicação com a mídia e a ausência de controle e interlocução parlamentares estimularam a imprensa a administrar a crise conforme

seus próprios interesses, o que não gerou debate propositivo e construtivo para a melhoria do serviço, mas tão somente a punição do centro com cortes orçamentários prejudiciais à capacidade operacional.

Uma das externalidades positivas das crises foi o esforço do Executivo e do Parlamento espanhóis para aperfeiçoar sua Inteligência. Em 2002, o CESID foi extinto, e foi criado o CNI, com legislação de apoio e respaldo de tribunais superiores, adoção de concurso público e aumento do controle civil, com a nomeação do diplomata de carreira Jorge Dezcallar para chefiar a transição e o novo serviço. A mesma lei criou, especificamente, comissão parlamentar de controle de fundos secretos para controle e supervisão das Atividades de Inteligência.

A Lei Orgânica 2, de 6 maio 2002, regulamenta que o CNI pode efetuar medidas de entrada em domicílio e escuta telefônica, desde que autorizados por um juiz designado do Tribunal Supremo. O magistrado deverá autorizar as ações propostas em até 72 horas. Os pedidos do CNI devem contemplar medidas e grau de alcance, fatos motivadores do pedido, a razão da solicitação dos meios especificados, identificação dos alvos, sempre que possível, local e duração das medidas. A inclusão do mais alto nível do Judiciário espanhol no ciclo da Inteligência tentou responder às críticas no parlamento e na imprensa sobre o CESID, geraram maiores controle, transparência e legitimidade às ações operativas do novo órgão e preservaram suas capacidades.

Todas essas medidas parecem ter reduzido a exposição negativa do CNI à imprensa, visto que as ações mais intrusivas da Inteligência espanhola são validadas tanto política quando judicialmente. Ainda que eclodam eventuais escândalos, eles parecem ser de alcance limitado e não afetam a institucionalidade do CNI.

A análise das perguntas dos parlamentares espanhóis em audiências públicas demonstrou que 89% eram baseadas em matérias de jornais (FERNÁNDEZ, 2012). A Assessoria de Comunicação do CIN é vinculada ao Gabinete, e não diretamente ao Diretor Geral. Não se identificou, no sítio eletrônico do CNI, política de comunicação que objetive, explicitamente, estabelecer relações com a imprensa local.

Por outro lado, as matérias escritas sobre o CNI no período 2004-2021 têm apontado maiores foco, profissionalismo, capacidade e sucesso do órgão. Parece haver consenso de que o CNI é órgão competente e necessário. Isso se deve, especialmente, aos êxitos percebidos no combate ao terrorismo *etarra* e jihadista. Matéria no jornal *El Mundo*, responsável pelas principais denúncias acerca do CESID, publicou em 2015:

> *Además, el Centro Nacional de Inteligencia ha potenciado su presencia en las zonas en las que el terrorismo islamista tiene más incidencia.*

> *Una actividad que ha dado enormes resultados a la inteligencia española, proporcionando informaciones relevantes no sólo para nuestro país, sino también para otros Estados europeos* (LAZARO, 2015).

Para a melhoria da percepção pública sobre a Inteligência espanhola, contribuíram audiências públicas e reservadas no parlamento espanhol, posteriormente vazadas para a imprensa, e os casos divulgados de sucesso de prisão de membros de grupos terroristas, em que o CNI trabalhou colaborativamente com a Guarda Nacional. A leitura dos principais jornais no período supracitado indica haver relação colaborativa entre o CNI e *El Mundo*, *El País* e *La Vanguardia* para publicização de sucessos, o que não impede, entretanto, haver reportagens críticas sobre o CNI.

Outro esforço tem sido a publicação de livros e artigos sobre o CNI (ROLDÁN, 2012), em especial de António Fernández Díaz, o principal pesquisador acadêmico sobre Inteligência na Espanha (FERNÁNDEZ, 2018); de Rueda Rieu; de Pilar Urbano, a primeira escritora convidada a conhecer o CESID; e de Pilar Cernuda, que escreveu sobre o papel das mulheres no CNI. A multiplicação de livros com tom positivo sobre o CNI indica abertura para academia e imprensa, cujos profissionais parecem ser selecionados e educados sobre a Atividade de Inteligência. Casos de insucesso, p. ex., a expulsão de equipe operacional do CNI de Cuba em 2010, que lá fora monitorar membros do ETA, são narrados como reveses, e não fracassos ou escândalos.

Considerações finais sobre a Inteligência Espanhola

O apoio político e social para a existência do serviço – fortalecido nas últimas duas décadas pela percepção pública da necessidade de ações efetivas contraterroristas (INGELMO, 2016) –, a boa legislação que apoia o CNI, a legitimidade e a segurança advindas de controle judicial prévio para ações mais intrusivas indicam apoio social e político ao centro. A abertura para academia e imprensa espanholas indicam que o CNI mantém estratégia de relacionamento reservado e focalizado para melhoria de sua imagem pública. A estratégia se baseia em privilegiar acesso tanto às instalações físicas, quanto ao pessoal e às informações específicas por meio de vazamentos controlados. O sucesso do modelo de acesso privilegiado se demonstra pela mudança observada no trato da Inteligência espanhola na imprensa, nas publicações acadêmicas e em livros temáticos.

Israel: exclusão controlada

Histórico

Israel possui três serviços de Inteligência principais: Mossad, abreviação de *Ha-Mōśād le-Mōdī`īn ū-le-Tafqīdīm Meyūhadīm* (Instituto para Informações e Operações Especiais), para atuação externa; o *Sherut haBitachon Haklali* (Serviço de Segurança Geral), conhecido como Shabak ou Shin

Bet, para atuação dentro do território israelense e palestino; e a *Agaf Hamodiin* (Aman), Diretoria de Inteligência Militar, focada em outros serviços militares e no desenvolvimento de capacidade cibernética (EISIN, 2008; SHPIRO, 2010).

A origem do Mossad é a Haganah, organização paramilitar que atuou nos territórios sob protetorado inglês pré-Israel. Ela era responsável por ações de segurança, como proteção dos assentamentos judaicos, e Inteligência, como transporte de imigrantes para a região, compra de armas e munições, ações de influência sobre a mídia internacional, sabotagem de navios ingleses de deportação e contraposição a quaisquer estruturas que se opunham à consolidação do movimento sionista e ao que se tornou Israel. Parte da organização se tornou as Forças de Defesa de Israel, e outra, o Mossad, em 1949.

Exclusão controlada

As forças de segurança de Israel contaram, desde sua criação, com enorme respaldo político, social e legal. Para Shpiro (2010), a estratégia de relação do Mossad com a mídia é de exclusão controlada, que compraz três pontos principais: (i) supressão de publicação de informações operacionais, (ii) ameaça ou punição de imprensa considerada não-cooperativa, e (iii) manipulação da mídia para dissuasão dos inimigos.

Supressão de informações: legislação e cultura institucional

A supressão de informações sobre a atuação da Inteligência é política desde os tempos da Haganah. "Oficiais argumentavam que, apenas com manutenção total do sigilo sobre cada um dos aspectos da organização, os servidores do Mossad poderiam prevalecer frente a chances ínfimas" (MAGEN, 2014). O que costuma ser público em outros serviços era, até recentemente, mantido secreto, p. ex., o nome do diretor geral e a localização do serviço (MAGEN, 2013).

Essa política teve implicações internas e externas. Externamente, ela se alicerça na Lei de Defesa de Emergência, que estabelece revisão da censura militar para todas as informações da mídia que possam acarretar risco a Israel ou às operações de suas Forças de Segurança. Pela legislação, originalmente da ocupação britânica, o governo israelense pode censurar trechos, proibir matérias e até interditar os meios de publicação por determinado período ou em definitivo.

O arsenal legal de censura foi e ainda é utilizado com regularidade e constitui o principal instrumento da estratégia do Mossad (MAGEN, 2013). Os primeiros casos de censura datam do início dos anos 1950, quando Mossad e Shabak fecharam e confiscaram gráficas pertencentes aos grupos clandestinos de Lehi e Ezel, que se

opunham ao governo de Ben-Gurion.

A transição da imprensa israelense para postura crítica aos serviços de segurança e Inteligência se iniciou com as falhas que culminaram na Guerra do Yom Kippur em 1973, quando o exército de Israel estava desprevenido contra os ataques coordenados das potências árabes, até uma imprensa plenamente crítica nos anos 1980, em especial com a invasão do Líbano em 1982 (EISIN, 2008).

Dois casos de reação à censura ilustram a mudança de comportamento. Em 1984, no "Caso do Ônibus 300", dois terroristas palestinos sequestraram um ônibus e foram apreendidos vivos pelo Shabak, conforme registo do jornal *Hadashot*. O comunicado oficial, entretanto, afirmou que não houve sobreviventes palestinos. Por saber que seria censurado pelos militares, o jornal publicou as fotos sem consentimento prévio. Como reação, o governo israelense o fechou por quatro dias, até que recuou devido a intenso protesto da sociedade israelense.

O segundo foi a peça crítica escrita pelo jornal *Há'ir,* de Telaviv, sobre o então diretor do Mossad Nahum Admoni (1982-1989), no qual o jornalista Aluf Benn o descreveu como "inativo e cinzento". Os militares censuraram o artigo, e Benn e o editor Meir Schnitzer apelaram ao Supremo israelense para revogar a proibição. Pela primeira vez, a Suprema Corte israelense estabeleceu precedente que garantiu a liberdade de imprensa para críticas aos chefes do Mossad.

Internamente, o silêncio do Mossad e de seus integrantes foi estabelecido pelo primeiro diretor do serviço, Reuben Shiloah (1949-1952), que adotou a postura de distanciamento total da mídia. Esse insulamento, seguido por quase todos os diretores seguintes, estabeleceu o padrão de conduta tanto para os chefes quanto para os membros da instituição, embora essa política não afetasse a relação com a mídia como instrumento de propaganda, desinformação e dissuasão.

O combate a vazamentos é considerado prioridade. Durante o comando de Shabtai Shavit (1989-1996), estabeleceu-se que todos os servidores deveriam informar contatos prévios com jornalistas, atuais ou mesmo acidentais. Os suspeitos de contatos não autorizados com jornalistas eram submetidos a testes de polígrafo, medida inédita. A regra era transversal, como se evidenciou no caso de Naftali Granot, Diretor Adjunto do Mossad, exonerado em 2007, por suspeita de ter repassado informações para a mídia. O caso, que contou com cooperação do Shabak, foi também exposto no jornal israelense *Yedioth Ahronot*, via vazamento controlado, a fim de se repassar recado interno para total apartamento dos membros da instituição da mídia (MAGEN, 2014).

Ameaças e ações desmobilizadoras

Na metade da década de 1950, usou-se de meios alternativos à censura para lidar com a mídia recalcitrante. O jornalista Uri Avineri, editor do jornal *Haolam Haze*, manifestava-se publicamente contra o *establishment* político e fazia reportagens críticas à atuação do Mossad e seus diretores. Vendo a impossibilidade de dialogar com Avineri, o serviço financiou o jornal Himon para competir com *Haolam Haze* e estrangular financeiramente o jornal. Embora não tenha conseguido encerrar as atividades de Avineri, a ação causou grandes danos econômicos (SHPIRO, 2010).

Outro destaque foi a publicação do livro *By Way of Deception*, do ex-oficial do Mossad Victor Ostrovsky, durante a gestão de Shavit. O livro expõe o funcionamento da organização, treinamento, nomes de agentes, meios de atuação, entre outros. O Mossad adotou duas táticas: (i) acionou colegas de Victor para constrangê-lo, e (ii) apelou aos tribunais do Canadá e dos EUA a fim de tentar censurar a publicação. Essa estratégia deu publicidade inesperada ao livro catapultou suas vendas, e o tornou *best-sellers* por semanas nos dois países apelados.

Manipulação da mídia internacional: propaganda e dissuasão

A relação da Inteligência externa israelense com a imprensa internacional foi pensada desde seu início em termos operacionais, a fim de servir como dissuasão de inimigos. Clila Margen (2014), dissertou sobre a influência dos Diretores Gerais do Mossad na relação entre serviço e mídia, e reconheceu que o grau de liberdade deles é limitado pela cultura institucional de silêncio. Entretanto, há grupo seleto de jornalistas, escolhido por cada um dos diretores, para diálogo e vazamentos seletivos.

O grande idealizador da relação entre serviço e mídia internacional foi o segundo diretor do Mossad, Isser Harel, que entendia a relação com a imprensa internacional como útil para avançar os objetivos da instituição. Ele conjugou o segredo das operações de Inteligência com vazamentos seletivos que ajudaram a criar e consolidar a mitologia do Mossad, a exemplo dos fugitivos nazistas capturados na América do Sul e trazidos clandestinamente para julgamento em Israel.

Seus sucessores, embora mantivessem reserva em relação à imprensa israelense, adotaram a estratégia de vazamentos seletivos, mesmo em face de falhas operacionais, a exemplo da prisão dos

agentes na Noruega pelo assassinato de um garçom em Lillehammer, que acreditavam ser Hassan Salameh, membro do Setembro Negro, participante da preparação dos atentados de Munique.

Outro exemplo da importância dada às ações de propaganda do Mossad se encontra no assassinato de Fathi Shqaqi, fundador da Jihad Islâmica Palestina, em Malta em 1995. A imprensa internacional, normalmente atenta a esses casos, manteve silêncio. Fontes do governo israelense passaram então ao Canal 1 de Israel a informação, para que ela fosse difundida com destaque. Isso ocorreu durante a gestão do mesmo Shavit, que introduziu a aplicação de polígrafos no Mossad para evitar vazamentos não autorizados e atacou judicialmente a publicação de Victor Ostrovsky.

Considerações finais sobre o Mossad

A relação do Mossad com a imprensa israelense prescinde de estratégia proativa (MAGEN, 2017) pelo reconhecimento da sociedade da importância do serviço, pelo respaldo político e legal que a instituição tem e, principalmente, porque o público israelense tem acesso aos resultados positivos da atuação do Mossad via mídia internacional, depois replicada internamente. Concomitantemente, a supressão das notícias negativas, seja por censura judicial ou autocensura da imprensa israelense, ajuda no fortalecimento da imagem de competência e profissionalismo.

Destaque-se também não haver registro de interferência ou envolvimento do Mossad com a política partidária doméstica, diferentemente dos casos estudados anteriormente. Por fim, segundo o ex-Diretor Geral do Mossad Ytzhak Hofi (1974-1982):

> O mistério em que somos envolvidos serve a uma função de segurança muito importante. Ninguém sabe precisamente o que somos capazes de realizar. Atribui-se a nós coisas que nunca poderíamos ou gostaríamos de fazer. Por outro lado, conseguimos fazer coisas que, se alguém soubesse, ficaria espantado. Da nossa perspectiva, nossa inescrutabilidade teve um papel extremamente significativo (MAGEN, 2014, p. 148).

Considerações finais

A relação entre mídia e Inteligência é sempre complexa pela natureza aparentemente oposta de ambos: publicidade e segredo. Nos casos em estudo, foi possível identificar que o primeiro passo para o sucesso da relação entre Inteligência e mídia é a educação da sociedade sobre o porquê de a Inteligência existir e, nesse mesmo sentido, se está cumprindo seu papel. Para que isso possa ocorrer, é necessário capacitar tanto jornalistas quanto membros do parlamento.

A forma e os meios são importantes e foram pensados por cada serviço conforme a realidade e a legislação local. Nos casos europeus, houve abertura de acesso pelos serviços para publicação de

livros por jornalistas e alguma abertura para a academia. Em Israel, o uso do transbordamento das notícias internacionais para nacionais, a educação escolar e o serviço militar obrigatório suprem a lacuna de conhecimento da sociedade sobre o serviço.

Vazamentos controlados, relações especiais com membros da imprensa e esforço de comunicação frente ao sistema político são características comuns aos três casos analisados e contribuem fortemente para uma visão positiva dos serviços, visto que, concomitantemente, educam sobre as Atividades da Inteligência e prestam contas, em especial, sobre os sucessos e eventuais necessidades de aprimoramento do serviço.

Referências

EISIN, M. The Israeli Intelligence Community and the Media. *Journal of Intelligence History*, v. 9, n. 1–2, p. 9–14, 2008.

ESPANHA. *Lei 11, de 06 de maio de 2002*. Regula o Centro Nacional de Inteligência. Disponível em https://www.boe.es/buscar/act.php?id=BOE-A-2002-8628. Acessado em 16 de outubro de 2023.

ESPANHA. *Lei Orgânica 2, de 06 de maio de 2002.* Regula o controle judicial prévio do CNI. Disponível em https://www.boe.es/buscar/act.php?id=BOE-A-2002-8627. Acessado em 16 de outubro de 2023.

ESPANHA. *Lei 9, de 5 de abril de 1968*. Sobre os segredos oficiais. Disponível em https://www.boe.es/buscar/act.php?id=BOE-A-1968-444 . Acessado em 16 de outubro de 2023.

FERNÁNDEZ, A. M. D. The Intelligence Services and the Mass Media in Spain. *Journal of Intelligence History*, v. 9, n. 1:2, p. 89–104, 2012.

FERNÁNDEZ, A. M. D. Spies and security: Assessing the impact of animated videos on intelligence services in school children. *Média Education Research Journal*, v. 56, n. XXVI, p. 81–89, 2018.

HESS, S. German Intelligence Organizations and the Media. *Journal of Intelligence History*, v. 9, n. 1–2, p. 75–87, 5 out. 2012.

HULNICK, A. Openness: Being Public About Secret Intelligence. *International Journal of Intelligence and CounterIntelligence*, v. 12, n. 4, p. 463–483, 2010.

INGELMO, P. El yihadismo nos acabará llevando a la israelización. *Diário de Cadiz,* 29 jul. 2016.

JOHNSON, L. The CIA and the Media. *Intelligence and National Security*, v. 1, n. 2, p. 143–169, 1986.

LAZARO, F. España: 1.200 agentes a la lucha antiyihadista. *El Mundo*, 20 nov. 2015.

MAGEN, C. Strategic Communication of Israel's Intelligence Services: Countering New Challenges with Old Methods**.** *International Journal of Strategic Communication*, v. 1, n. 1, p. 269–285, 12 jul. 2017.

MAGEN, C. Mossad directors and the media: a historical perspective. *Journal of Intelligence History*, v. 13, n. 2, p. 144–160, 2014.

MAGEN, C. The Israeli Mossad and the media: Historical and theoretical perspectives. *Public Relations Review*, v. 39, p. 111–123, 2013.

NUMERIANO, R. *Serviços secretos: a sobrevivência dos legados autoritários*. Recife: Editora Universitária da UFPE, 2011.

REPÚBLICA FEDERAL DA ALEMANHA. *Für eine starke Demokratie und ein sicheres Deutschland,* 27 out. 2021.

ROLDÁN, F. S. Opinión e Inteligéncia. *Instituto Español de Estudios Estratégicos*, n. 45, p. 1–4, 2012.

RUEDA RIEU, F. Las fuentes del periodismo de investigación sobre el servicio de inteligencia CNI. *Estudios sobre el Mensaje Periodístico*, v. 20, n. 1, p. 539-555, 2014.

SHPIRO, S. The Media Strategies of Intelligence Services. *International Journal of Intelligence and CounterIntelligence,* v. 14, n. 4, p. 485–502, 10 nov. 2010.

SCHMIDT-EENBOOM, Erich: Undercover. Colônia/Alemanha: Kiepenheuer & Witsch, 1997.

SCHIMIDT-EENBOOM, Erich: *Schnüffler ohne Nase: der BND – die unheimliche Macht im Staate*. Düsseldorf: Econ, 1993.

Artigo

14

COMO PEGAR UM ESPIÃO

DOI: https://doi.org/10.58960/rbi.2023.18.236

Alfredo Ribeiro Pereira *

Resumo

A espionagem é utilizada na obtenção de informações para apoiar o processo decisório estatal. Os Estados praticam a contraespionagem para proteger seus segredos. Três casos distintos de espionagem (Ana Montes, Brian Regan e os Ilegais) são brevemente apresentados. Trata-se de um caso de infiltração individual, um de empregado descontente e um de rede de espionagem. Apesar de serem muito diferentes, os três casos têm em comum o fato de que foram descobertos a partir de informações fornecidas por fonte recrutada no órgão de Inteligência adversário. O ensaio discute a contraespionagem ofensiva e conclui que uma contraespionagem eficaz requer um esforço de recrutamento de fontes em organizações de Inteligência adversárias.

Palavras-chave: contraespionagem; espionagem; estudo de casos.

HOW TO CATCH A SPY

Abstract

Espionage is used to obtain information to support the state decision-making process. States practice counterintelligence to protect their secrets. Three distinct cases of espionage (Ana Montes, Brian Regan and the Illegals) are briefly presented. These are an individual infiltration case, a disgruntled employee case, and a spy network case. Despite being very different, the three cases have in common the fact that they were discovered based on information provided by a source recruited from the opposing intelligence agency. This essay discusses offensive counterintelligence and concludes that effective counterintelligence requires an effort to recruit sources in opposing intelligence organizations.

***Keywords*:** *case study; counterespionage; espionage.*

CÓMO LOCALIZAR A UN ESPÍA

Resumen

El espionaje se utiliza para obtener información que apoye el proceso de toma de decisiones del estado. Los Estados practican la contra-inteligencia para proteger sus secretos. Se presentan brevemente tres casos distintos de espionaje (Ana Montes, Brian Regan y los Ilegales). Estos son un caso de infiltración individual, un caso de empleado descontento y un caso de red de espionaje. A pesar de ser muy diferentes, los tres casos tienen en común el hecho de que fueron descubiertos en base a información proporcionada por una fuente reclutada de la agencia de inteligencia contraria. El ensayo analiza la

* Mestre em Ciências pela Escola Superior de Agricultura "Luiz de Queiroz" da Universidade de São Paulo (ESALQ/USP). Servidor público federal com experiência em Proteção do Conhecimento.

contra-inteligencia ofensiva y concluye que la contra-inteligencia efectiva requiere un esfuerzo para reclutar fuentes en las organizaciones de inteligencia opuestas.

Palabras clave: *contra-espionaje; espionaje; estudio de caso.*

Introdução

Desde a antiguidade, a espionagem é utilizada na obtenção de informações para apoiar o processo decisório estatal, seja na política externa, econômica, desenvolvimento tecnológico, seja nas operações militares (EFTIMIADES, 2019; BAUER, 2013; SULMASY; YOO, 2007).

Em oposição às atividades de espionagem, os Estados praticam a contraespionagem, visando a anular os esforços do Estado adversário e proteger seus segredos. Nossa intenção aqui é, a partir da observação de casos descritos na literatura, estimular a discussão sobre a contraespionagem e sua eficácia.

A seguir, apresentaremos breves relatos de casos de espionagem. Deve-se observar que, apesar de existirem diferentes definições de espionagem na literatura, adotamos, neste ensaio, a definição elaborada por Hulnick (2004, p. 165) de que a espionagem é "o uso de espiões ou agentes secretos para roubar informações de inimigos, adversários ou concorrentes". E a definição do *Counterintelligence Glossary -- Terms & Definitions of Interest for CI Professionals* de que as atividades de contraespionagem são aquelas atividades projetadas para "detectar, destruir, neutralizar, explorar ou impedir atividades de espionagem" (COUNTERESPIONAGE, 2014, p. 54).

Ana Montes

Ana Belén Montes era uma analista de Inteligência sênior da Agência de Inteligência de Defesa (DIA) dos Estados Unidos da América (EUA), que espionou (e sabotou relatórios sigilosos) para a Inteligência cubana por 16 anos, até ser presa em 21 de setembro de 2001 (DEFENSE PERSONNEL SECURITY RESEARCH CENTER [PERSEREC], 2004).

Altamente eficiente no trabalho, dedicava-se ao estudo de milhares de documentos sigilosos, inclusive na hora do almoço (ROSE, 2019; POPKIN, 2013). Sua dedicação e eficiência lhe rendeu prêmios e distinções concedidos pela DIA, a Agência Central de Inteligência (CIA) e o Exército dos EUA (DE LA COVA, 2007). E, como seu foco de trabalho era a Inteligência militar latino-americana, especialmente a cubana, recebeu o apelido de "Rainha de Cuba" (PERSEREC, 2004, p. 32; POPKIN, 2013). Além dos atos de espionagem, também sabotou relatórios de Inteligência, o que "influenciou a política dos Estados Unidos em relação à América Latina" (FEDERAL BUREAU OF INVESTIGATION [FBI], 2011, p. 5).

A *Dirección General de Inteligencia* (DGI) de Cuba recrutou Ana durante seu o curso de pós-graduação na Escola de Estudos Internacionais Avançados (SAIS) da Universidade John Hopkins em 1984. Na época, ela trabalhava para o Departamento

de Justiça (DE LA COVA, 2007, p. 106).

Normalmente, os espiões são recrutados por causa de seu acesso a informações, organizações ou pessoas de interesse. No entanto, na época do recrutamento, Ana não tinha acesso a informações de interesse significativo (BISHOP, 2016). Assim, "após recrutá-la, o Serviço de Inteligência cubano a preparou para buscar emprego na Agência de Inteligência de Defesa" (CARMICHAEL, 2007, *apud* ANA, 2021). A operação foi um sucesso, pois os cubanos conseguiram infiltrá-la onde queriam e, por 16 anos, ela foi capaz de fornecer informações ultrassecretas relevantes a um custo extremamente baixo.

Porém, no fim dos anos 90 e no início dos anos 2000, Rolando Sarraff Trujillo, um cubano, recrutado pelos EUA (GOLDMAM, 2014), "forneceu informações críticas que levaram à prisão de vários espiões de alto escalão" (MCCOY, 2014).

O FBI foi informado sobre a existência de um funcionário do governo estadunidense que estava espionando para Cuba (DE LA COVA, 2007). No entanto, pouco se sabia além da informação de que o espião estava usando um laptop Toshiba (ROSE, 2019). Em setembro de 2000, o FBI contatou a DIA e compartilhou a informação sobre o laptop (POPKIN, 2013).

Os investigadores da DIA pesquisaram seus funcionários em bancos de dados (POPKIN, 2013) e descobriram que ela havia comprado um laptop Toshiba em uma loja de informática na Virgínia (ROSE, 2019). Então, o FBI iniciou uma investigação completa, que acabou levando a sua prisão (ROSE, 2019) e condenação a 25 anos de reclusão (PERSEREC, 2004).

Brian Regan

Brian Patrick Regan era um sargento reformado da Força Aérea estadunidense (*United States Air Force*), analista de Inteligência, especializado em Inteligência de sinais do *National Reconnaissance Office* (NRA, órgão estadunidense especializado em reconhecimento por satélites), que roubou mais de 20 mil páginas de documentos classificados, com o objetivo de vendê-los a nações estrangeiras, mas foi preso antes de conseguir um comprador (UNITED STATES OF AMERICA [USA], 2001a).

Tinha dislexia e uma personalidade esquisita, sofreu *bulling* na infância e era subestimado pelos colegas (BHATTACHAJEE, 2016). No trabalho, era tido como um idiota, e seus colegas não prestavam atenção nele, o que ironicamente permitiu que diariamente, ele saísse carregando os documentos roubados em uma mochila (SCHNEIDER, 2016).

Brian tinha de "garimpar" compradores, pois não tinha nenhum contato em serviços de Inteligência estrangeiros (BHATTACHAJEE, 2016). Por isso,

utilizando computadores de bibliotecas públicas, buscou endereços e telefones de embaixadas de países árabes nos EUA, na Suíça e na Áustria (USA, 2001b).

Em novembro de 2000, Brian enviou, pelos correios, três pacotes com amostras dos documentos roubados para o consulado líbio, com a intenção de vender todo o material sigiloso roubado por 13 milhões de dólares (SCHNEIDER, 2016). Mas um informante recrutado no Consulado da Líbia em Nova York entregou os pacotes de papéis ao FBI (CHRISTENSEN, 2019).

Segundo Bhattacharjee (2019), por meio da análise do material recebido, foi possível montar um perfil do espião, que apontou para alguém com formação militar, da comunidade de Inteligência dos EUA, provavelmente casado, com filhos, e que cometia erros ortográficos muito peculiares.

A investigação seguiu seu curso e, em 3 de agosto de 2001, Brian foi preso ao tentar embarcar em um voo para a Suíça, carregando informações de locais de mísseis no Iraque e informações de contato de embaixadas na Suíça (PERSEREC, 2008). Finalmente, em fevereiro de 2003, Regan foi condenado a prisão perpétua (FBI, sem data).

Anna Chapman e os ilegais

Anna Vasilyevna Kushchenko (nome de solteira) ou Anna Chapman (nome de casada) era uma espiã russa com ares de *Bond Girl*, que parecia ter saído das telas de cinema.

Ela participou de uma rede de espionagem que atuou por 25 anos nos EUA até seu desmantelamento em 2010, quando o FBI prendeu 11 integrantes, incluindo Anna, na operação *Ghost Stories* (U.S. DEPARTMENT OF JUSTICE, 2010; USA, 2010a). Em pouco tempo, eles se declaram culpados das acusações e foram trocados por quatro presos russos, que espionavam para os EUA e o Reino Unido (FAULCONBRIDGE; BADER, 2010).

Anna e seus colegas eram agentes do *Sluzhba Vneshney Razvedki* (SVR, Serviço de Inteligência Estrangeiro), que, em sua maioria, assumiam identidades falsas e viviam nos EUA com histórias profundas e de longo prazo, operando sem cobertura oficial (USA, 2010b).

Os ilegais geralmente operam como casal, para que possam viver e trabalhar juntos em um país anfitrião e, muitas vezes, têm filhos para aprofundar sua estória-cobertura (USA, 2010a). Anna e um outro agente, Mikhail Semenko, tinham um perfil um pouco diferente, eram solteiros e utilizavam seus nomes verdadeiros (LUCAS, 2012).

Anna chegou aos EUA em 2009, mas o primeiro casal dessa rede chegou em 1985, e, nos 25 anos antes da prisão, outros casais foram chegando (USA, 2010a; BOUDREAUX, 2010). Pelo que se sabe, a rede teria tido acesso ao gabinete da

presidência estadunidense, pois um dos agentes teria trabalhado no planejamento financeiro de Alan Patricof, um arrecadador de campanha com laços estreitos com Bill e Hillary Clinton (DID, 2011).

A investigação estadunidense que levou ao desmantelamento da rede de espionagem começou com informações fornecidas à Agência Central de Inteligência (CIA) pelo coronel Alexander Poteyev, desertor do SVR. Poteyev foi recrutado pelos estadunidenses e, na véspera da prisão dos agentes russos, fugiu para os EUA (POTEEV'S, 2011).

Considerações finais

Dos casos apresentados, observa-se que Ana Montes foi um caso de infiltração individual em um órgão de Inteligência, Brian Regan foi um caso de servidor insatisfeito de órgão de Inteligência, que resolveu roubar e vender segredos, e os "Ilegais" foi um caso de rede de espionagem que se infiltrou na sociedade estadunidense. Ana Montes e a maioria dos agentes "Ilegais" foram altamente competentes, mas Brian Regan e Anna Chapman não. Ana Montes e alguns dos agentes "Ilegais" atuaram por vários anos, mas Brian Regan e Anna Chapman não. Porém, os três casos têm um fato em comum, a descoberta da espionagem começou com informações fornecidas por um recrutado no órgão de Inteligência patrono da operação de espionagem.

Basicamente, existem dois tipos de atividades de contraespionagem, as defensivas e as ofensivas. As defensivas são aquelas "atividades de contraespionagem projetadas para proteger pessoal, operações, tecnologia e informações contra coleta ou exploração por um serviço de Inteligência estrangeiro, em contraste com atividades ofensivas de contraespionagem, que são projetadas para atacar os serviços de Inteligência adversários" visando a infiltração e recrutamento neles (DEFENSIVE, 2014, p. 114).

Segundo Wettering (2000), citado por Harber (2009, p. 229), ''as fontes mais eficazes de identificação de espiões dos EUA são oficiais de Inteligência desertores e os próprios espiões''. Por isso, Harber (2009, p. 228) preconiza que a contraespionagem deve ser ofensiva para ter sucesso e "deve trabalhar para se infiltrar nas redes e organizações".

Esse entendimento não é novo. A contraespionagem agressiva (Nastupatelnost1) foi um princípio orientador da KGB (e agências anteriores), desde a década de 1920, porque é bem-sucedida. O mote era: "Não esperar passivamente para detectar espiões, mas sair agressivamente para encontrá-los" (BAGLEY, 2015, p. 5).

1 "Estilo de atividade de contrainteligência (inteligência), que é proativo e cheio de iniciativa, garantindo o máximo sucesso na luta contra o inimigo" (NASTUPATELNOST, 2002, p. 261).

Na verdade, quando um país não pratica a contraespionagem ofensiva, fica dependente da sorte ou da colaboração de órgãos de Inteligência estrangeiros para identificar espiões que atuam internamente, o que obviamente não é saudável.

O próprio Gabinete do Inspetor Geral do Departamento de Justiça estadunidense, por considerar que o recrutamento de fontes humanas em serviços de Inteligência hostis é a ferramenta mais valiosa para identificar espiões, recomendou ao FBI "dar maior ênfase e fornecer mais recursos para o assinalamento e recrutamento de oficiais de Inteligência em serviços de Inteligência hostis" (U.S. Department of Justice, 2007).

Dos três casos apresentados, mesmo sendo completamente diferentes, ficou evidente a importância de se contar com o dado negado oriundo de serviço de Inteligência adverso, na identificação dos espiões. Uma contraespionagem eficaz requer um esforço de recrutamento de fontes em organizações de Inteligência adversárias.

Referências

BAGLEY, Tennent H. Ghosts of the Spy Wars: A Personal Reminder to Interested Parties. *International Journal of Intelligence and CounterIntelligence*, Londres, Taylor and Francis v. 28, n. 1, p. 1-37, 2015. Disponível em: https://www.tandfonline.com/doi/full/10.1080/08850607.2014.962362. Acesso em: 10 dez. 2020.

BAUER, Deborah Susan. *Marianne is Watching:* Knowledge, Secrecy, Intelligence and the Origins of the French Surveillance State (1870–1914). 2013. Tese (Doutorado em História) – University of California, 2013. Disponível em: https://escholarship.org/uc/item/7rt4z6js. Acesso em: 13 mar. 2023

BHATTACHARJEE, Y. How the FBI tracked down 'the spy who couldn't spell'. *CNN*. 1 Nov. 2019. Disponível em: https://edition.cnn.com/2019/11/01/us/declassified-the-spy-who-couldnt-spell/index.html. Acesso em: 24 jul. 2021.

BHATTACHARJEE, Y. The spy who couldn't spell: how the biggest heist in the history of US espionage was foiled. *The Guardian*. 16 out. 2016. Disponível em: https://www.theguardian.com/world/2016/oct/26/spy-couldnt-spell-how-biggest-heists-us-espionage-history-foiled. Acesso em: 24 jul. 2021.

BOUDREAUX, R. Busted Russian Spy Wants Old Life Back. *The Wall Street Journal*, Nova York, 7 ago. 2010. Disponível em: https://www.wsj.com/articles/SB10001424052748703309704575413600124475346. Acesso em: 10 dez. 2020.

CARMICHAEL, Scott True Believer: Inside the Investigation and Capture of Ana Montes, Cuba's Master Spy. Annapolis: Naval Institute Press, 2007 apud ANA Montes. *In*: WIKIPÉDIA: a enciclopédia livre. Disponível em: https://en.wikipedia.org/wiki/Ana_Montes. Acesso em: 5 abr. 2021.

CHRISTENSEN, C. Review of The Spy Who Couldn't Spell by Yudhijit Bhattacharjee, *Cryptologia*, Londres: Taylor and Francis, 43: 1, 65-68.

COUNTERESPIONAGE. *In*. REAGAN, L. M. (Ed.). *Counterintelligence Glossary -- Terms & Definitions of Interest for CI Professionals.* United States Department of Defense. 2014, p. 54. Disponível em: https://fas.org/irp/eprint/ci-glossary.pdf. Acesso em: 17 dez. 2020.

DE LA COVA, A. Review of Carmichael, S. W. True Believer: Inside the Investigation and Capture of Ana Montes, Cuba's Master-Spy. *History Reviews of New Books*, Londres, v. 35,

n. 3, p. 106, 2007. Disponível em: https://www.researchgate.net/publication/284724926_Review_of_Scott_W_Carmichael's_True_Believer_Inside_the_Investigation_and_Capture_of_Ana_Montes_Cuba's_Master_Spy. Acesso em: 5 abr. 2021.

DEFENSE PERSONNEL AND SECURITY RESEARCH CENTER. Defense Human Resources Activity. *Espionage and Other Compromises of National Security 1975-2008*. 2008. Disponível em: https://www.dhra.mil/PERSEREC/Espionage-Cases .Acesso em: 25 jul. 2021.

DEFENSIVE Counterintelligence Activities. *In*. REAGAN, L. M. (Ed.). *Counterintelligence Glossary -- Terms & Definitions of Interest for CI Professionals.* United States Department of Defense. 2014, p. 114. Disponível em: https://fas.org/irp/eprint/ci-glossary.pdf. Acesso em: 17 dez. 2020.

DID Russian spy get close to infiltrating Hillary Clinton's inner circle? FBI warns of 'new breed' of Moscow agents. *The Daily Mail*, Londres, 1º nov. 2011. Disponível em: https://www.dailymail.co.uk/news/article-2056301/Did-Russian-spy-close-infiltrating-Hillary-Clintons-inner-circle.html. Acesso em: 17 dez. 2020.

EFTIMIADES, Nicholas. On the Question of Chinese Espionage. Brown. *Journal of World Affairs,* Providence, v. 26, n. 1, p. 125-142. .2019. Disponível em: https://bjwa.brown.edu/26-1/on-the-question-of-chinese-espionage/. Acesso em: 21 abr. 2022.

FAULCONBRIDGE, Guy; BADER, Heinz-Peter. Russia, U.S. swap 14 in Cold War-style spy exchange. *Reuters,* Londres, 9 jul. 2010. Disponível em: https://www.reuters.com/article/idUSLDE6680KB20100709. Acesso em: 10 dez. 2020.

FEDERAL BUREAU OF INVESTIGATION. *Higher Education and National Security: The Targeting of Sensitive, Proprietary and Classified Information on Campuses of Higher Education*, 2011. Disponível em: https://www.fbi.gov/file-repository/higher-education-national-security.pdf/view. Acesso em: 24 jul. 2021.

FEDERAL BUREAU OF INVESTIGATION. *Brian P. Regan Espionage*. Disponível em: fbi.gov/history/famous-cases/brian-p-regan-espionage. Acesso em: 24 jul. 2021.

GOLDMAM, A. US Spy Freed by Cuba Was Longtime Asset. *The Washington Post*, 18 dez. 2014. Disponível em: https://www.washingtonpost.com/world/national-security/us-spy-freed-by-cuba-was-longtime-asset/2014/12/17/a3b374c4-8612-11e4-a702-fa31ff4ae98e_story.html?itid=lk_inline_manual_5. Acesso em: 24 jul. 2021.

HARBER, Justin R. Unconventional Spies: The Counterintelligence Threat from Non-State Actors. *International Journal of Intelligence and Counterintelligence*, Londres, Taylor and Francis, v. 22, n. 2, p. 221-23, 2009. Disponível em: https://www.tandfonline.com/doi/pdf/10.1080/08850600802698200. Acesso em: 12 dez. 2020.

HULNICK, Arthur S. Espionage: Does It Have a Future in the 21st Century? *Brown Journal of World Affairs*, v. 11, n. 1, p. 165-73. 2004. Disponível em: https://bjwa.brown.edu/11-1/espionage-does-it-have-a-future-in-the-21-st-century/. Acesso em: 13 mar. 2023.

LUCAS, E. *Deception: the untold story of East-West espionage today*. 1. ed. Nova York: Walker Publishing Company, 2012, pp. 120-139.

MCCOY, T. Cuba deal reveals new clues in case of Ana Montes, 'the most important spy you've never heard of'. *The Washington Post*, 18 dez. 2014. Disponível em: https://www.washingtonpost.com/news/morning-mix/wp/2014/12/18/cuba-deal-reveals-new-clues-in-case-of-ana-montes-the-most-important-spy-youve-never-heard-of/. Acesso em: 12 dez. 2020.

MITROKHIN, Victor. *KGB Lexicon:* The Soviet Intelligence Officers Handbook**.** London: Routledge, 2002.

POPKIN, J. Ana Montes did much harm spying for Cuba. Chances are, you haven't heard of her. *The Washington Post*. 18 abr. 2013. Disponível em: https://www.washingtonpost.com/sf/feature/wp/2013/04/18/ana-montes-did-much-harm-spying-for-cuba-chances-are-you-havent-heard-of-her/. Acesso em: 12 dez. 2020.

POTEEV'S case: traitor caused $ 50 million damage but could not deceive the authorities with his Ukrainian mistress. *Newsru.com*, Moscou, 28 jun. 2011. Disponível em: https://www.newsru.com/russia/28jun2011/poteev.html. Acesso em: 17 dez. 2020.

ROSE, S. Cold War Cuban Spies in the USA in the 1980s – The Case of Ana Montes. *History is Now Magazine*. 26 fev. 2019. Disponível em: http://www.historyisnowmagazine.com/blog/2019/2/24/cold-war-cuban-spies-in-the-usa-in-the-1980s-the-case-of-ana-montes#.YF-f6FVKj3g=. Acesso em: 17 dez. 2020.

SCHNEIDER, H. Treason the Easy Way. *The Wall Street journal*. 22 dez. 2016. Disponível em: https://www.wsj.com/articles/treason-the-easy-way-1482446149. Acesso em: 25 jul. 2021.

SULMASY, Glenn; YOO, John. Counterintuitive: Intelligence Operations and

International Law. *Michigan Journal of International Law*, Ann Arbor, v.28 n.3, p.625-638, 2007. Disponível em: https://repository.law.umich.edu/mjil/vol28/iss3/6. Acesso em: 03 abr. 2022

U.S. DEPARTMENT OF JUSTICE. Ten Alleged Secret Agents Arrested in the United States. *Justice News*, 28 jun. 2010. Disponível em: https://www.justice.gov/opa/pr/ten-alleged-secret-agents-arrested-united-states. Acesso em: 8 set. 2021.

U.S. DEPARTMENT OF JUSTICE. *A Review of the FBI's Progress in Responding to the Recommendations in the Office of the Inspector General Report on Robert Hanssen.* 2007. Disponível em: https://oig.justice.gov/sites/default/files/archive/special/s0710/index.htm. Acesso em: 27 fev. 2021.

UNITED STATES OF AMERICA. Southern District of New York. *United States of America X "Christopher R. Metsos", "Richard Murphy", "Cynthia Murphy", "Donald Howard Heathfield", "Tracey Lee Ann Foley", "Michael Zottoli", "Patricia Mills", "Juan Lazaro" and Vicky Pelaez*. 27 de junho de 2010a. Disponível em: https://www.justice.gov/sites/default/files/opa/legacy/2010/06/28/062810complaint2.pdf. Acesso em: 28 dez. 2020.

UNITED STATES OF AMERICA. Southern District of New York. *United States of America X Anna Chapman e Mikhail Semenko*. 27 de junho de 2010b. Disponível em: https://www.justice.gov/sites/default/files/opa/legacy/2010/06/28/062810complaint1.pdf. Acesso em: 28 dez. 2020.

UNITED STATES OF AMERICA. District Court for the Eastern District of Virginia. *United States of America v. Brian P. Regan, No. CRIM. 01-405-A*. *Criminal Complaint*, August, 2001a. Disponível em: https://fas.org/irp/ops/ci/regan_complaint.html. Acesso em: 25 jul. 2021.

UNITED STATES OF AMERICA. District Court for the Eastern District of Virginia. *United States of America v. Brian P. Regan, No. CRIM. 01-405-A*. *Indictiment*, October 23, 2001b. Disponível em: https://fas.org/irp/ops/ci/regan_indict.html. Acesso em: 25 jul. 2021.

WETTERING, Frederick L. Counterintelligence: The Broken Triad. *International Journal of Intelligence and Counterintelligence*, v. 13, n. 3, p. 265-300. Londres: Taylor and Francis, 2000. Disponível em: DOI: 10.1080/08850600050140607. Acesso em: 28 dez. 2020.

Artigo

15

NOVAS TECNOLOGIAS: INIMIGAS OU ALIADAS?
A atividade de Inteligência de Estado e a proteção dos direitos da personalidade

DOI: https://doi.org/10.58960/rbi.2023.18.240

Rogério Borges Freitas *
Rodrigo Valente Giublin Teixeira **

Resumo

A sociedade contemporânea poderia ser definida como a sociedade da informação, pela elevada produção de dados. Reúne como qualidades distintivas a tecnologia, a velocidade na comunicação, excesso de consumo e a globalização das relações. É nesse clima que está inserida a sociedade do século XXI, marcada por profundas desigualdades e sistemáticas violações de direitos individuais, entretanto, deslumbrada com inovações tecnológicas. A Atividade de Inteligência de Estado existe para assessorar o mais alto nível decisório de um país, de forma isenta, com informações que ajudem a reduzir as incertezas de quem tem a responsabilidade de tomar decisões estratégicas. É nesse contexto que este estudo transita: busca-se analisar como a criação de uma unidade de Inteligência no âmago dos órgãos públicos pode garantir a obtenção de informações confiáveis para a correta tomada de decisões para proteção dos direitos da personalidade.

Palavras-chave: tecnologia; Atividade de Inteligência; direitos da personalidade.

NEW TECHNOLOGIES: ENEMIES OR ALLIES?
State Intelligence activity and the protection of personality rights

Abstract

Contemporary society could be defined as the information society, due to the high production of data. It brings together as distinctive qualities technology, communication speed, excess consumption and the globalization of relationships. It is in this climate that the society of the 21st century is inserted, marked by profound inequalities, systematic violations of individual rights, but dazzled by technological innovations. Intelligence exists to advise at the highest level of decision-making in a country, in an impartial manner, with information that helps reduce uncertainty among those responsible for making strategic decisions. It is in this context that this study moves: it seeks to analyze how the creation of an intelligence unit in which public bodies can guarantee the obtaining of reliable information for the correct decision-making to protect the rights of the personality.

Keywords: *technology; Intelligence Activity; personality rights.*

* Mestre em Direito pela Universidade Cesumar (UniCesumar). Doutorando em Direito no programa de pós-graduação em Ciências Jurídicas pela UniCesumar. Defensor Público do Estado de Mato Grosso.

** Mestre em Direito pela Universidade Estadual do Paraná (UEL). Doutor em Direito pela Pontifícia Universidade Católica de São Paulo (PUC/SP). Professor Titular da Universidade Cesumar (UniCesumar). Advogado.

NUEVAS TECNOLOGÍAS: ¿ENEMIGOS O ALIADOS?
La actividad de Inteligencia del Estado y la protección de los derechos de la personalidad

Resumen

La sociedad contemporánea podría definirse como la sociedad de la información, debido a la alta producción de datos. Reúne como cualidades distintivas la tecnología, la velocidad de comunicación, el exceso de consumo y la globalización de las relaciones. Es en este clima en el que se inserta la sociedad del siglo XXI, marcada por profundas desigualdades, violaciones sistemáticas de los derechos individuales, pero deslumbrada por las innovaciones tecnológicas. La inteligencia existe para asesorar al más alto nivel de decisión de un país, de manera imparcial, con información que ayude a reducir las incertidumbres de los responsables de tomar decisiones estratégicas. Es en este contexto en el que se mueve este estudio: busca analizar cómo la creación de una unidad de inteligencia en el seno de los organismos públicos puede garantizar la obtención de información confiable para la correcta toma de decisiones para proteger los derechos de la personalidad.

Palabras clave: *tecnología; Actividad de Inteligencia; derechos de la personalidad.*

Introdução

A sociedade contemporânea poderia ser definida como a sociedade da informação. Isso porque possui como característica fundamental a elevada produção de dados relativos às notícias de interesses gerais, às ciências, às reflexões sobre as diversas áreas em torno da natureza, à propagação dos limites do conhecimento humano, aos acontecimentos ou às mudanças recentes em todas as áreas do saber. Reúne como qualidades distintivas a tecnologia, a velocidade na comunicação, o excesso de consumo e a globalização das relações. Essas características são evidenciadas, por exemplo, na política, na economia, na saúde, no cotidiano, ou seja, tudo que ocorre de novidade e passa a circular através da rede mundial de computadores, em sites, blogs, mídias sociais etc., com impacto imediato a milhões de pessoas ao redor de todo o mundo.

O elevado número de informações concentradas em bancos de dados públicos e privados, armazenam milhares de informações sobre o aspecto reservado da vida das pessoas em todas as áreas, tais como as movimentações bancárias, fiscais, empresariais, tributárias, familiares, todas contendo dados considerados sensíveis – que envolvem, em muitas situações, direitos da personalidade –, porque quando utilizados em cruzamento de informação são capazes de identificar e individualizar as pessoas dentre outras semelhantes no universo em que estão inseridas. Essas informações definem suas preferências, suas habilidades, suas visões de mundo, suas intenções financeiras, aptidões ao empreendedorismo, as relações com o Estado – sem contar os vínculos socioafetivos e familiares formados.

A produção e o armazenamento de dados sensíveis na sociedade da informação são vitais para que as relações se desenvolvam. A democracia exercida pelo processo eleitoral, o funcionamento das administrações públicas, os julgamentos nos tribunais, as transações bancárias, as operações empresariais, os relacionamentos sociais por meio de contratos que a todo instante são celebrados, têm criado uma imensurável quantidade de informações que podem ser captadas e utilizadas indevidamente.

O volume de informações constantes, por exemplo, nos bancos de dados de contribuintes da Receita Federal é imenso. Por outro lado, a quantidade de informações que os grandes grupos econômicos do campo tecnológico (*Big Techs*) detêm de seus clientes consumidores – por exemplo, *Google, Facebook, Apple, Amazon, Microsoft, Twiter, Instagran, TikTok, Youtube* – é estarrecedor. É nesse clima que está inserida a sociedade do século XXI, marcada por profundas desigualdades e sistemáticas violações de direitos individuais, entretanto, deslumbrada com inovações tecnológicas. No horizonte desponta a intensa produção

de dados sobre os gostos, as objeções, as inclinações e os comportamentos dos usuários do meio ambiente virtual.

Por meio do uso de algoritmos bem calibrados, ao cruzar os dados obtidos, depois de serem tratados, é possível estabelecer perfis de compras, preferências, aversões, apresentar *marketing* personalizado, intensificar o volume de publicidade e propagandas, explorar a crença, manipular opiniões políticas para se fazer gostar da opinião deste ou daquele candidato. São inúmeras as possibilidades de se direcionar os dados pessoais para o bem ou para o mal. Pascual Serrano (2022)[1], alerta para o poder que essas ferramentas representam nas mãos de pessoas mal-intencionadas.

O poder econômico dos conglomerados empresariais ligados à tecnologia se materializou diante de nossos olhos de modo irresistível e irreversível (HARDT; NEGRI, 2006, p. 60). O mercado global, assim como os microcircuitos de produção, quando interligados, fez nascer uma nova estrutura de comando, ou seja, uma nova supremacia, na forma de um poder supremo que governa o mundo. Reunir informações sobre os usuários se tornou uma atividade mercantil e se observou que transformar a informação em conhecimento, aumenta o poder dos conglomerados de tecnologia.

Nesse contexto, o presente estudo se volta à atuação estratégica que se desenvolve através da implementação de um serviço de inteligência capaz de reunir elementos de informações verdadeiras, originados de fonte de confiança, em condições de fornecer aos agentes políticos, ou seja, àqueles que formam a vontade superior do Estado, os elementos imprescindíveis para a tomada de decisão correta na busca do melhor interesse público. A Atividade de Inteligência de Estado existe para assessorar o mais alto nível decisório de um país, de forma isenta, com informações que ajudem a reduzir as incertezas de quem tem a responsabilidade de tomar decisões estratégicas.

O serviço de Inteligência é responsável por coletar essa informação e subsidiar a tarefa dos agentes políticos na correta decisão de Estado. Deve atender precipuamente ao Estado, não se colocando a serviço de grupos, ideologias e objetivos mutáveis e sujeitos às conjunturas político-partidárias. É uma atividade fundamental para construir um conhecimento antecipatório de ameaças ou identificar oportunidade para que o Estado assegure uma posição vantajosa do cidadão em face dos perigos invisíveis que há na sociedade da informação. A sociedade dos dias atuais está inserida em uma atmosfera de insegurança, na qual o cidadão nunca tem certeza de nada, por exemplo, quando as empresas comerciais, bancos ou planos de saúde

1 Disponível em: https://pascualserrano.net/la-verdad-sobre-los-topicos-contra-china-que-se-promueven-en-occidente/ Acesso em: 13 nov. 2023.

adotam um comportamento abusivo em face ao usuário, este não consegue por si só defender seus direitos violados.

É nesse contexto que este estudo transita: busca-se analisar como a criação de uma unidade de Inteligência no âmago dos órgãos públicos pode garantir a obtenção de informações confiáveis para a correta tomada de decisões nos mais variados cenários de atuação do ente público estatal.

A sociedade da informação e a produção de dados sensíveis

A sociedade da informação impõe o debate sobre a tutela jurídica do meio ambiente digital. No tocante a produção dos dados sensíveis nesta sociedade emerge a temática da confiança do indivíduo no Estado, em um contexto de cibercidadania — neologismo empregado para se referir à conduta dos indivíduos no espaço virtual. Em outras palavras é o comportamento ético das pessoas na internet. O ambiente virtual tem consumido com mais intensidade o tempo das pessoas no mundo concreto, por isso, é fundamental discutir o exercício da cidadania no meio digital.

Impõe-se observar que o conceito de cibercidadania pode ser encarado doravante como direito humano de terceira geração e o acesso à internet em alta velocidade se configura como condição de possibilidade para se garantir a efetiva inclusão digital. Nascimento e Neto (2013, p. 70) defendem que: "a evolução das Tecnologias da Informação e Comunicação – TIC – é uma das responsáveis pelas grandes mudanças que a sociedade contemporânea vem passando ao longo das últimas décadas". Mais adiante, prossegue argumentando que "com o desenvolvimento e popularização da internet, criou-se um novo espaço público, caracterizado por sua liberdade, pela inimaginável quantidade de informações, pela possibilidade de comunicação em escala global e em tempo real" (*ibidem*).

Neste contexto, as novas tecnologias resvalaram nos direitos humanos, causando uma fissura que deu origem a novos conceitos e à necessidade de adaptação de antigos termos, como é o caso do exercício da cidadania no ambiente virtual. "A sociedade está em constante evolução, em especial no que se refere aos avanços científicos e tecnológicos advindos da pós-modernidade, o que acarreta inúmeras mudanças no meio social e nas relações interpessoais", como afirmam Gregório e Teixeira (2023), ao abordarem o reconhecimento dos novos direitos da personalidade e a efetividade do acesso à justiça na pós-modernidade.

Como bem acentua Pérez Luño (2018, p. 44-48), a projeção da informática e do estruturalismo na análise do conceito dos direitos humanos, impôs transição das formas econômicas, sociais e políticas do século XIX para os dias de hoje e resultou numa importante mutação no significado,

assim como no alcance dos direitos humanos. O autor contextualiza o debate sobre os direitos humanos em confronto com a fundamentação filosófica e suas implicações jurídico-políticas.

Disso resulta, segundo entende o autor, que a tecnologia passou a ser uma parte integrante da vida humana, causando profundas mudanças no modo de comunicação e na velocidade da transmissão do pensamento humano. Desencadeou comportamentos narcisistas com a elevação do fenômeno da preocupação com a aparência, o que importa é ver e ser visto nas redes sociais. Sem contar o impacto nas relações empresariais, comerciais e sociais, por meio da formação de novas corporações, novos meios de se praticar o comércio e a forma como as pessoas passaram a se relacionar.

Em outro trabalho, Perez Luño (2014) afirma que, a partir das tecnologias de comunicação pela internet, surgiu a aplicação do conceito de governo eletrônico. Foram constituídas novas plataformas de relacionamento entre a Administração Pública e a sociedade. Este é um exemplo do que o referido autor entende por e-cidadania:

> (...) na vida política e cívica mais recente tem havido importantes apelos de massas feitos por meio das Redes Sociais e das mensagens móveis. É um fenômeno que influenciou notadamente a situação política de alguns países islâmicos: Egito, Tunísia, Líbia, Síria; (...) do Movimento 15-M, na Espanha, e de outros análogos registrados na Europa, na Ásia e na América, que contribuem para a atribuição de relevância máxima à reflexão sobre a incidência das novas tecnologias e das tecnologias de informação e comunicação na vida política atual (PÉREZ-LUÑO, 2014, p. 10).

Despertou-se a atenção aos direitos humanos, porque por meio da internet as pessoas tendem a se mobilizar contra governos arbitrários. A força individual do cidadão se potencializa quando encontra outros milhares de apoiadores. O autor destaca o fenômeno que influenciou a política dos países islâmicos no norte da África com a consequente queda de antigos regimes de governo. O uso amplamente difundido das redes sociais e de outros meios de comunicação foi capaz de desestruturar governos que perduraram no poder por décadas, por isso a importância de discutir o impacto das novas tecnologias na revitalização da democracia.

Sob outra perspectiva, Fermentão e Thomazini (2021, p. 127-142), ao refletirem sobre o contexto tecnológico da sociedade contemporânea, salientam que "a sociedade se reestrutura de tempos em tempos", o que varia de acordo com "a cultura, a forma de pensar dos indivíduos, com o avanço da tecnologia, com os hábitos e jeitos de viver, que faz com que a comunidade caminhe para rumos diferentes e não fique estagnada." A perspectiva das autoras aponta para eventuais dificuldades entre gerações e a disrupção, ou seja, a interrupção do curso normal de um processo entre as gerações de uma época

anterior. Em certa medida as pessoas mais idosas poderiam ser escanteadas por não acessarem a tecnologia atual.

Nesse cenário, convém destacar que a educação da cidadania digital, isoladamente, não basta para melhorar o ambiente virtual: é preciso o estabelecimento de leis cibernéticas. Isto é, a produção dos dados sensíveis na sociedade contemporânea, a partir do desenvolvimento das tecnologias digitais de informação e comunicação, requer a atenção legislativa. A partir do aprofundamento teórico e da consolidação do vínculo de confiança, no que tange à coleta, armazenamento e tratamento dos dados sensíveis, é que se poderá compreender o tema com mais lucidez. É esperado que se obtenha novas interpretações com elementos facilitadores para auxiliar a solução das intrincadas questões que ainda carecem de uma resposta jurídica.

Com efeito, revela-se legítimo dentro desse cenário levantar discussões sobre a produção de dados sensíveis do ponto de vista de informações estratégicas que merecem uma proteção especial por albergarem direitos da personalidade. Elementos de identificação pessoal, tais como: saúde, inclinação política ou ideológica, orientação sexual, gostos, preferências, capacidade financeira, são dados que não podem ser descuidados. Washington Platt (1974, p. 83), quando abordou o processo de produção de informações estratégicas como processo intelectual, destacou que "em cada caso temos uma massa de dados para exame, alguns são válidos, outros nada têm a ver com o caso, outros relacionam-se remotamente com o assunto".

Isso significa dizer que alguns dados são verdadeiros, outros falsos, e outros parcialmente verdadeiros. Desta forma, os dados devem ser selecionados, avaliados, interpretados e integrados. Após a formulação de uma hipótese – que dever ser entendida como uma resposta preliminar ao problema que se pretende responder – os elementos captados devem compor um quadro coerente da situação. Havendo nexo entre os fragmentos da informação será possível obter conclusões e verificá-las. O produto final deve ser exposto de modo claro a fim de permitir classificar o grau de confiança que se pretende atribuir ao processo de formação da informação estratégica realizada.

O tema envolvendo o tratamento de dados sensíveis ainda depende de maior exploração na academia. Em pesquisa ao Banco de Tese da Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes), entre os anos de 2020 a 2023, apenas quatro teses de doutorado abordaram diretamente a questão dos dados pessoais.

Chiara Antônia Spadacini de Teffe (2022), escreveu a tese intitulada "Dados pessoais sensíveis: uma análise funcional da categoria e das hipóteses de tratamento". A tese foi

apresentada para a Universidade Estadual do Rio de Janeiro e abordou a ampliação da informação pessoal na contemporaneidade e os riscos de seu titular sofrer interferências indevidas em sua liberdade e tratamentos discriminatórios ilícitos ou abusivos. Destacou a importância de se estabelecer uma categoria especial de informações: os dados sensíveis. Em seguida, discutiu-se a possibilidade de serem qualificados dados como altamente sensíveis, em razão, por exemplo, da hipervulnerabilidade de seus titulares e do conteúdo que guardam.

Tania Giandoni Wolkoff Giorgi (2021), por sua vez, abordou o tema com a tese "A era da comunicação digital: a necessidade de uma política nacional de inteligência artificial", apresentada para a Pontifícia Universidade Católica de São Paulo, na qual discorreu sobre o momento em que as relações humanas outrora desenvolvidas a partir de uma vida associativa predominantemente presencial passam cada vez mais a serem regidas por máquinas, aplicativos, redes sociais, *hardwares*, *softwares*, internet, *cloud computing*, aprendizado profundo, redes neurais de computadores, dados e algoritmos. O estudo sobre novas tecnologias despertou preocupações sobre a segurança na coleta, manipulação, tratamento, arquivamento e descarte de dados pessoais, inclusive dados sensíveis, o que torna imprescindível a compreensão a respeito dos marcos legais sobre proteção de dados no Brasil, da existência da tecno regulamentação da Inteligência Artificial e consequentemente de frequentes ofensas aos direitos fundamentais. Assim, propôs uma Política Nacional de Inteligência Artificial em consonância com os princípios fundantes do Estado e construída com base na lei, na sua implementação através de adequadas políticas públicas e sobretudo a partir da revisitação da capacidade humana de argumentar e resistir.

Silvia Helena Picarelli Goncalves Johonsom Di Salvo (2022), apresentou a tese nominada de "Direitos e garantias da proteção de dados pessoais tratados pela Administração Pública brasileira: o piso da proteção normativa". A tese foi apresentada para a Universidade de São Paulo e abordou o tratamento de dados pessoais pela Administração Pública brasileira sob a ótica do regime jurídico-normativo à luz da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD). Apresentou os tipos morfológicos que compõem o sistema normativo brasileiro de tratamento de dados pessoais pela Administração Pública e os desafios que confrontam esse sistema. Além disso, destacou a proteção normativa, a partir de estratégias sistematizadas em consonância com a morfologia do regime de tratamento de dados pessoais pela Administração Pública. A autora concluiu "que as manifestações de poder estatal pela digitalização têm efeitos sensíveis para o comportamento individual e social, induzindo comportamentos antinaturais no indivíduo em razão da vigilância" (DI

SALVO, 2022, p. 8).

Maria Regina Detoni Cavalcanti Rigolon (2022), apresentou a tese "Revisão de decisões automatizadas na Lei Geral de Proteção de Dados Pessoais" para a Universidade do Estado do Rio de Janeiro. Discorreu sobre o regime jurídico da revisão de decisões automatizadas, previsto pela Lei Geral de Proteção de Dados Pessoais. Concentrou atenção a partir dos estudos de Stefano Rodotà sobre o diagnóstico da "ditadura dos algoritmos", com a necessidade de desenvolver prerrogativas para a proteção da pessoa, em atenção às premissas do direito civil-constitucional, para investigar se a revisão de decisões automatizadas, tal como concebido na LGPD. Defendeu a privacidade até a concepção de proteção de dados pessoais como direito fundamental autônomo. A insuficiência da categoria de dados sensíveis foi apresentada com o propósito de demonstrar que a proteção da pessoa, no campo das decisões automatizadas, está associada à discriminação, por exemplo, das minorias e dos grupos vulneráveis.

Nesse percurso, é correto afirmar que a tutela dos dados hipersensíveis e a proteção da personalidade da pessoa natural ainda é um campo com lacunas que não foram colmatadas pela academia. Ante a relevância do tema versado, vale registrar os argumentos de Otero e Rodrigues (2018, p. 257-287), em relação à discriminação ambiental e à proteção das minorias excluídas pela sociedade contemporânea. As pessoas buscam aceitação em suas relações interpessoais, por exemplo, na família, no trabalho e na sociedade. A desigualdade econômica e cultural escanteia seres humanos e os torna excluídos do ambiente social. A situação de desamparo, afastando-os para longe dos olhos da maioria, geralmente para áreas urbanas longínquas e desprovidas de infraestrutura urbana, configuram o que os autores denominam de discriminação ambiental.

Tarcízio Silva (2022), pesquisador da área da comunicação, reflete sobre a questão do racismo algorítmico, inteligência artificial e discriminação nas redes digitais, e as inquietações tais como: reconhecimento facial, filtros para *selfies*, moderação de conteúdo, *chatbots*, policiamento preditivo e escore de crédito. O autor busca respostas para saber o que pode ocorrer quando as máquinas e programas apresentam resultados discriminatórios. Investiga se os algoritmos podem ser calibrados para serem racistas ou se trata apenas de erros inevitáveis. Ao final procura apurar a responsabilidade entre humanos e máquinas e como combater os impactos racistas das tecnologias que automatizam o preconceito.

Além dos desafios financeiros, pessoas que vivem, por exemplo, nas favelas, nas tribos indígenas e aqueles que estão encarcerados possuem grandes limitações de acesso à

justiça, paralelamente a outros grupos que também são vitimados pela desigualdade estrutural, como os indivíduos que são portadores de deficiência, soropositivos etc. Além desses, pode-se mencionar aqueles indivíduos que estão morando nas ruas e, em certa medida, as pessoas idosas, que também não possuem recursos tecnológicos adequados para exercerem seus direitos na sociedade contemporânea.

Muito precisa, quanto a esse ponto, a lição de Hironaka (2006, p. 120), que propõe "impedir a opressão do fraco pelo forte, do tolo pelo esperto, do pobre pelo rico." A distribuição da justiça não pode ser distinta para quem é abastado financeiramente e para quem é carente. Trata-se de um valor essencial à democracia para minimizar as deficiências para que todos tenham as mesmas condições de acesso. A orientação da "ética da situação", expressão utilizada por Miguel Reale (2002, p. 8), que indica que a noção de sujeito de direitos se perceba em sua essencial pluralidade. Engloba-se o rico e o pobre, o empresário e o desempregado, a grande corporação econômica e os adolescentes em situação de risco, o contratante forte e contratante débil, o latifundiário e o sem-terra, o consumidor e o fornecedor, enfim, o ser humano em suas circunstâncias, sempre urgentes e concretas.

As novas performances da Administração Pública contemporânea passam pela criação de uma unidade de Inteligência. O conhecimento advindo da informação estratégica pode ter duas utilizações: serve para uso preventivo, como forma de evitar um dano ou defensivo quando há resistência a ataque (SHERMAN, 1967, p. 147). Zelar pelos dados sensíveis da população fragilizada é um caminho necessário para progredir no modelo de se proteger os indivíduos vulneráveis. Pessoas que estão nessas situações, como, por exemplo, na área da saúde, os deficientes — físicos ou mentais — e os encarcerados, podem receber a proteção necessária da Administração Pública para que seus direitos não sejam sistematicamente violados. Por isso, a reunião de informações e a produção do conhecimento conduz a uma gestão com absoluto rigor de determinação nas decisões (SIQUEIRA; SANTOS; SANTOS, 2021).

A Atividade de Inteligência se destina a buscar informações para subsidiar a tomada de decisões. Isto é, o administrador público que reunir maiores informações sobre o caso concreto em análise, em tese, terá melhores condições de obter êxito na proteção dos direitos destas pessoas. "Afinal, o Estado e a sociedade precisam ser protegidos, e os tomadores de decisão nas mais altas esferas da Administração Pública necessitam de assessoramento nos moldes do realizado pelos serviços secretos" (GONÇALVES, 2008, p. 591-607).

Esse novo regime de atuação exige uma análise aprofundada da tutela judicial e

extrajudicial dos direitos da personalidade das pessoas hipossuficientes no contexto da cibercidadania (FORNASIER, 2020). O exercício da teledemocracia por meio das tecnologias de informação e a proteção dos dados hipersensíveis das pessoas hipervulneráveis se afiguram como recorte para se investigar o impacto da criação dos serviços de Inteligência no campo da Administração Pública, tema com o qual se ocupa o tópico a seguir.

A implementação de serviços de Inteligência no âmbito da Administração Pública e a tutela dos direitos da personalidade

"Decisões importantes devem ser tomadas em meio a uma névoa de incerteza" (FREYTAG-LORINGHOVEN, 1986, p. 79). O General-de-divisão Barão Hugo von Freytag-Loringhoven, do Exército Alemão, asseverou aos integrantes do Estado-maior, que na essência a guerra é o domínio da incerteza. A afirmação merece reflexões porque nem sempre é possível ter com clareza todos os elementos em mãos para tomar uma decisão importante, após avalição de todas matrizes de risco mapeadas. A implantação de um serviço de Inteligência no âmbito da Administração Pública pouparia os riscos que gestor público está exposto se fossem reunidos em um relatório de Inteligência as principais informações, como assessoramento, a fim de que possa visualizar o campo decisório com clareza.

Examinar o presente assunto evidencia que além da concentração de informações relevantes para tomada de decisão, a contrainteligência poderia antecipar e evitar ameaças que possam comprometer a ações de determinada Instituição Pública. A implantação de um serviço de contrainteligência na estrutura de um órgão público de relevância nacional, protegeria contra ameaças externas tais como atividades de espionagem e vazamento de dados sensíveis, bem como identificaria indivíduos com intuito nocivo aos interesses públicos. Jorge Bessa (2009, p. 58) definiu a contrainteligências como sendo "um componente fundamental da Atividade de Inteligência, já que ela é a responsável pela proteção do país contra as ameaças externas de qualquer ordem"; ademais, ela também se presta a "defender a própria organização das atividades de espionagem e infiltração por parte dos serviços de inteligência estrangeiros" (*ibidem*).

Não se pode desconhecer, a propósito do tema aqui abordado, os pertinentes argumentos de Andrade (2018, p. 112), ao salientar a análise de risco envolvendo os dados sensíveis e a Atividade de Inteligência. O autor pondera que:

> Conhecendo os riscos, sua probabilidade de ocorrência e o seu impacto, bem como compreendendo suas ameaças e vulnerabilidades, o processo decisório certamente terá maior segurança na escolha

> da opção mais vantajosa para alcançar seus objetivos ao adotar uma abordagem sistemática e disciplinada para a avaliação e melhoria da eficácia dos processos de gerenciamento de riscos, de controle e de governança corporativa (*ibidem*).

Essa percepção da matéria encontra pleno apoio na pesquisa de Borges, Menez e Cabral (2021, p. 6), que escreveram sobre o processo de formulação e implementação de planejamento estratégico em instituições do setor público, "uma vez que a Administração Pública está vinculada a normas jurídicas, como por exemplo, o Acórdão TCU 1.603/2008-Plenário, que tratou sobre os problemas de gestão, devido à ausência de planejamento estratégico". A falta de conhecimento dos riscos expõe a fragilidade do processo decisório. Sem conhecimento o tomador de decisões pode se precipitar e cometer erros administrativos graves que poderão inserir a Administração Pública em zona de riscos e de descontrole governamental.

O escopo da Atividade de Inteligência, nesse cenário, é assessorar o processo decisório de autoridades (políticas e militares), além de apoiar o planejamento para detectar ameaças e evitar crises/conflito. Por meio da produção de conhecimentos adequados e em conformidade com os interesses políticos e estratégicos, a Inteligência deve se apoiar em larga gama de informações, englobando os fatores políticos, econômicos, científico-tecnológicos, psicossociais e questões militares. Isto é possível de se obter através da integração de todas as fontes de informação e de Inteligência no processo de produção de conhecimento.

Observa-se, de outro lado, no que concerne à necessidade de a Atividade de Inteligência ser tratada como um serviço de Estado, que a União Europeia estabeleceu que a informação pode ser restringida nas seguintes áreas: defesa nacional, relações com outros Estados, relações com organizações internacionais, questões comerciais, financeiras e fiscais, questões relacionadas com a repressão e prevenção de crimes, em determinados aspectos da administração da justiça e qualquer evento que viole a privacidade das pessoas e se refira a arquivos pessoais e clínicos (PALÁCIOS, 2021, p. 13-28).

"A legislação sobre as chamadas informações confidenciais em diferentes países inclui estes pontos e estabelece limitações à livre circulação de informações" (RUEDA, 2016, p. 9). Aquele que possuir informações dessa natureza, ainda que adotando a postura de boa-fé, pode pecar pelo zelo excessivo ao optar pela restrição ou tornar pública a informação, por meio da divulgação, com o risco de violação de direitos da personalidade, por exemplo, em um ou em outro caso, porque se expõe os dados pessoais que identificam a pessoa no meio social em que ela vive ou se priva os demais cidadãos de informações que poderiam ser relevantes para a sociedade.

Oportuno referir ainda, nesse ponto,

que outro aspecto da Atividade de Inteligência que não se pode olvidar, é a contrainteligência, ou seja, a ação antecipatória que neutraliza as ameaças detectadas. "A segurança da informação e comunicações são as ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações" (BRASIL, 2019, p. 16). A adoção de protocolos e de medidas de segurança antecipatórias se destinam ao resultado que se conhece como contrainteligência. São ações concretas que têm como finalidade prevenir, detectar, obstruir e neutralizar a inteligência adversa, espionagem e ações de qualquer natureza que constituam ameaças à proteção de dados, informações, conhecimento de interesse e da segurança dos cidadãos (*ibidem*).

Não se pode desconhecer, a propósito da questão, a pertinência da doutrina de inteligência militar terrestre, que traz o ramo da contrainteligência como uma parte indissociável do serviço de inteligência. O objetivo é a neutralização da atuação da Inteligência adversa e de ações de qualquer natureza que possam se constituir em ameaças à salvaguarda de dados, informações, conhecimentos e seus suportes, tais como documentos, áreas, instalações, pessoal, materiais e meios de tecnologia da informação, como desdobramento da lógica de expansão dos sistemas de Inteligência (CEPIK, 2003 p. 102).

A matéria ganha relevo, quando se discute exatamente a extensão do uso da inteligência cibernética (*Cyber Intelligence* – CYBINT) elaborada a partir de dados, protegidos ou não, obtidos no espaço cibernético. "Este, por sua vez, é caracterizado como o espaço virtual composto por dispositivos computacionais conectados em rede, onde informações digitais trafegam, são processadas" (BRASIL, 2015. p. 22).

O modo de tratar um dado sensível, a partir do olhar da Atividade de Inteligência, assume, nesse contexto, espaço de centralidade na discussão ora proposta. Torna-se premente fixar parâmetros para a utilização de dados sensíveis dos usuários pela Administração Pública, por meio da implementação dos serviços de Inteligência. Afinal, "cabe à Atividade de Inteligência acompanhar o ambiente interno e externo, buscando identificar oportunidades e possíveis ameaças e riscos aos interesses do Estado e à sociedade brasileira" (BRASIL, 2017, p. 07).

Ao receber o conhecimento produzido, o usuário poderá utilizá-lo em seu processo decisório e também fazer demandas à Inteligência para que aprofunde determinado tema. Esse retorno por parte do usuário é menos comum à medida que o conhecimento chega a escalões mais superiores. Daí que se ensina aos analistas, no curso de formação, a não esperarem qualquer reação do usuário em virtude dos relatórios e documentos produzidos, por

mais relevantes que pareça a seu autor – isso se dá dentro de uma prática de Inteligência relacionada ao "desenvolvimento de resistências a frustrações" (GONÇALVES, 2008, p. 74).

Todas as informações pessoais obtidas durante o atendimento ao público, na atuação do agente público, exigem redobrada atenção porque podem ser usadas indevidamente e causar discriminação do indivíduo. Em especial aquelas que revelam a origem racial ou étnica, as convicções religiosas ou filosóficas, as opiniões políticas, a filiação sindical, questões ligadas à genética, informações biométricas, à saúde física e mental e à vida sexual.

A vulnerabilidade é um fator que faz com que a pessoa natural abandone o senso de privacidade e se lance nas mãos daqueles profissionais com seus segredos, angústias e aspirações mais íntimas que carrega. O consentimento para tratamento desses dados na maioria das vezes é um ato mecânico, formal, que nem sempre é esclarecido suficientemente pelo profissional que está coletando os dados, sem proteger adequadamente os direitos da personalidade. Não se pode tolerar o desenvolvimento do direito de negligência, como discorreu Dennis Lloyd (2000, p. 332), na obra "A ideia da Lei".

Diante das situações emergenciais que exigem rápida intervenção o quadro se agrava, porque não se pode afirmar que existe o livre consentimento do usuário em face da premente necessidade de se revelar o que lhe foi requerido/solicitado pelo agente público. Não se pode afirmar com exatidão se há transparência nos termos e clareza suficiente nas palavras para que a pessoa, por exemplo, analfabeta, tenha plena compreensão do que será feito com as informações coletadas.

Assentadas essas premissas, torna-se importante assinalar os argumentos de Ambros e Lodetti (2019, p. 14), a respeito de vieses cognitivos na Atividade de Inteligência, sobretudo quando "o profissional de Inteligência comete involuntariamente ao processar informações". O autor desenvolve o raciocínio e argumenta que "é importante que o profissional de Inteligência conheça o funcionamento de seu próprio processo mental e esteja alerta para os erros que pode cometer ao desenvolver sua análise".

Esse tema assume inquestionável relevo, porque as características essenciais dos modelos intelectuais no trabalho de analistas da Inteligência designados para produzir avaliações são firmadas em quatro elementos comuns no ambiente da Inteligência: a complexidade das matérias, a ambiguidade nos dados coletados, as compressões de tempo e a pressão para prenunciar uma informação segura.

Portanto, é atual e necessário aprofundar o exame da atuação da Administração Pública na tutela dos dados hipersensíveis das pessoas hipervulneráveis na sociedade

contemporânea. Será a partir dessas reflexões que se poderá propor o desenvolvimento de parâmetros institucionais para a utilização dados sensíveis com respeito aos direitos da personalidade dos usuários.

Considerações finais

A partir das análises empreendidas ao longo deste estudo, é possível extrair que a sociedade da informação na perspectiva da produção de dados sensíveis trouxe o conceito de cibercidadania, que pode ser encarado doravante como direito humano de terceira geração. Além disso, o acesso à internet em alta velocidade se configura como condição de possibilidade para se garantir a efetiva inclusão digital.

Foram constituídas novas plataformas de relacionamento entre a Administração Pública e a sociedade e o uso amplamente difundido das redes sociais e de outros meios de comunicação foi capaz de desestruturar governos que perduraram no poder por décadas. Disso decorre a importância de discutir o impacto das novas tecnologias na revitalização da democracia.

Os elementos de identificação pessoal – tais como: saúde, inclinação política ou ideológica, orientação sexual, gostos, preferências, capacidade financeira etc. – são dados que não podem ser descuidados. O tema envolvendo o tratamento de dados sensíveis ainda depende de maior exploração na academia. É correto afirmar que a tutela dos dados hipersensíveis e a proteção da personalidade da pessoa natural ainda é um campo com lacunas que não foram colmatadas pela academia.

No tocante à implementação de serviços de Inteligência no âmbito da Administração Pública e a tutela dos direitos da personalidade, é possível sintetizar que a implantação desse serviço pouparia os riscos que o gestor público está exposto, se fossem reunidas em um relatório de Inteligência as principais informações, como assessoramento, a fim de que o gestor possa visualizar o campo decisório com clareza. Inaugurar um serviço de contrainteligência na estrutura de um órgão público de relevância nacional o protegeria contra ameaças externas, contra atividades de espionagem, vazamento de dados sensíveis para pessoas não autorizadas, bem como identificaria indivíduos com intuitos nocivos aos interesses públicos.

A falta de conhecimento dos riscos expõe a fragilidade do processo decisório. Sem conhecimento, o tomador de decisões pode se precipitar e cometer erros administrativos graves que poderão inserir a Administração Pública em zona de riscos e de descontrole governamental. Isto é possível de se obter através da integração de todas as fontes de informação e de Inteligência no processo de produção de conhecimento

A adoção de protocolos e de medidas

de segurança antecipatórias se destinam ao resultado que se conhece como contrainteligência. São ações concretas que têm como finalidade prevenir, detectar, obstruir e neutralizar a Inteligência adversa, espionagem e ações de qualquer natureza que constituam ameaças à proteção de dados, informações, conhecimento de interesse e da segurança dos cidadãos. Afinal, cabe à Atividade de Inteligência acompanhar o ambiente interno e externo, buscando identificar oportunidades e possíveis ameaças e riscos aos interesses do Estado e à sociedade brasileira.

Portanto, é atual e necessário aprofundar o exame da atuação da administração pública na tutela dos dados sensíveis das pessoas hipervulneráveis na sociedade contemporânea. Será a partir dessas reflexões que se poderá propor o desenvolvimento de parâmetros institucionais para a utilização dados sensíveis com respeito aos direitos da personalidade dos usuários.

Referências

AMBROS, Christiano. LODETTI, Daniel. Vieses Cognitivos na Atividade de Inteligência: Conceitos, Categorias e Métodos de Mitigação. *Revista Brasileira de Inteligência.* Gabinete de Segurança Institucional. Agência Brasileira de Inteligência n. 14. Brasília: Abin, 2019.

ANDRADE, Felipe Scarpelli. Inteligência Policial: Efeitos das distorções no entendimento e na aplicação. *Revista Brasileira de Ciências Policiais.* Brasília. [Vol. 3], nº 2. Disponível em: https://periodicos.pf.gov.br/index.php/RBCP/article/view/57. Acesso em: 24 set. 2023.

BESSA, Jorge. *A contra-espionagem brasileira na guerra fria.* Brasília: Thesaurus, 2009.

BORGES, Paulo Cesar Rodrigues. MENEZ, Josemar Bezerra. De. CABRAL, Josilene Bispo Pinheiro. O processo de formulação e implementação de planejamento estratégico em instituições do setor público. *Revista Processus de Políticas Públicas e Desenvolvimento Social*. [S. l.], v. 3, n. 6, 2021. Disponível em: https://periodicos.processus.com.br/index.php/ppds/article/view/351. Acesso em: 20 set. 2023.

BRASIL. Ministério da Defesa. *Doutrina de Operações Conjuntas:* conceitos doutrinários,1º volume. 2. ed. Brasília: Ministério da Defesa; Estado-Maior Conjunto das Forças Armadas, 2020. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md30-m-01-vol-1-2a-edicao-2020-dou-178-de-15-set.pdf. Acesso em: 20 set. 2023.

BRASIL. Ministério da Justiça e Segurança Pública. *Doutrina Nacional de Atuação Integrada de Segurança Pública: DNAISP*. 2ª. ed. Brasília, 2019. Disponível em: https://dspace.mj.gov.br/handle/1/1080. Acesso em: 21 set. 2023.

BRASIL. Gabinete de Segurança Institucional. *Estratégia Nacional de Inteligência.* Brasília: Gabinete de Segurança Institucional, 2017. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/ENINT.pdf. Acesso em: 23 set. 2023.

CEPIK. Marco. *Espionagem e democracia:* agilidade e transparência como dilemas na institucionalização de serviços de inteligência. Rio de Janeiro: Editora FGV, 2003.

FERMENTÃO, Cleide Aparecida Gomes Rodrigues; THOMAZINI, Maria Clara. A relevância dos direitos dos idosos no Século XXI: sob o panorama do expressivo crescimento populacional. *Revista da Faculdade de Direito da Uerj*, n. 40, p. 0127–0142,

2021. Disponível em: https://search.ebscohost.com/login.aspx?direct=true&db=lgs&AN=155291958&lang=pt-br&site=eds-live. Acesso em: 14 set. 2023.

FORNASIER, Mateus de Oliveira. *Democracia e tecnologias de informação e comunicação:* mídias sociais, bots, blockchain, e inteligência artificial na opinião pública e na decisão política. Rio de Janeiro: Lumen Juris, 2020.

FREYTAG-LORINGHOVEN, Hugo Friedrich Phillip Johan, Frei-herr von. *O poder da personalidade na guerra*; tradução de Monica de Mattos Scheliga, Marcelo Soares Brando, Rio de Janeiro: Biblioteca do Exército, 1986.

GONÇALVES, Joanisval Brito. *Atividade de inteligência e legislação correlata*. Niterói-RJ: Impetus, 2009.

GONÇALVES, Joanisval Brito. *Conhecimento e poder:* A atividade de inteligência e a Constituição brasileira. Organizadores: Bruno Dantas [et al.]. Imprenta: Brasília, Senado Federal, Instituto Legislativo Brasileiro, 2008.

GREGÓRIO, Daniely Cristina da Silva. TEIXEIRA, Rodrigo Valente Giublin. O reconhecimento dos novos direitos da personalidade e a efetividade do acesso à justiça na pós-modernidade. *Revista de Constitucionalização do Direito Brasileiro*, v. 4, nº 2, 2023. Disponível em: https://search.ebscohost.com/login.aspx?direct=true&db=edsdoj&AN=edsdoj.1fb3d945443142328975e1ae70d6bea4&lang=pt-br&site=eds-live. Acesso em: 13 set. 2023.

HARDT, Michael. NEGRI, Antonio. *Império*. 8ª ed. Rio de Janeiro: Editora Record, 2006.

HIRONAKA, Giselda Maria Fernandes Novaes. *Contrato*: estrutura milenar de fundação do direito privado. Superando a crise e renovando princípios, no início do vigésimo primeiro século, ao tempo da transição legislativa civil brasileira. In: BARROSO, Lucas Abreu. Introdução crítica ao direito civil. Rio de Janeiro: Forense, 2006.

KENT, Shermarn. *Informações Estratégicas*. Vol. 57. Rio de Janeiro: Biblioteca do Exército, 1967.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. *Revisão de decisões automatizadas na Lei Geral de Proteção de Dados Pessoais***.** 2022. 329 f. Tese (Doutorado em Direito) - Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2022.

LLOYD, Dennis. *A ideia da lei*. São Paulo: Martins Fontes: 2000.

OTERO, Cleber Sanfelici; RODRIGUES, Mithiele Tatiana. Discriminação ambiental: da proteção das minorias excluídas pela sociedade contemporânea. *Direito da Cidade*, v. 10, n. 1, 2018. Disponível em: https://search.ebscohost.com/login.aspx?direct=true&db=lgs&AN=128097871&lang=pt-br&site=eds-live. Acesso em: 14 set. 2023.

PALACIOS, José Miguel. Cooperación entre servicios de inteligencia: la dimensión regional. *Revista De Relaciones Internacionales, Estrategia y Seguridad*, 2021. Disponível em: http://www.scielo.org.co/pdf/ries/v16n1/1909-3063-ries-16-01-13.pdf. Acesso em: 23 set. 2023.

PÉREZ LUÑO, A. E. Teledemocracia, ciberciudadania y derechos humanos. *Revista Brasileira de Políticas Públicas* - UNICEUB, vol. 4, n. 2, 2014. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/2835/pdf. Acesso em: 17 jan. 2023.

PÉREZ LUÑO, A. E. *Derechos Humanos, Estado de Derecho y Constitución*. 6ª ed. Tecnos: Madrid. Espanha, 2012.

PÉREZ LUÑO, Antonio Enrique. *Internet y los derechos humanos***.** Navarra: Cizur Menor, 2006. v. 3.

PÉREZ LUÑO, Antonio Enrique. *Nuevas tecnologías, sociedad y Derecho: el impacto socio-jurídico de las N.T. de la información*. Madrid: Fundesco, 1987.

PLATT, Washington. *Produção de informações estratégicas*. Tradução dos Major Álvaro Galvão Pereira e Capitão Heitor Aquino Ferreira. Rio de Janeiro, Biblioteca do Exército: Livraria Agir Editora, 1974.

RUEDA, Fernando. *Servicios de Inteligencia*: ¿fuera de la ley? Bibliotecaonline. Madrid, 2016.

SALVO, Sílvia Helena Picarelli Gonçalves Johonson Di. *Direitos e garantias da proteção de dados pessoais tratados pela administração pública brasileira*: o piso da proteção normativa. 2022. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2022. . Acesso em: 14 nov. 2023.

SICHONANY NETO, Saul de Oliveira; NASCIMENTO, Valéria Ribas do. *A cibercidadania como direito humano de terceira geração e o acesso à internet em alta*

velocidade: a PEC 479/2010 frente à inclusão digital. In: ROVER, Aires José; Disponível em: http://www.publicadireito.com.br/artigos/?cod=5bcbb81902363066. Acesso em: 13 nov. 2023.

SILVA, Tarcízio. *Racismo algorítmico*: inteligência artificial e discriminação nas redes digitais. E-book. São Paulo: Edições Sesc SP, 2022.

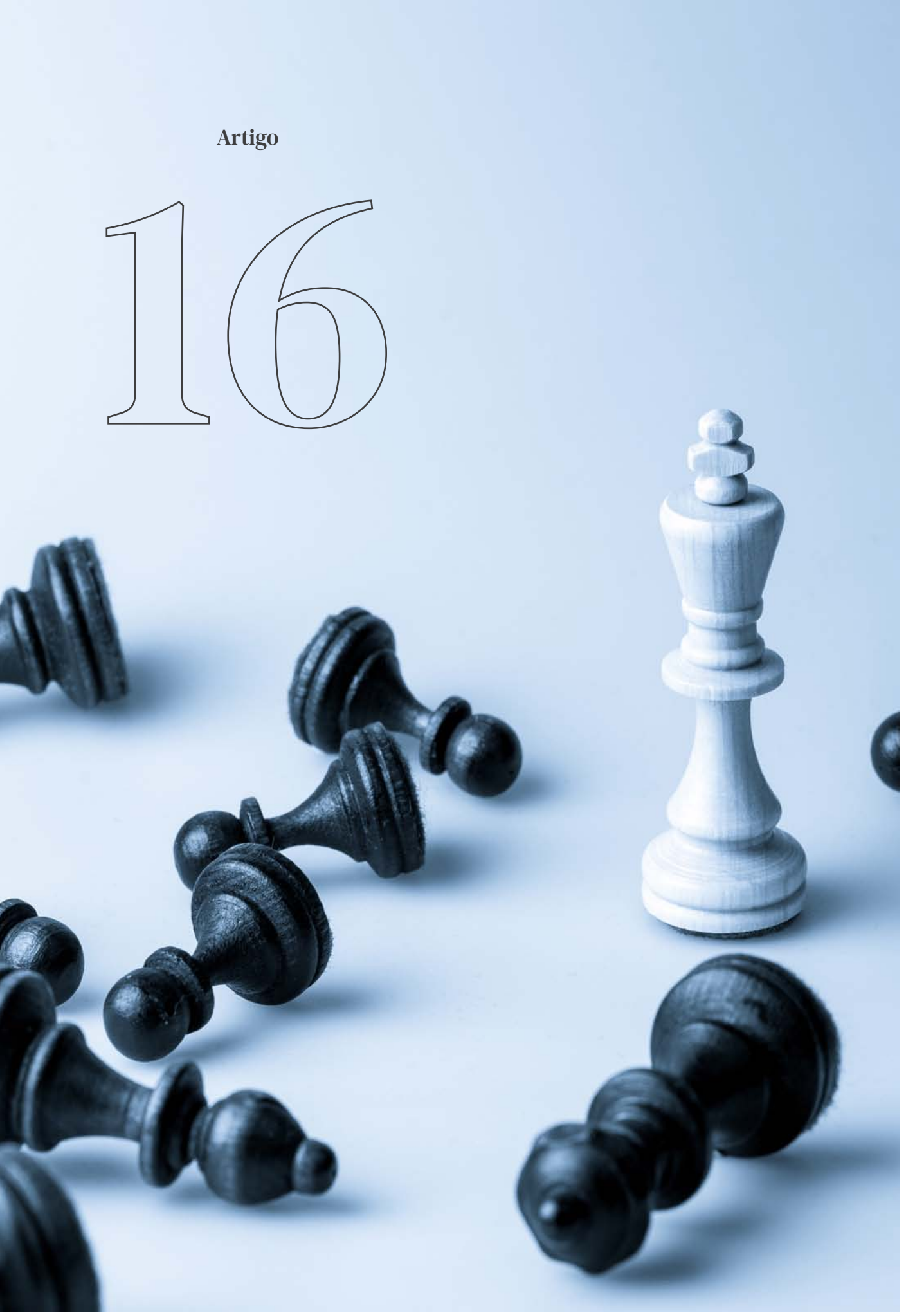
SIQUEIRA, Dirceu Pereira. SANTOS, Marcel Ferreira. SANTOS. Bianca El Hage Ferreira. Auxílio Inclusão à Luz da Dignidade da Pessoa Humana: Benefício de Prestação Continuada à Pessoa com Deficiência e a Lei 14.176/2021. *Revista Jurídica Cesumar.* V. 22, n. 2, 2022, maio/ago.

TEFFÉ, Chiara Antonia Spadaccini de. *Dados pessoais sensíveis:* uma análise funcional da categoria e das hipóteses de tratamento. 2022. 310 f. Tese (Doutorado em Direito) - Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2022

WOLKOFF, Tania Giandoni. *A era da comunicação digital:* a necessidade de uma política nacional de inteligência artificial. 2021. Tese (Doutorado em Direito) - Programa de Estudos Pós-Graduados em Direito da Pontifícia Universidade Católica de São Paulo, São Paulo, 2021.

Artigo

16



Resenha de: JIA, Mai. 2022. *O criptógrafo*. São Paulo: Cia das Letras, 336 p. ISBN: 978-6-5592-1214-9

GUERRA DE CÉREBROS

WAR OF BRAINS

GUERRA DE CEREBROS

DOI: https://doi.org/10.58960/rbi.2023.18.237

Hércules Rodrigues de Oliveira *

Em março de 2016, Edward Snowden, ex-consultor da Agência de Segurança Nacional (NSA), asilado na Rússia, posta, em seu *Twitter,* a seguinte mensagem: "*Going dark* [2] é um conto de fadas: três anos após as manchetes de escuta de *@dilmabr* ela ainda está fazendo chamadas não criptografadas". Snowden se referia ao caso revelado em 2013, em que a presidente Dilma Rousseff foi apontada como alvo direto da espionagem da NSA em documentos classificados como ultrassecretos, obtidos pelo jornalista Glenn Greenwald.

Esse é o ponto de partida para compreender a importância do estudo da criptografia, e, para tanto, convidamo-lo à leitura do livro: "O criptógrafo", de Mai Jia, pseudônimo de Jiang Benhu. O livro foi publicado em inglês em março de 2015 e somente em 2022 chega ao Brasil. Mister registrar que o hiato temporal de sua publicação não diminui a importância do tema, haja vista que todos os serviços de Inteligência de países democráticos ou mesmo totalitários estão desenvolvendo, ininterruptamente, códigos criptográficos para proteção de suas comunicações sigilosas dentro ou fora de seus domínios.

Mai Jia, nascido em 1964, também foi oriundo do serviço militar, serviu no Exército de Libertação Popular (ELP) da China em 1983, sendo especialista em rádio comunicação. Curioso é que o atual serviço secreto chinês, denominado Ministério da Segurança do Estado (*Ministry of State Security* – MSS), foi criado no mesmo ano, embora a espionagem

* Graduado em Pedagogia e Direito pela Universidade Federal de Minas Gerais (UFMG). Mestre em Administração pela Faculdade Novos Horizontes. Instrutor de Contrainteligência.

2 A expressão "ficando no escuro", em português, é usada geralmente para se referir ao uso de criptografia em comunicações.

e a contraespionagem na China sejam ancestrais, e registros de suas práticas datam bem antes da era cristã.

O escritor trilhou os mesmos caminhos de grandes autores de livros de espionagem e de Contrainteligência, tais como Ian Fleming e John le Carré. É considerado um dos autores de grande êxito na atualidade; ganhou, no ano de 2008, pelo conjunto de sua obra, a mais alta honraria literária da China, o prêmio *Mao Dun Literature Prize*[3], realizado de quatro em quatro anos com o objetivo de premiar romances chineses. Vale o registro de que o livro foi adaptado em 2016 para uma série de televisão chinesa com o nome original em inglês: "*Decoded*[4]".

A publicação de Mai Jia traz, de forma inédita, um romance precursor de espionagem do "Império do Meio"[5], que mescla história, ficção, política, criptografia e recrutamento, e envolve os personagens em um mundo hermético, que havia sido bem descrito por Sun Tzu[6] ao dizer: "As luzes e as trevas, o aparente e o secreto: eis toda a arte".

Resenhar o livro abre oportunidade para discutir temas relacionados a Contrainteligência, espionagem, segurança da informação e serviços de Inteligência. Além de temas não necessariamente ligados à Atividade de Inteligência como a xenofobia e a fragilidade humana por meio da jornada do anti-herói solitário que supera obstáculos com um final inesperado.

A obra nos brinda com a "guerra de cérebros", o embate entre os operadores de Inteligência ideologicamente antagônicos, mas que se respeitam mutuamente em razão das ciências exatas que usam para desvendar "segredos". E demonstra uma assertiva da Contrainteligência o homem continuará sendo o elo mais fraco na corrente da segurança pública e privada.

O criptógrafo, personagem vivido pelo introspectivo Rong Jinzhen, criado desde tenra idade por um estrangeiro, gerou desconfiança de muitos compatriotas em razão da xenofobia, mas foi com ele que Jinzhen aprendeu a elucidar a "quimera que nos chega à noite"

O leitor, ao mergulhar nesta obra, perceberá que o emblemático Jinzhen se parece tal qual os indecifráveis algoritmos aos quais se entrega e terá a sensação do antigo mito grego sobre a Esfinge de Tebas e seu misterioso ultimato: "Decifra-me ou te devoro". O futuro "espião que não se

3 Mao Dun: pseudônimo de Shen Dehong, dramaturgo chinês que foi Ministro da Cultura de Mao Zedong em 1965.

4 Decodificado, de 2017, ganhador do Prêmio Nacional de Melhor Produção de Televisão.

5 A China era chamada de Império do Meio, porque ingleses e portugueses comerciavam em Cantão, ao Sul, ao Norte ficavam outros povos, e, no meio, a China, que era avessa a estrangeiros.

6 Filósofo, general e estrategista chinês conhecido por seu tratado militar "A Arte da Guerra".

amava[7]", órfão, com sintomas de depressão, autista e desgracioso, foge do estereótipo fictício criado por Ian Fleming: charmoso, conquistador e letal, o agente secreto 007, James Bond, com licença para matar, a serviço da espionagem britânica MI-6[8].

Com seu jeito taciturno, ganhou o apelido na família de "coisinha". A princípio ignorado e admoestado pelos colegas de escola, recebe inicialmente o apelido de "cabeção". Com o tempo e de forma silente, mostra-se, aos colegas de sala de aula, um gênio da matemática e um místico revelador de sonhos. Devido à glória e à ruína presentes ao mesmo tempo no personagem, resolveram mudar o apelido para "bobogênio".

O livro está dividido em cinco partes, cujos títulos atípicos são: Prelúdio; Desdobramento; Viravolta; Reviravolta e Conclusão. O autor acrescentou "Anexos", onde são apresentados ao público parte do diário de Ron Jinzhen e entrevistas, que criam no leitor um clima de jornalismo investigativo e invasivo sobre a vida do grande herói.

O "Prelúdio" foi escrito em um ritmo envolvente, e descreve a origem da família do protagonista, principalmente de seu pai, que ele não chegou a conhecer, cujos comportamento e moral não eram nada edificantes; por outro lado, a consanguinidade maternal lhe concedeu a intelectualidade.

No "Desdobramento", passamos a conhecer a infância, onde aprendeu a interpretar sonhos, e a origem de seu nome Jinzhen, que significa: "sinceridade de ouro". Assistimos a sua adolescência, ao início da vida adulta e a sua trajetória acadêmica, cujo cerne era sua obsessão pela matemática, em virtude da facilidade com cálculos e com o raciocínio lógico.

Na universidade, conhece um professor polonês de descendência judaica que o inicia nos primeiros passos da Inteligência Artificial (IA). Os acontecimentos se sucedem em uma China que havia sido invadida pelo Japão, terminava a 2ª Grande Guerra e estava em plena guerra civil contra o Kuomintang[9].

Chegamos ao capítulo da "Viravolta". Ron Jinzhen é recrutado na universidade pela Unidade Especial 701, uma agência do Serviço de Inteligência Chinês, cujo objetivo é a contraespionagem, a decifração de códigos e o emprego da criptografia. Esse fato ocorre em junho de 1956, três

7 Alusão ao filme "007 O Espião que Me Amava", de 1977, homônimo do romance de Ian Fleming, escrito em 1962.

8 *Military Intelligence Section 6:* agência britânica de Inteligência que atua junto ao governo britânico com informações estrangeiras.

9 Partido Nacionalista Chinês que tem sido historicamente o governante da República da China (Taiwan), desde a década de 1970.

anos após o cessar-fogo da Guerra da Coreia[10].

Ron Jinzhen recebe o seu codinome "5603K". O número 56 se refere ao ano de seu recrutamento, 1956; o número 03 informa que é o terceiro membro a fazer parte da Unidade Especial 701; e "K" informa que faz parte da área de criptografia. Para a Contrainteligência, recrutar pessoas certas significa êxito no embate da espionagem. Como não poderia faltar o toque cômico à narrativa, o recrutador entrega documento secreto ao reitor da universidade com a seguinte ordem: "queime depois de ler", uma clara alusão ao filme de comédia americano, de mesmo nome, dirigido pelos irmãos Coen, e uma crítica ao Serviço de Inteligência dos Estados Unidos da América (EUA), país inimigo, eufemisticamente aqui chamado de País X.

Na conturbada Revolução Cultural que inicia em 1966 (ano de seu casamento), o protagonista se vê obrigado a interceder pela família, alvo de violência ideológica, o que conseguiu, haja vista que já era considerado um herói nacional, condecorado pelo Comitê Central do Partido, pois havia decifrado o Código Púrpura, concebido pelo seu ex-professor polonês, que, na verdade, era um espião do País X.

Reviravolta. Uma vez solucionado o Código Púrpura, uma nova "guerra de cérebros" se inicia. O antigo mestre agora tinha convicção de que fora Ron Jinzhen quem havia elucidado seu código. Eis que surge o Código Black, mais sofisticado, uma outra ameaça à segurança nacional chinesa. A sina comum a todos os criptógrafos do mundo é sempre buscar algo que se encontra em um lugar inatingível. A obsessão em desvendar o Black leva nosso criptógrafo ao cansaço físico e ao colapso mental.

Enfim, a conclusão. O desafio ao leitor para aproveitar a chance de expandir a visão sobre o tema apresentado, momento propício para conhecer um pouco da história e da cultura da China, um país unipartidário, segundo mais populoso do mundo e com um Produto Interno Bruto (PIB) extraordinário.

Ao final, retorno ao dilema da Esfinge. No desenlace, enxergamos o caminho percorrido pelo protagonista que foi do brilhantismo à insanidade. Por derradeiro, a triste constatação de que a Esfinge de Tebas venceu.

10 Assinado um armistício em 27 julho 1953 que determinou o paralelo 38 como limite geográfico entre a República Popular Democrática da Coreia do Norte e República da Coreia.

Artigo

17

Resenha de: Kissinger, Henry A.; Schimdt, Eric; e Huttenlocher, Daniel, 2021. *The age of AI and our human future*. John Murray Press. 272p. ISBN 978-1529375985

A ERA DA INTELIGÊNCIA ARTIFICIAL: UMA RESENHA CRÍTICA PARA A INTELIGÊNCIA NACIONAL

THE AGE OF ARTIFICIAL INTELLIGENCE: A CRITIAL REVIEW FOR NATIONAL INTELLIGENCE

LA ERA DE LA INTELIGENCIA ARTIFICIAL: UNA REVISIÓN CRÍTICA PARA LA INTELIGENCIA NACIONAL

DOI: https://doi.org/10.58960/rbi.2023.18.238

Bruno Martini Moreira *
Maria Célia Barbosa Reis da Silva **

A Inteligência Artificial (IA) é uma das principais tecnologias emergentes com potencial para revolucionar a compreensão de mundo pela humanidade e do seu lugar nele, oferecendo tanto riscos quanto oportunidades revolucionárias e profundas implicações filosóficas, como o que é a faculdade mental da inteligência e o que é o ser humano quando confrontado com outra forma de inteligência. Uma das mais importantes obras internacionais a tratar desses assuntos é "*The Age of AI: and our human future*", em português "A Era da IA: e nosso futuro como humanos".

O peso literário atribuído à obra é, em grande parte, reflexo da notoriedade dos seus três autores. Henry Kissinger, Secretário de Estado dos Estados Unidos da América (EUA) de 1973 a 1977, ganhador do Nobel da Paz em 1973, da Medalha Presidencial da Liberdade (dos EUA) em 1977 e Medalha da Liberdade em 1986. Atualmente, é diretor da consultoria internacional Kissinger Associates. Eric Schmidt é engenheiro de *software*, empresário e um dos maiores bilionários do mundo. Foi CEO de 2001 a 2011

* Mestre em Dinâmica de Sistemas Costeiros e Oceânicos pela Universidade Federal do Paraná (UFPR). Doutorando em Ciências Aeroespaciais pela Universidade da Força Aérea (UNIFA). Professor no Rockfeller Language Center.

** Mestre em Vernáculas pela Universidade Federal do Rio de Janeiro (UFRJ). Doutora em Literaturas de Língua Portuguesa pela Pontifícia Universidade Católica do Rio de Janeiro (PUC/RJ). Professora Titular da Universidade da Força Aérea (UNIFA) e da Escola Superior de Guerra (ESG). Editora Executiva da Revista da Escola Superior de Guerra. Pesquisadora convidada da Fundação Casa de Rui Barbosa.

e atual presidente executivo e conselheiro técnico do Google. Serviu na Comissão de Segurança Nacional (dos EUA) sobre IA. E Daniel Huttenlocher foi Reitor-fundador da Cornell Tech da Universidade de Cornell em Nova Iorque e primeiro Reitor da Faculdade de Computação Schwarzman do Instituto de Tecnologia de Massachusetts (MIT). Além de acadêmico em ciência da computação, tendo dezenas de patentes registradas, já ocupou cargos de diretor em grandes indústrias tecnológicas, como Xerox e Amazon.

Logo no Prefácio, os autores comentam que procuraram não celebrar e nem lamentar a Inteligência Artificial (IA). Independentemente de sentimentos e opiniões, o assunto tem se tornado onipresente. Responsavelmente, os autores ressalvam que não têm a presunção de esgotar o assunto, se propondo mais a elaborar perguntas do que a fornecer todas as respostas. Algumas dessas perguntas são: A IA percebe aspectos da realidade que nós não? Quais e como serão as inovações em saúde, biologia, espaço, física quântica e estratégia permitidas pela IA? A IA pode realmente ser capaz de pensamento independente? Tem consciência ou algum senso de moralidade? Como a IA afetará a humanidade em sua cognição, interação e percepção do mundo e de si mesma? A humanidade será capaz de entender tudo o que a IA descobrir e como ela fez isso? E quando não entender, deve confiar nas decisões da IA? Ou deve assumir o risco de recusar uma performance superior? E como um Estado pode confiar que seu oponente também está recusando, ou pelo contrário, que está confiando na decisão incompreensível da IA?

O primeiro capítulo, "Onde Estamos", apresenta alguns exemplos notáveis de IAs contemporâneas, que podem ser classificadas como Inteligência Artificial Restrita (IAR), consideradas ainda em um nível abaixo da capacidade intelectual humana. Alguns exemplos mencionados são a AlphaZero que inovou em estratégias de xadrez; a GPT-3 que simula textos e conversas; e o desenvolvimento do antibiótico halicina com o auxílio de uma IA. Os autores alertam no livro que, mesmo enquanto a IA evolui se mantendo sem autoconsciência, intenção, motivação moralidade ou emoção, muitas pessoas que aprendem, treinam ou interagem com ela, tendem a antropomorfizá-la, mesmo que inconscientemente. O primeiro capítulo é então concluído com a dedução de que o número de indivíduos capazes de criar IA segue crescendo, entretanto a quantidade de profissionais dedicados a estudar suas implicações na humanidade (sociais, legais, filosóficas espirituais e morais) permanece muito pequena.

O capítulo 2 "Como Chegamos Aqui", descreve a história da filosofia (no ocidente) como expressão do pensamento humano e como a emergência da IA poderá influenciá-lo. Compreender aspectos

da própria experiência de percepção da realidade é historicamente um enorme desafio intelectual da humanidade. O ser humano busca identificar e explicar certos aspectos da realidade, seja de forma científica ou teológica, para satisfazer sua ânsia de compreensão de sua própria existência e do seu ambiente. Cada sociedade tem sua própria forma de compreender certos aspectos da realidade, com sua visão particular do mundo moldando sua própria política, economia e regras sociais. O método científico e o Iluminismo aceleraram muito a inovação e o desenvolvimento tecnológico, inaugurando a "Era da Razão". Ficaram notórias diversas distorções humanas de percepção e processamento da realidade, as teorias físicas da Relatividade Geral e Restrita e da mecânica quântica desafiaram ainda mais a capacidade humana de construir uma imagem objetiva da realidade.

Computadores e novos sensores aumentaram muito o potencial humano para captar, armazenar e processar dados. A subsequente interconexão de computadores permitiu o surgimento do ciberespaço, um novo domínio que abre novas possibilidades para uma existência na realidade virtual. Com o surgimento do mundo digital e da IA, novos níveis de percepção e compreensão estão sendo possíveis. O livro argumenta que mesmo que a IA não tenha plena consciência sobre o conhecimento que acessa, sua capacidade de identificar, conectar e explorar padrões da realidade podem fazê-la se aproximar ou até exceder a performance e a razão humanas.

O Capítulo 3 "De Turing Até Hoje – E Além", explora as origens do estudo da Inteligência Artificial, traçando-o metaforicamente até a mitologia grega do ferreiro divino Hefesto, que criou servos autômatos, e cientificamente até 1943, quando foi criado o primeiro computador moderno, levando muitos a especular sua futura capacidade de pensar. Em 1950 o matemático Alan Turing publicou "Maquinário de Computação e Inteligência", onde propôs um teste para identificar se uma máquina pensa. Este Teste de Turing, rotula uma máquina como inteligente para observadores que não sejam capazes de distinguir seu comportamento daquele de humanos. O que importa é a performance e não o processo.

Os autores definem a IA como imprecisa, dinâmica, emergente e capaz de aprendizado. Ela aprende consumindo dados, então estabelece observações e conclusões baseadas nos dados. É considerada imprecisa porque não depende mais de entradas e nem de saídas precisas de informação. É dinâmica porque se mostra capaz de evoluir com a mudança das circunstâncias. E é emergente porque pode encontrar soluções inovadoras para humanos. Então contam o surgimento de redes neurais e das três

formas de aprendizado de máquinas (o supervisionado; o não supervisionado; e o por reforço), enfatizando a necessidade de humanos regularem e monitorarem a IA, afinal ela não tem consciência de suas ações. Apresentam a Lei de Moore (1965), que prevê que a capacidade computacional dobra a cada dois anos e como ainda assim ela não permite antever quando pode surgir uma Inteligência Artificial Geral (IAG) de capacidade comparável à humana, embora este seja um conceito ainda impreciso. Cientistas e filósofos ainda debatem se uma IAG é realmente possível e quais seriam suas características. Os autores se mostram conservadores ao pouco explorarem a IAG e ao não mencionarem sua teoricamente possível evolução para uma Super IA (SIA). SIA é o conceito de uma IA que poderá ter um intelecto superior à soma de todos os intelectos humanos vivos e que já viveram.

No quarto capítulo "Plataformas de Redes Globais", abordam as implicações das redes de contato virtuais, sendo as mais relevantes do mundo provenientes dos EUA (como Google, Facebook e Uber) ou da China (Baidu, WeChat, Didi Chuxing). Nelas a IA já é responsável por sugerir e restringir conteúdos, informações, contatos e armazenar dados de um número de usuários dessas redes que costuma ser maior que as populações nacionais. E este papel será ainda mais onipresente e difícil de monitorar, moldando ideologias e crenças em diversas sociedades. Essas redes estão se tornando atores geopolíticos de peso, competindo entre si, com economias e interesses nacionais e até influenciando agendas diplomáticas. A regulamentação dessas redes e da influência da IA nelas não estão claras, e para um debate informado faltam até mesmo novos termos e definições que abarquem esta nova realidade.

O capítulo seguinte, "Segurança e a Ordem Global", trata da segurança, fato-chave e histórico para a organização social. Após um breve apanhado histórico da defesa, enfocam na emergente ciberguerra, com armas, doutrinas, e estratégias pouco conhecidas e possibilidades para desinformação, inteligência, espionagem, sabotagem e apoio ao conflito tradicional com opacidade (discrição) e baixo custo. Também mencionam que a União Soviética explorou um sistema autônomo capaz de detectar e retaliar um ataque nuclear sem intervenção humana. Sistemas autônomos de armas podem levar a uma corrida armamentista. E o ciberespaço pode se mostrar muito vasto para ser defendido por humanos. Assim, a IA tem potencial para revolucionar estratégias cibernéticas e nucleares, alterando o equilíbrio de forças atual e talvez ameaçando o conceito atual de dissuasão. Quando duas ou mais IAs se confrontarem, pode ser impossível para os humanos de ambos os lados prever os resultados e efeitos colaterais. Os autores argumentam que a IA pode ser facilmente copiada e difundida e advogam a necessidade de conceituar um "cyber equilíbrio de poder" e "dissuasão por

IA". A IA pode ser a primeira tecnologia a ter uso dual, ser facilmente dispersiva e de potencial altamente destrutivo, quebrando um paradigma estratégico atual para o equilíbrio de forças. O capítulo é concluído com a sugestão de seis princípios para ajudar a conter a ameaça global, ao controlar melhor os arsenais sob possível futura influência estratégica, tática e operacional da IA.

"Em uma era na qual máquinas cada vez mais realizam tarefas que apenas humanos costumavam ser capazes, o que então constitui nossa identidade como seres humanos?". A primeira frase do capítulo 6, "IA e a Identidade Humana", o resume bem e faz um bom retrato do livro, em que os narradores propõem perguntas filosóficas sobre a IA. A humanidade viverá a experiência em que os grandes exploradores do mundo, que ajudam a explicar e organizar a realidade, deixarão de ser os humanos, mas IAs que desafiarão a autopercepção humana, seu senso de identidade, realização pessoal e segurança financeira. Sociedades terão de escolher quais decisões aceitarão que sejam tomadas pela opaca IA, decisões que podem se tornar ainda mais difíceis para gerações nascidas, cuidadas e educadas desde bebês por IAs. Até os pais poderão decidir limitar o acesso dos seus filhos à IA, afinal, a crescente quantidade de informação já está diminuindo a frequência do pensamento concentrado e contemplativo das pessoas. A IA também estará sujeita a erros e manipulações no seu quase ininteligível processamento de vastos bancos de dados; e alguns destes podem ser quase impossíveis de serem detectados, afetando a qualidade da informação e até a segurança dos usuários. Mesmo cientistas e especialistas podem se ver incapazes de compreender as compilações e conexões de dados feitas pelas máquinas para seu processo de decisão.

A realidade virtual também implicará desafios éticos como o direito de uma pessoa ser ali representada (simulada) sem o seu consentimento. E quão genuína pode ser essa simulação? Mesmo a própria realidade explorada com o auxílio da IA pode se mostrar algo que os humanos jamais imaginaram e até com padrões que humanos podem não reconhecer ou conceptualizar. Os autores preveem que a revolução da IA ocorrerá mais rapidamente do que a maioria das pessoas espera.

O último capítulo (7. IA e o Futuro) retoma o histórico da difusão do conhecimento no mundo ocidental. E na medida em que sociedades adotarem IAs para produzir conhecimento, revoluções tão profundas surgirão, que a própria "Era da Razão" humana poderá parecer arcaica, sendo substituída pela "Era da IA". Se a IAG se provar possível, esta sofisticada entidade poderá ser vista por muitos como quase divina. E a humanidade terá três opções principais: confiar na IA, associar-se a ela ou postergá-la. E a competição pode

fazer com que a IAG seja utilizada antes de ser devidamente ponderada. A natureza etérea, opaca e facilmente distribuível desta tecnologia torna difícil acordos internacionais que dependam de regimes de verificação efetivos. "A era da IA" precisa de seu próprio Descartes, de seu próprio Kant, para explicar o que está sendo criado e o que isso significará para a humanidade".

Os autores ponderam que sendo os sistemas habilitados pela IA tão disruptivos, os adversários podem decidir atacar antes que eles sejam operacionalizados. E uma vez criados, tais sistemas de IA podem se tornar rapidamente disponíveis para empresas e grupos irregulares. IAs combinadas às armas cibernéticas as tornarão mais destrutivas, imprevisíveis, difíceis de detectar e de atribuir responsabilidade. As distinções entre ações ofensivas e defensivas tenderão a ser pouco claras. O desenvolvimento de computadores quânticos pode acelerar e potencializar ainda mais as capacidades da IA. E no veloz desenvolvimento tecnológico, a humanidade avança mais automaticamente do que conscientemente, sem compreender as implicações filosóficas envolvidas. "Na era da Inteligência Artificial, a busca duradoura pela vantagem nacional deve ser informada por uma ética de preservação humana".

A Estratégia Nacional de Inteligência (Enint) de 2017 menciona como certas tecnologias trazem novas oportunidades e ameaças ao ambiente estratégico de Inteligência de Estado. A IA é uma destas inovações tecnológicas disruptivas da ordem social estabelecida, como no caso do mencionado conceito de "dissuasão por IA". Portanto, cabe ao Sistema Brasileiro de Inteligência (Sisbin) monitorar e informar desenvolvimentos teóricos e tecnológicos em IA e ciências potencialmente associadas, como aprendizado de máquinas, robótica, gestão de metadados e computação quântica.

Impactos tão profundos e prováveis requerem a devida profundidade de planejamento. E sendo a IA uma tecnologia difícil de desenvolver, mas relativamente fácil de se copiar e difundir (como destacado neste livro), um Estado bem informado e preparado com antecedência, mesmo sem o pioneirismo, poderá obter vantagens estratégicas da sua prontidão, caso usada com responsabilidade e sabedoria.

Um grupo de trabalho que permeie distintas agências do Sisbin especificamente dedicado à Atividade de Inteligência tecnológica para *mapear inovações disruptivas nacionais e internacionais, identificando seus pontos fortes, fracos, ameaças e oportunidades tem muito a contribuir para a defesa e o desenvolvimento nacionais.* A Agência Brasileira de Inteligência (Abin), precisa ser um dos principais atores nacionais nas discussões estratégicas por essa busca ética pela vantagem competitiva brasileira.

No mesmo espírito questionador da obra,

esta resenha crítica pergunta: Como será o futuro da Atividade de Inteligência em um mundo em que a inteligência humana não será mais a única participante do jogo? Fazendo uma analogia entre ciência e arte a imagem abaixo foi criada para esta resenha crítica pelo artista Pedro Wadt em associação à IA chamada "Leonardo.ai". A imagem representa a figura mítica de Janus, o deus romano das mudanças e transições e um dos símbolos da Atividade de Inteligência, com sua dupla face aqui composta pelo criador (intelecto humano) e criatura (IA) compartilhando e se complementando no exercício da lógica e da razão. Nessa "Era da IA", como a Inteligência nacional poderá contribuir para acompanhar os desenvolvimentos relevantes em IA? Como responsavelmente incorporar as inovações em IA às suas atividades para aumentar sua eficiência e moldar um futuro mais favorável ao Brasil? Quais os cenários nacionais e internacionais mais realistas e prováveis para os quais o Brasil deve se preparar em uma geopolítica cada vez mais influenciada por IAs? E afinal, como revisitar todos os nossos conceitos de Inteligência?

Figura 1 - Janus, símbolo da Atividade de Inteligência, com uma face dotada de inteligência humana e outra de IA.

Fonte: Wadt, Pedro; Leonardo.AI (2023)

gov.br/abin
revista@abin.gov.br
ouvidoria@abin.gov.br